



Politecnico di Bari

Repository Istituzionale dei Prodotti della Ricerca del Politecnico di Bari

Advanced modeling techniques and methodologies for reliable and secure blockchain platforms design

This is a PhD Thesis

Original Citation:

Advanced modeling techniques and methodologies for reliable and secure blockchain platforms design / Fiore, Marco. - ELETTRONICO. - (2025). [10.60576/poliba/iris/fiore-marco_phd2025]

Availability:

This version is available at <http://hdl.handle.net/11589/281780> since: 2025-01-10

Published version

DOI:10.60576/poliba/iris/fiore-marco_phd2025

Publisher: Politecnico di Bari

Terms of use:

(Article begins on next page)



LIBERATORIA PER L'ARCHIVIAZIONE DELLA TESI DI DOTTORATO

Al Magnifico Rettore
del Politecnico di Bari

Il sottoscritto **Fiore Marco** nato a **Terlizzi (BA)** il **26/05/1997**

residente a **Ruvo di Puglia (BA)** in **Piazza F. Cavallotti, 6** e-mail **marco.fiore@poliba.it**

iscritto al 3° anno di Corso di Dottorato di Ricerca in **Ingegneria Elettrica e dell'Informazione** ciclo **XXXVII**

ed essendo stato ammesso a sostenere l'esame finale con la prevista discussione della tesi dal titolo:

Advanced Modeling Techniques and Methodologies for Reliable and Secure Blockchain Platforms Design

DICHIARA

- 1) di essere consapevole che, ai sensi del D.P.R. n. 445 del 28.12.2000, le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del codice penale e delle Leggi speciali in materia, e che nel caso ricorressero dette ipotesi, decade fin dall'inizio e senza necessità di nessuna formalità dai benefici conseguenti al provvedimento emanato sulla base di tali dichiarazioni;
- 2) di essere iscritto al Corso di Dottorato di ricerca in Ingegneria Elettrica e dell'Informazione ciclo XXXVII, corso attivato ai sensi del "Regolamento dei Corsi di Dottorato di ricerca del Politecnico di Bari", emanato con D.R. n.286 del 01.07.2013;
- 3) di essere pienamente a conoscenza delle disposizioni contenute nel predetto Regolamento in merito alla procedura di deposito, pubblicazione e autoarchiviazione della tesi di dottorato nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica;
- 4) di essere consapevole che attraverso l'autoarchiviazione delle tesi nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica del Politecnico di Bari (IRIS-POLIBA), l'Ateneo archiverà e renderà consultabile in rete (nel rispetto della Policy di Ateneo di cui al D.R. 642 del 13.11.2015) il testo completo della tesi di dottorato, fatta salva la possibilità di sottoscrizione di apposite licenze per le relative condizioni di utilizzo (di cui al sito <http://www.creativecommons.it/Licenze>), e fatte salve, altresì, le eventuali esigenze di "embargo", legate a strette considerazioni sulla tutelabilità e sfruttamento industriale/commerciale dei contenuti della tesi, da rappresentarsi mediante compilazione e sottoscrizione del modulo in calce (Richiesta di embargo);
- 5) che la tesi da depositare in IRIS-POLIBA, in formato digitale (PDF/A) sarà del tutto identica a quelle **consegnate**/inviata/da inviarsi ai componenti della commissione per l'esame finale e a qualsiasi altra copia depositata presso gli Uffici del Politecnico di Bari in forma cartacea o digitale, ovvero a quella da discutere in sede di esame finale, a quella da depositare, a cura dell'Ateneo, presso le Biblioteche Nazionali Centrali di Roma e Firenze e presso tutti gli Uffici competenti per legge al momento del deposito stesso, e che di conseguenza va esclusa qualsiasi responsabilità del Politecnico di Bari per quanto riguarda eventuali errori, imprecisioni o omissioni nei contenuti della tesi;
- 6) che il contenuto e l'organizzazione della tesi è opera originale realizzata dal sottoscritto e non compromette in alcun modo i diritti di terzi, ivi compresi quelli relativi alla sicurezza dei dati personali; che pertanto il Politecnico di Bari ed i suoi funzionari sono in ogni caso esenti da responsabilità di qualsivoglia natura: civile, amministrativa e penale e saranno dal sottoscritto tenuti indenni da qualsiasi richiesta o rivendicazione da parte di terzi;
- 7) che il contenuto della tesi non infrange in alcun modo il diritto d'Autore né gli obblighi connessi alla salvaguardia di diritti morali od economici di altri autori o di altri aventi diritto, sia per testi, immagini, foto, tabelle, o altre parti di cui la tesi è composta.

Luogo e data Bari, 07/01/2025

Firma Marco Fiore

Il/La sottoscritto, con l'autoarchiviazione della propria tesi di dottorato nell'Archivio Istituzionale ad accesso aperto del Politecnico di Bari (POLIBA-IRIS), pur mantenendo su di essa tutti i diritti d'autore, morali ed economici, ai sensi della normativa vigente (Legge 633/1941 e ss.mm.ii.),

CONCEDE

- al Politecnico di Bari il permesso di trasferire l'opera su qualsiasi supporto e di convertirla in qualsiasi formato al fine di una corretta conservazione nel tempo. Il Politecnico di Bari garantisce che non verrà effettuata alcuna modifica al contenuto e alla struttura dell'opera.
- al Politecnico di Bari la possibilità di riprodurre l'opera in più di una copia per fini di sicurezza, back-up e conservazione.

Luogo e data Bari, 07/01/2025

Firma Marco Fiore



Politecnico
di Bari



REGIONE
PUGLIA



Department of Electrical and Information Engineering

ELECTRICAL AND INFORMATION ENGINEERING

Ph.D. Program

SSD: ING-INF/05 – INFORMATION PROCESSING SYSTEMS

Final Dissertation

Advanced Modeling Techniques and Methodologies for Reliable and Secure Blockchain Platforms Design

by

Fiore Marco

Supervisor:

Prof. Marina Mongiello

Coordinator of Ph.D. Program:

Prof. Eng. Mario Carpentieri

La ricerca è stata realizzata con il cofinanziamento dell'Unione europea - POC Puglia 2014-2020 - Asse X - Azione 10.4 "Interventi volti a promuovere la ricerca e per l'istruzione universitaria". Approvazione Avviso pubblico n. 1/POC/2021 "Dottorati di ricerca in Puglia XXXVII Ciclo".

Course n°37, 01/11/2021-31/10/2024

*Here's to the fools who dream
crazy as they may seem*

Mia Dolan,
La La Land

Ringraziamenti

Il film *La La Land*, uscito nel 2016 e candidato a 14 premi Oscar, ha segnato il mio percorso universitario. Questo musical parla di Mia Dolan e Sebastian Wilder, rispettivamente un'aspirante attrice e un musicista jazz, che cercano di inseguire i loro sogni. Il titolo del film è sia un riferimento alla città di Los Angeles sia al significato di essere proprio nel "mondo dei sogni" o "fuori dalla realtà." La locandina italiana recita: "Dedicato ai folli e ai sognatori."

Ho visto il film più volte nell'arco di questi 8 anni in università e ogni volta sono stato travolto da una serie di emozioni complesse ma coese, un vortice in cui spesso mi piace entrare e che spesso voglio esplorare. In particolare, in questi ringraziamenti vorrei focalizzarmi su una frase, presente anche all'inizio di questa tesi. Si tratta di una frase detta da Mia durante un provino, in cui racconta la storia di sua zia, che apparentemente senza motivo entrò a piedi scalzi nella gelida Senna. Sorrise, esultò senza guardare, e le disse che lo avrebbe rifatto, di nuovo.

"Here's to the fools who dream, crazy as they may seem."

Mia, verso la fine della canzone, rivela di ricondurre la sua ispirazione per intraprendere la carriera di attrice proprio a quel momento, un aneddoto che la zia usava per dimostrarle che "un po' di follia è la chiave per darci nuovi colori da vedere", anche se non sappiamo dove questo ci porterà. Un elogio a quel pizzico di follia che contraddistingue il talento di un artista che osa alla ricerca di una scintilla, per quanto a volte possa sembrare sciocco.

Trovo alcune analogie interessanti con il percorso che ho intrapreso in questi tre anni di dottorato: lottare ogni giorno per conquistarsi un posto in un mondo vasto, in cui devi costantemente costruire qualcosa di nuovo. Un mondo in cui devi essere un sognatore, devi inseguire i tuoi obiettivi, perchè no, anche essere un po' folle. Eppure, alla fine del viaggio, tutto ciò per cui hai lottato prende forma e nasce in te una nuova consapevolezza. Inizi a guardare la tua vita e ciò che ti circonda con occhi diversi, inizi a capire qual è il tuo contributo nella società. In te c'è la sicurezza di aver costruito qualcosa che, anche se non trovasse dimostrazioni empiriche, rimarrà per sempre indistruttibile.

Il finale del film è un elogio a quei folli che hanno avuto il coraggio di vivere un sogno, dandosi manforte per alimentare i sogni che nutrivano singolarmente; ai folli disposti a sacrificare qualcosa di più concreto pur di realizzare i propri sogni più profondi. Ai folli che, quando ce la fanno, hanno uno sguardo diverso. Quello sguardo è la sensazione di possedere qualcosa che riempie la nostra anima ogni giorno, per sostenerla. Io quel sogno lo sto realizzando, e non voglio smettere di realizzarlo. Eppure, da solo sarebbe stato molto più complicato affrontare questo percorso. Fortunatamente, non sono stato solo, anzi! Questo lavoro è frutto di una serie di aiuti, diretti o indiretti, ricevuti negli ultimi 3 anni. Per questo, la tesi non è solo mia, ma è dedicata a più persone che ritengo fondamentali per definirmi ciò che sono oggi.

A Francesca, mia moglie. Per la prima volta non scrivo "la mia fidanzata" nei ringraziamenti, ed effettivamente fa uno strano effetto. Ho sempre parlato di come lei riesca sempre a inseguire i suoi sogni e a conquistarli: un po' folle, come me. Le nostre idee sono tutte fuori dal comune, entrambi sappiamo che a volte, se si vola troppo vicini al sole, ci si può bruciare, ma senza un po' di calore non ci sarebbe divertimento. E il meglio deve ancora arrivare.

Ai miei genitori, dimostrazione che delle fondamenta efficaci sono indispensabili per costruire un edificio stabile. Mi hanno sempre accompagnato, hanno sempre festeggiato ogni mio traguardo e spronato a ogni difficoltà. Sono davvero l'esempio da seguire, un modello a cui rivolgermi nel corso della vita. Non riuscirò mai a ringraziarvi abbastanza. A mia sorella, a Gianluca e alla loro famiglia che cresce sempre più: sposata quando mi sono laureato in triennale, con Giorgio in magistrale, ora con Stefano per il dottorato. Un esempio efficace di perseveranza e dedizione.

A tutti i colleghi che mi hanno accompagnato in questo lungo percorso. A Mqtt-Team, a tutto ciò che siamo diventati in tre anni e a tutto ciò che diventeremo. Alle giornate insieme, al cibo cucinato e agli album creati in Google Foto. A quei ricordi che occupano uno spazio speciale, che mai si esaurirà, nel mio cuore. A Federico, Cico, Giovanni, a quegli amici e colleghi che ho avuto l'onore di accompagnare lungo il loro percorso da laureandi all'interno del Politecnico.

Al mio tutor, la prof.ssa Mongiello, che mi ha mostrato cosa vuol dire lavorare nella ricerca e come trasformare un'idea in un paper. Mi ha fatto capire tutto ciò che vorrò diventare negli anni a venire. A tutti gli altri professori, del PoliBa e non, con cui ho avuto modo di collaborare o anche solo di scambiare due chiacchiere. Ai confronti sempre attivi, allo scambio costante di punti di vista e al perfezionamento continuo dei lavori. La ricerca e la didattica sono dei settori affascinanti, e sono onorato di aver lavorato con voi.

A te, che stai leggendo questi ringraziamenti: che tu possa essere folle e inseguire il tuo sogno, lottare per realizzarlo e infine conquistarlo. Ricorda sempre:

"A bit of madness is key
To give us new colors to see
Who knows where it will lead us?
And that's why they need us."

Abstract

This dissertation explores the transformative potential of Blockchain technology with a primary focus on its application in agri-food traceability and contributions to Software Engineering Education and Training (SEET). Conducted over three years at the Polytechnic University of Bari, this research investigates Blockchain's capabilities to enhance transparency, security, and efficiency across various domains, with an emphasis on bridging the gap between producers and consumers within supply chains.

The work is structured around two main research approaches: a comprehensive analysis of Blockchain technology and the practical development of traceability platforms. The Systematic Literature Review (SLR) conducted as part of this research identifies the primary challenges for Blockchain application in agri-food traceability, including security, architectural design, and the integration of supporting technologies. These insights form the foundation for the proposed traceability models, which reinforce trust between consumers and producers. In addressing Blockchain's technical challenges, the research delves into quantum-safe cryptography, exploring encryption methods capable of withstanding future quantum computing threats. Additional focus areas include hybrid Blockchain architectures combining public and private models and integrating NoSQL databases to support scalable, flexible platforms. Complementary technologies such as Augmented Reality (AR) and Large Language Models (LLMs) are explored for their potential to extend Blockchain's usability across various fields, including digital tourism. In the context of SEET, this dissertation examines methods to enhance training. The integration of gamification and the role of LLMs in peer assessment are analyzed as innovative approaches to improve educational outcomes. This focus on workforce training addresses one of the major open challenges identified in the SLR and underscores the importance of a well-prepared workforce to drive future Blockchain innovation.

Finally, this dissertation outlines several key areas for future research, including decision-support tools for novice Blockchain developers, the automated generation of smart contracts through LLMs, and the integration of Blockchain in the Internet of Drones (IoD). These avenues represent the potential for expanding Blockchain's application scope, enhancing its accessibility, and further reinforcing its role as a transformative technology across industries.

Contents

List of Figures	IX
List of Tables	XII
List of Acronyms	XIII
List of Publications	XVI
1 Introduction	1
2 Background - Blockchain technology	3
2.1 History	3
2.2 Key Elements	5
2.2.1 Distributed Ledger and Block Structure	5
2.2.2 Network Architecture and Node Types	6
2.2.3 Transactions and State Management	6
2.3 Types of Blockchain Networks	7
2.4 Cryptography	8
2.4.1 Merkle Trees and Chain Structure	9
2.5 Consensus Protocols	10
2.5.1 Proof-based Consensus Mechanisms	10
2.5.2 Byzantine Fault Tolerance Based Protocols	11
2.5.3 Hybrid and Emerging Consensus Mechanisms	11
2.6 Mining	12
2.6.1 Mining Economics and Incentives	12
2.6.2 Environmental Impact and Sustainability	13
2.7 Smart Contracts	14
2.7.1 Security Challenges and Vulnerabilities	15
2.8 Non-Fungible Tokens	17
2.9 Common Blockchains	18
2.9.1 Ethereum	18
2.9.2 Hyperledger Fabric	18
2.9.3 IOTA	20

3	Research methodology	21
3.1	Systematic Literature Review	22
3.2	Design and Development	23
3.2.1	Architectural Modeling	23
4	State of the Art analysis	26
4.1	Related work	27
4.2	Research Methodology - Literature Review	28
4.2.1	Definition of Research Questions	28
4.2.2	Paper Selection Strategy	30
4.2.3	Inclusion and Exclusion Criteria	30
4.3	Results and discussion	32
4.3.1	RQ1: What are the Blockchain trend issues in the agri-food sector from 2016 to 2022?	32
4.3.2	RQ2: What research themes have been addressed in previous studies on Blockchain technology and agriculture?	33
4.3.3	RQ3: What solutions may Blockchain build to simplify the problems of stakeholders across the full agri-food chain?	33
4.3.4	RQ4: What kind of information could stakeholders receive and integrate using Blockchain?	34
4.3.5	RQ5: What are the present research gaps between the benefits of Blockchain technology and its limitations?	35
4.3.6	RQ6: Is the matter of security addressed, and if so, at what level?	35
4.4	Open challenges	36
5	Blockchain for Agri-food Traceability	38
5.1	Transparency and Accountability enhancement	39
5.2	Consumers perception	42
5.2.1	Econometrics Results and Discussion	43
6	Blockchain and Cryptography	46
6.1	Quantum Computing	46
6.1.1	Qubits, Superposition, and Entanglement	47
6.1.2	Quantum States Representation: The Bloch Sphere	47
6.1.3	Post-Quantum Cryptography	47
6.1.4	Applications to Blockchain Technology	48
6.2	Related Work	49
6.3	Quantum safe algorithms in a Blockchain	51
6.3.1	Workflow	53
6.3.2	Discussion	55
6.4	Quantum safe signatures	55

6.5	Biometric key-pair generation	57
6.5.1	Common background	57
6.5.2	Fingerprint-based generation	58
6.5.3	Iris-based generation	59
7	Blockchain Architecture	71
7.1	Hybrid private and public Blockchain platform	71
7.1.1	Proposed architecture	72
7.1.2	Scenario	76
7.2	Blockchain implementation on IoT devices	78
7.2.1	Proposed architecture	79
7.2.2	Results and discussion	82
7.3	Hybrid Blockchain and NoSQL Platform	84
7.3.1	Related Work	85
7.3.2	System description	86
7.3.3	Experimental results	88
7.4	Blockchain sustainability	90
7.4.1	Related Work	90
7.4.2	Proposed approach	92
7.4.3	Smart contracts definition	94
7.4.4	Tests and results	94
7.4.5	Collected gas fees	95
7.4.6	Sustainability analysis	96
7.5	Reward-based Architecture	99
7.5.1	Related work	99
7.5.2	System design	100
7.5.3	System analysis	101
7.5.4	Economics considerations	101
7.6	Architecture proposal in a smart city	103
7.6.1	Related work	105
7.6.2	Our approach	107
7.6.3	Clean energy production	107
7.6.4	Encryption of sensitive information	108
7.6.5	Statistical analysis	109
7.6.6	Path planning	109
7.6.7	Proposed architecture	110
8	Additional technologies	113
8.1	Augmented Reality	113
8.1.1	Architecture	114
8.1.2	Sample scenario	115
8.2	Metaverse	116

8.3	Large Language Models	118
8.3.1	Background	119
8.3.2	Related work	120
8.3.3	Research Methodology	122
8.3.4	Results and discussion	124
9	Software Engineering Education and Training	139
9.1	Review on Gamification in SEET	139
9.1.1	Background	140
9.1.2	Related work	142
9.1.3	Research methodology	143
9.1.4	Results and discussion	147
9.2	Gamification in Industries	164
9.3	Intersection between Metaverse and LLMs	166
9.3.1	Our approach	167
9.4	Role of ChatGPT in Education	169
9.4.1	Software Engineering Education techniques	170
9.4.2	Related work	172
9.4.3	Methodology	173
9.4.4	Results	179
9.4.5	Threats to validity	185
10	Conclusion and future research directions	187
10.1	Blockchain and agri-food traceability	187
10.2	Software Engineering Education and Training	190
10.3	Open challenges	191
	Bibliography	192

List of Figures

1.1	Conceptual map summarizing thesis contents	2
2.1	Generic blocks structure in a Blockchain	5
2.2	SHA-256 outputs given a string as input	8
2.3	Merkle Tree Structure in a Blockchain Block	9
2.4	Ethereum block architecture	19
3.1	Systematic Mapping process	23
4.1	PRISMA search methodology	29
4.2	Distribution by pub year	32
4.3	Distribution by search type	32
4.4	Distribution by search area	33
4.5	Distribution by papers base	33
4.6	Distribution by solution	34
4.7	Industry involvement	34
4.8	Traceability information proposed in papers	35
4.9	Technologies used in selected papers	35
4.10	Distribution by treatment of security topic	36
5.1	An architecture incorporating components presented in different works	39
5.2	Architecture of the proposed system	40
5.3	Sequence diagram showing a common scenario of the Tracecoop project	42
5.4	WTP estimate for the attributes	44
6.1	Ethereum block header with SignAlg field added	53
6.2	Proposed architecture overview	53
6.3	UML sequence diagrams for (a) adding a new block to the chain, encrypting it with a defined algorithm and (b) getting a block, de- crypting it with the used encryption algorithm.	54
6.4	Modified node running on Ethereum	56
6.5	Signing and verifying transactions using the modified interface . . .	56
6.6	Architecture of the proposed fingerprint-based system	58

6.7	Architecture of the proposed approach	59
6.8	Distributed architecture organization	61
6.9	UML Sequence diagram	63
6.10	“Search template” smart contract output	64
6.11	HyperLedger Fabric network topology	66
6.12	Required time comparison to generate 1, 10, 100 and 1000 simultaneous key-pairs	69
7.1	Architecture of the proposed platform	72
7.2	Hyperledger Fabric chaincode written in a context-aware approach .	74
7.3	Execution of the Fabric chaincode in a Blockchain-based traceability system	75
7.4	Architecture showing two different approaches for calculating THI .	80
7.5	Hybrid system layered architecture and information flow	87
7.6	Time comparison (in seconds) during data storing activities	89
7.7	Time comparison (in seconds) when performing data retrieving . . .	89
7.8	Gas spent for each Blockchain	96
7.9	CO2 emission per transaction for each analyzed Blockchain	98
7.10	Network example with 10 nodes, each one starting with 100 coins .	100
7.11	Workflow of the system	102
7.12	Layers of the system showing a single interface in the access layer .	104
7.13	Sample process for a citizen requesting a service to government institutions	108
7.14	Architecture of the proposed Blockchain-based smart city	110
7.15	Sequence diagram for a smart city service request	111
8.1	Architecture of the proposed platform	114
8.2	Two alternative graphical interfaces. (a) a pear, with quality 2/10, is surrounded by the attributes gathered from the Blockchain. (b) an apple, with quality 9/10, has its attributes rotating on top of it.	115
8.3	Development steps for the metaverse platform	117
8.4	LLMs evolution until 2023	120
8.5	Evolution of interest in Generative AI related to the appearance of ChatGPT	121
8.6	PRISMA methodology	123
8.7	Papers distribution by month between 2021 and 2023	125
8.8	Papers distribution by type	126
8.9	Papers divided by research category	128
8.10	Papers divided by value added to the community	129
8.11	Papers divided by main application area	130
9.1	A common architecture for gamified educational platforms	141
9.2	PRISMA search methodology	145

9.3	Publication trends over time for gamification in SEET	148
9.4	Distribution of publication types for gamification in SEET	149
9.5	Sectors of application for gamification in SEET	150
9.6	Distribution by search type	151
9.7	Application areas of gamification in SEET	152
9.8	Geographical distribution of studies on gamification in SEET	161
9.9	PRISMA flow diagram	165
9.10	Overview of the research steps	167
9.11	Details of the LLM training phase	168
9.12	Solution generation: first prompt with less details	175
9.13	Solution generation: second prompt with extended details	176
9.14	Class diagram generated by ChatGPT	178
9.15	Sequence diagram generated by ChatGPT	178
9.16	Answers for form question: How easy was it to understand the UML solution generated by ChatGPT?	182
9.17	Answers for form question: Have you ever participated in similar exercises involving human-generated solutions or other tools?	182
9.18	Scores obtained by students in pre- and post-intervention assessment	184
9.19	Completion rate in pre- and post-intervention assessment	184
10.1	Blockchain-based platforms common architecture	188
10.2	Work in progress novel architecture	190

List of Tables

2.1	Comparison of Blockchain Types	7
2.2	Comparison of Major Consensus Mechanisms	11
2.3	Smart Contract Vulnerabilities and Mitigations	16
4.1	Comparison between the related work and the present review	28
4.2	Research questions and their corresponding value	31
5.1	MNL coefficients estimate	44
6.1	Comparative table of encryption algorithms security levels	48
6.2	Post-quantum cryptographic algorithms chosen by NIST in Round 3	52
6.3	Validation scenarios and effects	70
7.1	Memory needed to store transaction in the Blockchain and time needed to upload 100 new transactions	77
7.2	Discomfort Considerations	81
7.3	Benchmark report in Hyperledger Caliper	82
7.4	Retrieving and saving time comparison	90
7.5	Results of contracts execution, in gas, in each chosen Blockchain . .	95
7.6	Analysis of CO2 emission for each analyzed Blockchain	97
7.7	State of the art analysis	106
8.1	Programming languages analyzed in relevant papers	131
8.2	Pros and cons according to the analyzed papers	133
9.1	Comparison between related works and our review	144
9.2	Main finding for each analyzed paper	153
9.3	Comparison of LLMs available online	168
9.4	Feedback form questions and answers	180

List of Acronyms

AR Augmented Reality

DLT Distributed Ledger Technology

EVM Ethereum Virtual Machine

IoD Internet of Drones

IoT Internet of Things

IPFS InterPlanetary File System

LLM Large Language Model

NFT Non-Fungible Token

P2P Peer-to-Peer

PBFT Practical Byzantine Fault Tolerance

PCA Principal Component Analysis

PICO Population, Intervention, Comparison, and Outcome

PoS Proof of Stake

PoW Proof of Work

PQC Post-Quantum Cryptography

PRISMA Preferred Reporting Items for Systematic Review and Meta-Analysis

RQ Research Question

SEET Software Engineering Education and Training

SLR Systematic Literature Review

UML Unified Modeling Language

WTP Willingness-to-Pay

Preface

This dissertation summarizes the work I have done within Blockchain technology during my three years as a Ph.D. candidate at Polytechnic University of Bari. The research was conducted at the Laboratory of Information Systems under the supervision of Professor Marina Mongiello. Most parts of this thesis have been published in International Journals and Conference Proceedings over the last three years.

The main topic relates to the analysis of advancements in Blockchain technology research, starting from the agri-food traceability sector. A secondary topic regarding Software Engineering Education and Training has also been discovered. With respect to the main topic, two main approaches have been followed: a comprehensive state-of-the-art analysis to understand the pros and cons of Blockchain applied to agri-food traceability, and modeling and designing traceability platforms for both producers and consumers. The research started with the acquisition of basic knowledge of Blockchain by examining its historical developments [1], followed by investigating its use in agri-food traceability through a Systematic Literature Review (SLR) [2]. This review highlighted the key challenges and opportunities that Blockchain presents in this sector. Blockchain has been shown to greatly enhance the connection between producers and consumers in agri-food traceability. For consumers, it builds trust in the products they purchase [3], while for producers, it enhances supply chain management through greater transparency and responsibility [4].

The SLR highlighted several open challenges, primarily focused on security and privacy, Blockchain architectures, the integration of complementary technologies, and the need for specialized employee training.

- In terms of security and privacy, my research has addressed the potential threats posed by quantum computing, evaluating quantum-safe encryption algorithms [5], as well as the implications for signatures and key-pair generation [6]. In addition, I contributed to the development of a machine learning-based cyber-attack mitigation system in cloud and fog environments [7].

- Architecturally, my work explored the design of hybrid Blockchain frameworks, merging public and private Blockchain models [8], and integrating Blockchain with NoSQL databases [9]. Additionally, I proposed a reward-based architecture for managing the exchange of goods and services [10], alongside frameworks to enhance the management of smart cities [11] and Internet of Things (IoT) devices [12]. Furthermore, I conducted a deployment cost analysis for smart contracts, assessing their sustainability [13]. An additional review focused on Edge and Fog computing for IoT extended this research scope [14].
- As Blockchain platforms continue to evolve, integrating additional technologies has become crucial. My research also examined the role of the Metaverse in digital tourism [15] and education [16], the potential of Augmented Reality (AR) [17], and the relevance of Large Language Models (LLMs) in Blockchain development.

The employee training open challenge connects to Software Engineering Education and Training (SEET). In this context, I conducted two reviews: one on the usage of gamification in SEET [18], and another exploring gamification in industrial settings [19]. Additionally, I examined how LLMs can enhance SEET, particularly in peer assessment [20].

The findings from these studies have opened new avenues for future research, including Blockchain interoperability, the development of decision support tools for Blockchain developers, the integration of Blockchain in emerging fields such as the Internet of Drones (IoD), and the automation of smart contracts generation using LLMs.

The following is a list of papers published throughout the Ph.D. program.

List of Publications

- [1] M. Fiore and M. Mongiello, “History of Blockchain Technology and its Impact in Social Good”, in *2023 8th IEEE History of Electrotechnology Conference (HISTELCON)*, pp. 36–38, Sept. 2023.
- [2] M. Fiore and M. Mongiello, “Blockchain Technology to Support Agri-Food Supply Chains: A Comprehensive Review”, *IEEE Access*, vol. 11, pp. 75311–75324, 2023.
- [3] M. Fiore, M. Frem, M. Mongiello, F. Bozzo, C. Montemurro, G. Tricarico, and A. Petrontino, “Blockchain-based food traceability in Apulian marketplace: Improving sustainable agri-food consumers perception and trust”, *Internet Technology Letters*, p. e503, 2024.
- [4] M. Fiore, M. Mongiello, G. Tricarico, F. Bozzo, C. Montemurro, A. Petrontino, C. Giambattista, and G. Mercuri, “Blockchain-based Food Traceability System for Apulian Marketplace: Enhancing Transparency and Accountability in the Food Supply Chain (S).”, in *2023 35th International Conference on Software Engineering & Knowledge Engineering (SEKE)*, pp. 114–117, 2023.
- [5] M. Fiore, F. Carrozzino, M. Mongiello, G. Volpe, and A. M. Mangini, “A Blockchain-Based Modular Architecture for Managing Multiple and Quantum-Safe Encryption Algorithms”, in *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, pp. 598–601, July 2023.
- [6] M. Fiore, F. Carrozzino, M. Mongiello, and F. Nocera, “Key-pair Generation using Fingerprint-based Seed in Blockchain Systems”, in *Blockchain & Cryptocurrency Conference (B2C’ 2022)*, p. 112, 2022.
- [7] F. Nocera, S. Abascià, M. Fiore, A. A. Shah, M. Mongiello, E. Di Sciascio, and G. Acciani, “Cyber-Attack Mitigation in Cloud-Fog Environment Using an Ensemble Machine Learning Model”, in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, July 2022.

- [8] M. Fiore, M. Mongiello, and G. Acciani, “A context-aware multiple Blockchain architecture for managing low memory devices”, in *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, June 2023.
- [9] A. Longo, A. Di Palma, L. Casamassima, M. Fiore, and M. Mongiello, “Blockchain and NoSQL: Enhancing throughput via a deep learning-based hybrid architecture”, *Internet Technology Letters*, 2024.
- [10] M. Fiore, F. Nocera, and M. Mongiello, “A Reward-based Blockchain Platform for Exchanging Goods and Services”, in *Blockchain & Cryptocurrency Conference (B2C’ 2022)*, p. 45, 2022.
- [11] M. Fiore and M. Mongiello, “Blockchain for Smart Cities Improvement: An Architecture Proposal”, in *2023 7th International Conference on Computer, Software and Modeling (ICCSM)*, pp. 1–5, July 2023.
- [12] G. Spadavecchia, M. Fiore, M. Mongiello, and D. De Venuto, “A Novel Approach for Fast and Secure Data Transmission using Blockchain and IoT”, in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, June 2024.
- [13] S. Bistarelli, M. Fiore, A. I. Lazzizzera, I. Mercanti, and M. Mongiello, “Analysis of Blockchain Sustainability through the Comparison of Different Smart Contracts Programming Languages”, in *6th Distributed Ledger Technology Workshop (DLT 2024)*, vol. 3791, (Turin, Italy), pp. 1–11, 2024.
- [14] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, “Edge Computing and Cloud Computing for Internet of Things: A Review”, *Informatics*, vol. 11, p. 71, Dec. 2024.
- [15] E. C. Ciliberti, M. Fiore, and M. Mongiello, “Development of a Metaverse Platform for Tourism Promotion in Apulia”, in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pp. 680–681, June 2023.
- [16] M. Fiore, M. Gattullo, and M. Mongiello, “First Steps in Constructing an AI-Powered Digital Twin Teacher: Harnessing Large Language Models in a Metaverse Classroom”, in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 939–940, Mar. 2024.
- [17] M. Fiore, M. Gattullo, M. Mongiello, and A. Uva, “Merging Blockchain and Augmented Reality for an Immersive Traceability Platform”, in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 933–934, Mar. 2024.

- [18] V. Di Nardo, R. Fino, M. Fiore, G. Mignogna, M. Mongiello, and G. Simeone, “Usage of Gamification Techniques in Software Engineering Education and Training: A Systematic Review”, *Computers*, vol. 13, p. 196, Aug. 2024.
- [19] M. Fiore and M. Mongiello, “Gamification for Machinery and Infrastructure Learning in Industries: A Review”, in *Automation, Robotics & Communications for Industry 4.0/5.0*, p. 157, 2023.
- [20] M. Fiore and M. Mongiello, “Using Peer Assessment Leveraging Large Language Models in Software Engineering Education”, *International Journal of Software Engineering and Knowledge Engineering*, July 2024.

Chapter 1

Introduction

The agri-food sector faces several critical challenges, including ensuring food safety, improving traceability, and enhancing transparency across the supply chain. These challenges are exacerbated by the involvement of multiple stakeholders, diverse systems, and the need for trust in the recorded data. As the demand for secure and efficient traceability systems grows, Distributed Ledger Technologies (DLTs), such as Blockchain, emerge as a promising solution to address these issues.

Blockchain systems have been widely adopted in various domains, ranging from cryptocurrency to traceability systems, and from videogames to smart cities. The technology's core characteristics, including data immutability, high resistance to tampering, and the ability to ensure trust in multi-stakeholder environments, make it particularly suitable for solving issues in the agri-food sector. Blockchain is an append-only data storage solution where data, once added, is cryptographically linked to the preceding records. This structure makes tampering highly challenging, as modifying a single block would compromise the integrity of the entire chain.

In contexts like the agri-food sector, where data integrity and trust are paramount, Blockchain's capability to provide transparency and verifiability is invaluable. For example, its adoption enables the tracking of food products from farm to fork, thereby ensuring compliance with safety standards and fostering consumer trust. Additionally, advancements in Blockchain technology, such as the transition from Proof of Work (PoW) to Proof of Stake (PoS) in certain systems, highlight ongoing efforts to enhance efficiency and sustainability without compromising security.

This thesis investigates the application of Blockchain technology to the agri-food sector. It begins with an exploration of Blockchain's historical development and foundational concepts in Chapter 2. A Systematic Literature Review (SLR), presented in Chapter 4, focuses specifically on the use of Blockchain in agri-food traceability systems [2]. The SLR identifies key challenges and research gaps, which serve as the basis for subsequent chapters.

The findings from the SLR have informed the design and development of Blockchain-based traceability platforms, which aim to benefit both producers and consumers.

These platforms are detailed in Chapter 5. Furthermore, the identified research challenges are addressed in various dedicated chapters:

- Chapter 6 examines security and privacy considerations, including the implications of quantum computing and biometric key-pair generation.
- Chapter 7 models hybrid architectures that integrate multiple Blockchain platforms and approaches.
- Chapter 8 explores complementary technologies, such as Augmented Reality (AR) and Large Language Models (LLMs), which can enhance Blockchain-based systems.
- Chapter 9 discusses Software Engineering Education and Training (SEET), with a focus on gamification and the role of LLMs in academic and professional training. This chapter is linked to the need for employee training, a key challenge highlighted in the SLR.

Finally, Chapter 10 concludes the thesis by summarizing the contributions and providing an outlook for future research directions. A conceptual map summarizing the thesis contents and their interconnections is shown in Fig. 1.1.

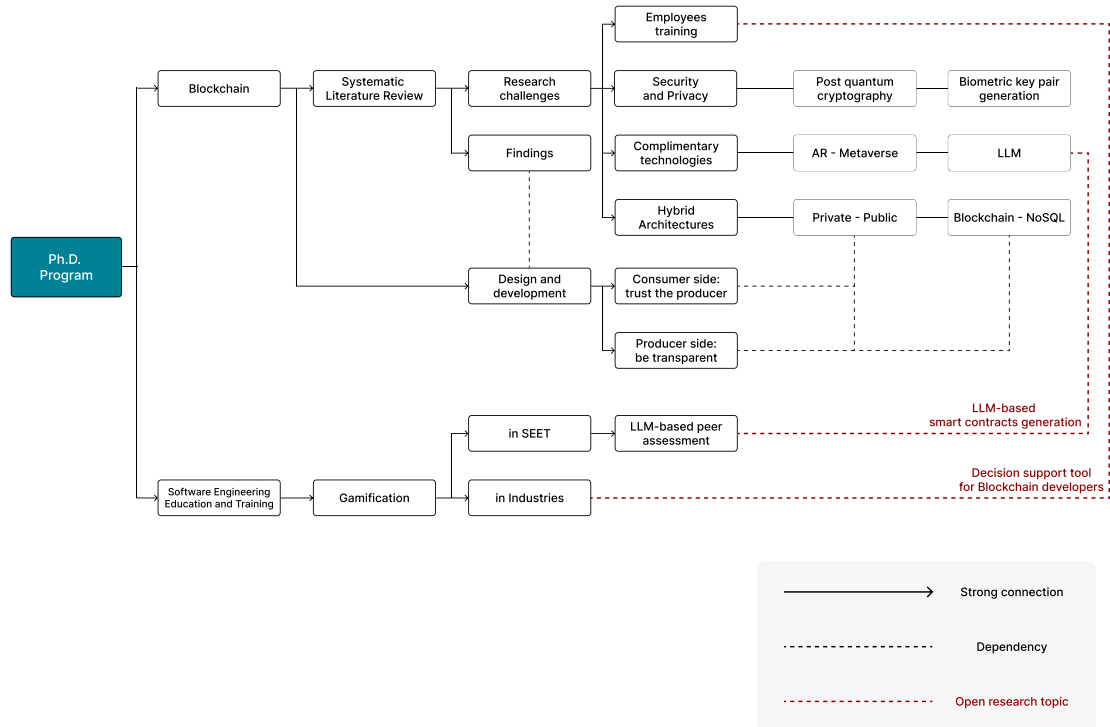


Figure 1.1: Conceptual map summarizing thesis contents

Chapter 2

Background - Blockchain technology

2.1 History

A brief history of Blockchain technology has been proposed in a dedicated history conference [1].

The first traces of Blockchain technology date back to 1979, with a book written by David Chaum [21]. Chaum describes the idea of a distributed computer system where suspicious groups can interact in a consistent and private way. Transactions are stored in some blocks, called *vaults*, responsible of signing, recording and broadcasting transactions.

In 1991, Haber and Stornetta published a book describing how to timestamp a digital document [22]. In this discussion, cryptographically secured chain of blocks are introduced, with timestamps that could not be modified.

In 2008, Nakamoto published the whitepaper of Bitcoin [23], the first decentralized Blockchain application, which was designed to function without the need for a central authority, such as a government or financial institution. The Nakamoto whitepaper is a seminal document in the field of cryptocurrencies and Blockchain technology. It outlines the technical design and features of the Bitcoin system, including the use of a distributed ledger known as the Blockchain, which records all transactions on the network in a transparent and immutable way.

The Nakamoto whitepaper has been the focus of various scientific studies and analyses, ranging from technical evaluations of the Bitcoin protocol to explorations of the socio-economic consequences of cryptocurrencies. Some key areas of research related to the Nakamoto whitepaper include: a) cryptography: the Nakamoto whitepaper introduced a number of cryptographic techniques that are essential to the Bitcoin system, such as digital signatures and hash functions; b) distributed systems: the Bitcoin network is a decentralized system that relies on a network of nodes to maintain the integrity of the Blockchain; c) economics: the whitepaper advocated a new sort of money unattached to any central authority.

This has resulted in an increasing research on the economic implications of cryptocurrencies, such as price stability and adoption rates; d) social and political implications: the decentralized and anonymous nature of cryptocurrencies has raised important questions about privacy, regulation, and the role of governments in controlling the flow of money. Overall, the Nakamoto whitepaper has played a key role in shaping the development of the cryptocurrency and Blockchain ecosystem.

After the introduction of Bitcoin, the Blockchain technology evolved rapidly. In 2013, Vitalik Buterin proposed Ethereum [24], a revolutionary Blockchain platform that introduced the concept of programmable smart contracts. The Ethereum whitepaper described a platform that would go beyond simple cryptocurrency transactions, allowing developers to create decentralized applications (DApps) and implement complex business logic through smart contracts. This marked the beginning of what is commonly referred to as Blockchain 2.0.

The evolution of Blockchain technology can be categorized into three main generations:

- **Blockchain 1.0:** Represented by Bitcoin and other cryptocurrencies, this generation focused primarily on monetary transactions and digital currency applications. The main innovation was the ability to transfer value in a decentralized manner without intermediaries.
- **Blockchain 2.0:** Initiated by Ethereum in 2015, this generation introduced programmable smart contracts and enabled the development of decentralized applications. This evolution expanded Blockchain's potential beyond financial transactions, enabling complex automated agreements and introducing new concepts like tokens and decentralized finance.
- **Blockchain 3.0:** The current generation focuses on addressing the limitations of previous generations, particularly in terms of scalability, interoperability, and sustainability. Projects in this generation aim to enable cross-chain communication, reduce energy consumption through alternative consensus mechanisms, and provide enhanced privacy features.

Recent developments have seen the emergence of various specialized Blockchain platforms designed for specific use cases. For instance, Hyperledger Fabric [25], launched in 2015, was specifically designed for enterprise use, offering modularity and privacy features crucial for business applications. Similarly, platforms like Cardano introduced new consensus mechanisms to address the environmental concerns associated with traditional mining.

The period from 2018 to present has been characterized by increasing institutional adoption and the emergence of new applications beyond cryptocurrencies. Notable developments include the rise of Non-Fungible Tokens (NFTs), decentralized finance protocols, and the integration of Blockchain technology in various sectors including supply chain management, healthcare, and notably, the agri-food

industry. These advancements have demonstrated the technology's potential to transform traditional business processes and create new paradigms for digital interaction and value exchange.

2.2 Key Elements

The fundamental architecture of Blockchain technology comprises several key elements that work together to ensure its functionality, security, and decentralization. This section explores the core components that form the foundation of Blockchain systems.

2.2.1 Distributed Ledger and Block Structure

The cornerstone of Blockchain technology is the distributed ledger, which maintains a complete record of all transactions across a network of nodes. Unlike traditional centralized databases, this ledger is replicated and synchronized across all participants, ensuring transparency and redundancy [26].

Each block in the Blockchain contains fundamental elements:

- **Timestamp:** A timestamp of when the block was created
- **Data:** The actual content of the transactions or information being stored
- **Hash:** A unique cryptographic identifier of the current block
- **Previous Hash:** The hash of the preceding block, creating the chain structure

The linking of blocks through hash references creates an immutable chain, where any attempt to modify historical data would require changing all subsequent blocks, making tampering practically impossible in well-established networks. Fig. 2.1 shows the content of a generic block.

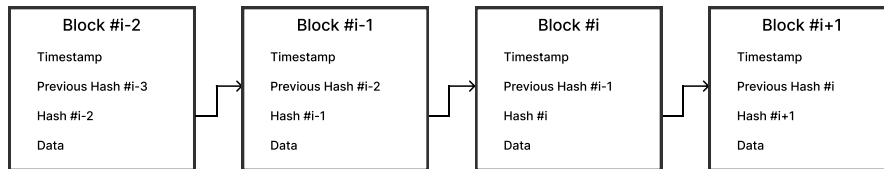


Figure 2.1: Generic blocks structure in a Blockchain

2.2.2 Network Architecture and Node Types

The Blockchain network operates on a Peer-to-Peer (P2P) architecture, where nodes communicate directly without intermediaries. Three primary types of nodes exist within most Blockchain networks [27]:

- **Full Nodes:** Store the complete Blockchain and validate all transactions and blocks. They play a crucial role in maintaining network integrity by independently verifying adherence to protocol rules.
- **Mining/Validator Nodes:** Specialized nodes that participate in the consensus process, creating new blocks and adding them to the chain. These nodes compete or collaborate (depending on the consensus mechanism) to maintain network security.
- **Light Nodes:** Store only block headers and rely on full nodes for complete information. They are particularly useful for resource-constrained devices that still need to interact with the network.

2.2.3 Transactions and State Management

Transactions represent the atomic unit of change in a Blockchain system. Each transaction undergoes several stages before being permanently recorded [28]:

1. *Creation:* A transaction is initiated and digitally signed by the sender
2. *Propagation:* The transaction is broadcast to the network for validation
3. *Verification:* Nodes verify the transaction's validity (e.g., sufficient funds, correct signatures)
4. *Inclusion:* Valid transactions are included in a new block
5. *Confirmation:* The block is added to the chain through consensus

The state of the Blockchain represents the current status of all accounts and smart contracts at any given point. State management is crucial for maintaining consistency across the network and ensuring that all nodes reach the same conclusions about the validity of transactions.

2.3 Types of Blockchain Networks

Blockchain networks can be categorized based on their access control and permission management mechanisms. Each type serves different purposes and offers distinct advantages for specific use cases [29].

Public and private Blockchains represent the two fundamental approaches to network accessibility:

- **Public Blockchains** are completely open networks where anyone can participate as a node, validate transactions, and access the ledger. Bitcoin and Ethereum are prominent examples of public Blockchains. Key characteristics include complete decentralization and transparency, no central authority, high redundancy and security, slower transaction processing, and higher energy consumption.
- **Private Blockchains** are controlled by a single organization that determines participation rights. These networks are typically used for internal business operations [30]. Notable features include controlled access and participation, faster transaction processing, lower energy consumption, higher privacy and confidentiality, and centralized control over network rules.

Consortium or federated Blockchains represent a hybrid approach where a group of organizations operates the network collaboratively [31]. This model is particularly relevant for industry-specific applications, such as supply chain management in the agri-food sector. Key characteristics include pre-selected nodes for validation, shared governance among participating organizations, balanced trade-off between decentralization and efficiency, enhanced privacy while maintaining partial decentralization, and customizable consensus mechanisms. A comparison of Blockchain types is shown in Table 2.1.

Table 2.1: Comparison of Blockchain Types

Characteristic	Public	Private	Consortium
Decentralization	High	Low	Medium
Performance	Low	High	High
Scalability	Limited	High	High
Privacy	Low	High	Medium
Cost Efficiency	Low	High	Medium

The selection of a Blockchain type depends on specific requirements and constraints [32]:

- **Public Blockchains:** Cryptocurrencies, public record-keeping, decentralized finance

- **Private Blockchains:** Internal audit trails, asset management, organizational record-keeping
- **Consortium Blockchains:** Supply chain traceability, inter-bank settlements, industry-specific collaboration

2.4 Cryptography

Cryptography is fundamental to Blockchain technology, providing the security mechanisms that ensure data integrity, authentication, and immutability. Hash functions and digital signatures form the backbone of Blockchain's security architecture.

Hash Functions are one-way cryptographic functions that generate a fixed-size output (hash) from any input data. In Blockchain, the most commonly used hash function is SHA-256 [33, 34, 35]. Hash functions possess several critical properties, shown in Fig. 2.2:

- *Deterministic*: The same input always produces the same hash
- *Pre-image resistance*: It is computationally infeasible to derive the input from its hash
- *Collision resistance*: It is extremely unlikely for two different inputs to produce the same hash
- *Avalanche effect*: A small change in input produces a significantly different hash



Figure 2.2: SHA-256 outputs given a string as input

Digital Signatures utilize asymmetric cryptography to provide authentication and non-repudiation. The process involves generating public-private key pairs, signing messages with the private key, and verification using the corresponding public key.

2.4.1 Merkle Trees and Chain Structure

The Merkle Tree, also known as a hash tree, is a fundamental data structure in Blockchain that enables efficient verification of large datasets [36]. Its implementation in Blockchain provides several advantages:

- **Efficient Verification:** Allows verification of a single transaction without processing the entire block
- **Data Integrity:** Any modification to transaction data would change the Merkle root
- **Scalability:** Enables light nodes to verify transactions without storing the complete Blockchain

The structure of a Merkle tree in a Blockchain block is represented in Fig. 2.3.

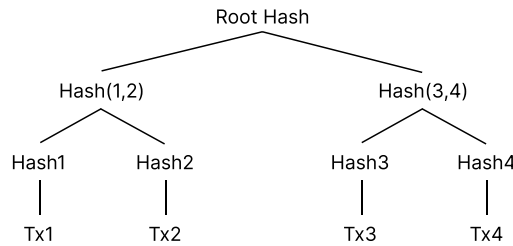


Figure 2.3: Merkle Tree Structure in a Blockchain Block

Modern Blockchain systems employ several advanced cryptographic techniques to enhance privacy and security.

- **Zero-Knowledge Proofs (ZKP):** Allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement. Applications include:
 - Privacy-preserving transactions
 - Confidential smart contract execution
 - Identity verification without data disclosure
- **Ring Signatures:** Enable a user to sign a transaction on behalf of a group without revealing their identity within that group. This technique is particularly useful in:
 - Privacy-focused cryptocurrencies
 - Anonymous voting systems
 - Confidential business transactions

- **Homomorphic Encryption:** Allows computations to be performed on encrypted data without decryption, enabling:
 - Confidential smart contract execution
 - Private data processing
 - Secure multi-party computation

2.5 Consensus Protocols

Consensus protocols are fundamental to the operation of Blockchain networks, as they ensure that nodes within a decentralized, distributed system can reliably agree on the state of the Blockchain. These protocols establish a standardized process that safeguards consistency and security across the network without the need for a central authority [37]. Consensus mechanisms also help to maintain the decentralized nature of the system by enabling network participants to validate and add blocks independently, promoting trust in the network.

2.5.1 Proof-based Consensus Mechanisms

Among the various types of consensus mechanisms, proof-based systems have been widely adopted for public Blockchains. In these systems, network participants — whether they are miners or validators — must demonstrate a form of commitment or stake, thereby contributing to the network’s security and stability.

One of the most recognized proof-based mechanisms is Proof of Work (PoW), which was pioneered by Bitcoin. In PoW, participants, called miners, compete by solving complex mathematical problems, with the first to solve the puzzle being awarded the right to validate the next block. The security of PoW lies in its requirement for significant computational power, making attacks highly impractical due to the substantial energy and resource cost. However, this reliance on computing power also means that PoW is energy-intensive, drawing significant environmental criticism. Nonetheless, PoW’s inherent design serves as a natural deterrent against Sybil attacks, where malicious entities try to gain control by creating multiple fake identities [23].

In response to PoW’s energy demands, Proof of Stake (PoS) was developed as an alternative that requires significantly less computational power. Instead of competing with computing resources, validators in PoS “stake” a certain amount of cryptocurrency as collateral, with the probability of being selected to validate a new block directly proportional to the amount staked. This mechanism, although more energy-efficient, introduces potential centralization risks, as participants with larger stakes have a higher likelihood of selection, potentially concentrating power among wealthier stakeholders. PoS mechanisms often incorporate penalties, or “slashing,”

to discourage malicious behavior, enhancing overall security while maintaining efficiency [38]. Table 2.2 presents a comparison of the features of PoW, PoS, and other major consensus mechanisms.

Table 2.2: Comparison of Major Consensus Mechanisms

Feature	PoW	PoS	PBFT
Energy Efficiency	Low	High	High
Scalability	Limited	Medium	High
Decentralization	High	Medium	Low
Finality	Probabilistic	Probabilistic	Immediate
Security	Very High	High	High

2.5.2 Byzantine Fault Tolerance Based Protocols

In permissioned Blockchain networks where all participants are known, Byzantine Fault Tolerance protocols offer another approach to achieving consensus. These protocols are particularly suitable for private or consortium Blockchains due to their focus on ensuring agreement among nodes even when some may behave maliciously. A prominent example is Practical Byzantine Fault Tolerance (PBFT), which is well-suited for smaller networks. In PBFT, nodes undergo a structured process involving pre-prepare, prepare, commit, and reply phases, through which a block proposal is presented by a leader and then confirmed by the other nodes. PBFT provides immediate finality, meaning that once a transaction is confirmed, it is permanently recorded, a feature that enhances its efficiency in controlled environments such as Hyperledger Fabric.

2.5.3 Hybrid and Emerging Consensus Mechanisms

The demand for higher scalability, energy efficiency, and environmental sustainability in Blockchain networks has led to the development of hybrid and emerging consensus mechanisms that combine aspects of traditional protocols with novel approaches [39]. For example, Delegated Proof of Stake is a variation of PoS in which token holders vote for a limited number of block producers to validate transactions. This system, used in high-performance networks like EOS, enhances transaction throughput but often results in more centralized control, as fewer individuals are responsible for block production.

Another emerging model is Proof of Authority, which uses validator identity rather than staked tokens as the basis for block validation. Proof of Authority is highly efficient for permissioned networks and is widely used in private and consortium networks due to its high throughput and low energy requirements. The increasing variety of consensus mechanisms reflects the Blockchain community's

ongoing efforts to develop protocols that address the limitations of earlier designs while balancing decentralization, security, and scalability. Emerging trends focus on enhancing transaction speed, improving energy efficiency, strengthening security measures, and exploring solutions that prioritize environmental sustainability.

2.6 Mining

Mining is the critical process by which new transactions are validated and incorporated into the Blockchain. Through the creation of new blocks, mining ensures both the security and integrity of Blockchain networks. Additionally, this process sustains network participation by providing economic incentives for miners, while raising essential considerations about its environmental impact.

The mining process involves a sequence of computational tasks that require specific technical components. Hardware plays a central role, with high-performance systems such as Application-Specific Integrated Circuits (ASICs), Graphics Processing Units (GPUs), and, less frequently, Central Processing Units (CPUs) being used depending on the network's requirements. ASICs, specialized for the sole purpose of mining, provide efficiency unmatched by other hardware, making them the choice hardware for networks with significant hash power demands like Bitcoin. GPUs, meanwhile, offer versatility and are commonly used in smaller or emerging networks where ASICs are not yet as cost-effective.

Mining also requires specialized software: miners use software for performing hash calculations essential for proof-of-work computations, wallet software for receiving rewards, and a network client to facilitate the propagation of new blocks once validated. Together, this hardware and software ecosystem enables miners to participate in the validation and security of the network.

The mining workflow consists of collecting unconfirmed transactions from the mempool, followed by validating these transactions for accuracy and integrity. Once validated, miners organize these transactions into a candidate block, which is then subjected to a computational proof-of-work challenge. Upon solving this challenge, the miner propagates the validated block across the network, where other nodes verify its correctness before it is permanently added to the Blockchain.

2.6.1 Mining Economics and Incentives

The economics of mining are integral to maintaining Blockchain security, incentivizing participants, and ensuring that miners are rewarded in line with their contributions [40]. Miners earn revenue through a combination of block rewards and transaction fees, providing a financial incentive for miners to dedicate resources to the network. Block rewards introduce new coins into circulation with each mined block, and transaction fees serve as an additional source of income, added by users

to prioritize their transactions in the mempool.

Over time, block rewards undergo scheduled reductions, known as “halving” events. These events, initially implemented in the Bitcoin network, reduce the amount of new cryptocurrency released per block, ultimately preserving scarcity and helping to stabilize the asset’s value. To overcome the high computational costs associated with mining, many participants join mining pools, which are collaborative groups where rewards are distributed proportionally based on each participant’s contributed hash power. Pools employ various payout schemes, such as Pay-per-Share (PPS), Proportional, and Score-based, to ensure fair compensation according to each miner’s contribution.

The profitability of mining depends on several factors, including the block reward (R_b), transaction fees (F_t), the current cryptocurrency market price (P_c), and the costs associated with mining, such as energy costs (C_e), hardware expenses (C_h), and maintenance costs (C_m). These factors combine into a profitability equation:

$$\text{Profit} = (R_b + \sum F_t) \times P_c - (C_e + C_h + C_m) \quad (2.1)$$

This equation underscores the financial considerations miners must assess to determine the feasibility of mining as an ongoing operation.

2.6.2 Environmental Impact and Sustainability

The environmental impact of mining, particularly in PoW networks like Bitcoin, has become a topic of intense debate. The substantial energy consumption associated with mining stems from the extensive computational work required, with estimates indicating that Bitcoin’s annual energy consumption rivals that of medium-sized countries. This energy demand has prompted calls for more sustainable practices and has encouraged the relocation of mining facilities to areas with lower electricity costs, often to regions with abundant renewable energy sources.

In response to environmental concerns, the Blockchain community has explored various sustainability initiatives. One approach is the transition to PoS mechanisms, which drastically reduce energy consumption by eliminating the need for intensive PoW calculations. Another initiative is “green mining,” where mining operations are powered by renewable energy sources like solar, wind, and hydroelectric power, helping to reduce the carbon footprint associated with mining [41].

Other strategies include carbon offset programs, where miners can invest in initiatives that reduce carbon emissions elsewhere, and the development of energy-efficient hardware to minimize the power required per hash. Additionally, heat recycling has gained traction as an innovative approach where the excess heat generated by mining equipment is repurposed for other applications, such as heating buildings or powering agricultural operations.

2.7 Smart Contracts

Smart contracts are self-executing programs stored on the Blockchain that autonomously enforce the terms of a given agreement, providing automation and reliability without the need for intermediaries. By embedding logic directly onto the Blockchain, smart contracts enable complex, decentralized applications that go beyond simple transactions, marking a significant advancement in Blockchain's capabilities [42].

Smart contracts function as autonomous agents, interacting with users and other contracts through the Blockchain. These contracts are defined by specific architectural components that ensure they can perform their operations securely and efficiently [43].

Each smart contract comprises key elements that together facilitate its execution on the Blockchain:

- **Code:** The contract's program logic is written in a language suited to Blockchain platforms (e.g., Solidity on Ethereum). This code defines the contract's behavior, including functions, events, and conditions that must be met for different actions.
- **State:** This is the current condition of the contract's variables. As users interact with the contract, state variables are updated to reflect changes, such as balances or user-defined values.
- **Storage:** Contracts require persistent data storage on the Blockchain, ensuring that contract states are recorded in an immutable ledger.
- **Interface:** This represents the set of functions exposed by the contract that users or other contracts can invoke. The interface defines how external entities interact with the contract, whether through public functions or events emitted during execution.

Smart contracts operate through a systematic execution model, where they are deployed, invoked, and updated in line with Blockchain protocols. The execution model includes the following steps:

1. Deployment to the Blockchain, at which point the contract's code and initial state are recorded immutably.
2. Function invocation through transactions, where users or contracts trigger the smart contract's functions.
3. Validation by network nodes, ensuring that the contract's terms are upheld and that no unauthorized actions occur.

4. State update based on execution results, where changes to contract variables are recorded.
5. Storage of the updated state onto the Blockchain, preserving contract interactions for future reference and audits.

An illustrative example of a smart contract, “ExampleContract,” is shown below:

```
contract ExampleContract {
    // State variables
    address public owner;
    uint256 public value;

    // Events
    event ValueChanged(uint256 newValue);

    // Constructor
    constructor() {
        owner = msg.sender;
    }

    // Functions
    function setValue(uint256 newValue) public {
        require(msg.sender == owner);
        value = newValue;
        emit ValueChanged(newValue);
    }
}
```

This example demonstrates basic smart contract elements, including state variables, a constructor, and a function with access control.

2.7.1 Security Challenges and Vulnerabilities

Smart contracts, despite their benefits, face significant security challenges. Vulnerabilities can expose contracts to various risks, as shown in Table 2.3, highlighting the need for robust design patterns and security protocols [44].

While smart contracts offer automation and security, they face inherent limitations:

- **Immutability:** Once deployed, a contract’s code and logic cannot be changed, making bug rectification challenging.
- **Resource Constraints:** Limited computational resources restrict complex operations, as excessive computation leads to higher costs.

- **Oracle Dependency:** Smart contracts lack native access to external data, relying on oracles to provide accurate information. This dependency can affect contract reliability if the oracle's data is inaccurate or tampered with.
- **Scalability Constraints:** The need for consensus validation limits the transaction throughput, affecting contract scalability.
- **Interoperability Issues:** Contracts on different Blockchains have limited direct interaction, hindering the exchange of data and functionality across platforms.

Table 2.3: Smart Contract Vulnerabilities and Mitigations

Vulnerability	Description	Mitigation
Reentrancy	External calls allowing recursive execution	Check-Effects-Interactions pattern
Integer Overflow	Arithmetic operations exceeding value limits	SafeMath library usage
Access Control	Improper permission management	Role-based access control
Logic Errors	Flaws in business logic implementation	Formal verification

To enhance smart contract efficiency and broaden their applicability, ongoing research and development efforts focus on:

- **Enhanced Security Measures:** Advanced verification techniques and auditing tools aim to minimize vulnerabilities and ensure safe deployment.
- **Scalability Improvements:** Solutions such as layer-two networks, sharding, and cross-chain communication are being explored to overcome scalability limitations.
- **Cross-Chain Interoperability:** Protocols and bridges enabling contracts to communicate across different Blockchains are in development, facilitating data sharing and resource management.
- **Development Tools:** User-friendly development environments and testing frameworks continue to evolve, simplifying the creation and debugging of smart contracts.
- **Standardization Efforts:** Initiatives focused on establishing standards for contract design, function naming, and security guidelines are underway, aiming to streamline contract development and improve reliability.

2.8 Non-Fungible Tokens

Non-Fungible Tokens (NFTs) have introduced a new paradigm in digital asset representation on the Blockchain. Unlike cryptocurrencies, which are fungible and interchangeable, NFTs are unique, indivisible, and provide verifiable ownership of digital assets, fostering authenticity and traceability. Initially popularized through digital art and collectibles, NFTs have rapidly expanded in application across various fields, with emerging uses in the agri-food industry as well [45].

NFTs are based on specific token standards that guide their creation, transfer, and interaction on the Blockchain. Among the most popular standards is Ethereum’s ERC-721, which laid the foundation for creating unique tokens that differ from each other in attributes and identifiers [46]. The ERC-1155 standard followed, allowing the creation of both fungible and non-fungible assets within a single smart contract [47]. This dual functionality has made ERC-1155 particularly versatile for projects requiring various asset types. Other Blockchain platforms, like Binance Smart Chain and Flow, have developed their own standards to address specific technical needs, such as enhancing scalability or lowering transaction fees.

The core characteristics that define NFTs—uniqueness, indivisibility, and provenance—are instrumental in their practical applications. Each NFT contains unique metadata, ensuring that no two tokens are alike, while their indivisibility prevents them from being divided into smaller units. The Blockchain’s transparent, immutable record further guarantees that ownership history, or provenance, remains secure and publicly accessible. Additionally, the programmability of NFTs enables complex interactions and autonomous actions via smart contracts, such as automated royalties or conditional transfers, greatly expanding their potential uses.

In the agri-food sector, NFTs support transparency and product verification throughout the supply chain. For premium products, NFTs offer a tool for verifying authenticity, such as by certifying the organic or geographical origins of items like wine or specialty foods. NFTs can document each stage in the production and distribution processes, protecting against counterfeiting and giving consumers a reliable source of information. For example, by associating individual products or batches with unique NFTs, producers and retailers can ensure that quality standards are met and visible to buyers. NFTs are also being explored in supply chain tracking, enabling stakeholders to follow the journey of high-value items with precision. For instance, agricultural products like specialty grains or produce can be tracked from the farm to the consumer, with relevant data—such as harvest dates or storage conditions—stored immutably. Integrating IoT devices with Blockchain-based systems allows for real-time monitoring, further enhancing traceability through live status updates. NFTs have applications beyond products as well, such as in land management, where they can represent ownership records, leases, or rights, helping stakeholders manage resources and ownership in a digitally secure format.

However, despite these benefits, NFTs in agri-food face both technical and practical challenges. Integrating NFT systems with traditional supply chain operations can be complex, and achieving Blockchain scalability to support high transaction volumes remains a significant issue. Further, data standardization across different supply chains is required to ensure consistent record-keeping, yet it is challenging in a sector as diverse as agri-food. Additionally, implementing NFT-based solutions can be costly, and widespread adoption requires substantial training and regulatory support. Consequently, while NFTs offer innovative solutions for transparency and efficiency, their adoption in agri-food will depend on overcoming these technical and institutional barriers [48].

2.9 Common Blockchains

As Blockchain technology matures, a variety of platforms have emerged, each optimized for specific use cases and technical characteristics. This section explores three widely utilized Blockchain platforms — Ethereum, Hyperledger Fabric, and IOTA — highlighting their distinct features, architectures, and applications.

2.9.1 Ethereum

Ethereum, launched in 2015, is a decentralized, open-source Blockchain platform designed to support smart contracts and decentralized applications. Unlike Bitcoin, which primarily serves as a digital currency, Ethereum’s Turing-complete virtual machine, known as the Ethereum Virtual Machine (EVM), enables developers to deploy self-executing code directly on the Blockchain. This capability has made Ethereum the most widely adopted platform for applications requiring complex logic and automated interactions [24].

Ethereum’s consensus mechanism initially operated on PoW, similar to Bitcoin, but transitioned to PoS through the Ethereum 2.0 upgrade in September 15th, 2022. Ethereum has become a foundation for various decentralized finance applications, NFT marketplaces, and more. The architecture of an Ethereum block is shown in Fig. 2.4.

2.9.2 Hyperledger Fabric

Hyperledger Fabric is an enterprise-focused Blockchain platform developed under the Linux Foundation’s Hyperledger project. Unlike public Blockchains like Ethereum, Hyperledger Fabric is a permissioned Blockchain, which restricts access to a defined network of participants. This permissioned approach is particularly suitable for businesses and consortiums where privacy and control over data sharing are critical. Hyperledger Fabric’s modular architecture allows organizations to

tailor the platform's components, such as consensus mechanisms and data storage, to meet their unique requirements [25].

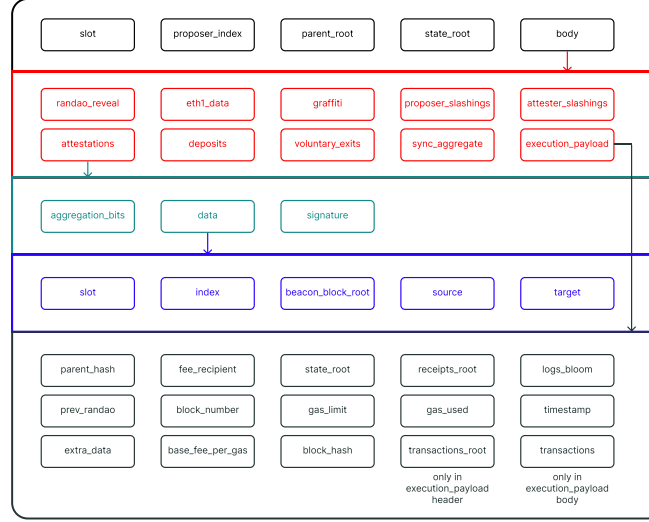


Figure 2.4: Ethereum block architecture

One of the key features of Hyperledger Fabric is its use of "channels," which create private, isolated ledgers between specific participants in the network, ensuring that only authorized members can view certain transactions. Additionally, Hyperledger Fabric does not rely on a single consensus protocol but supports pluggable consensus, enabling users to choose mechanisms based on their needs. Its architecture allows for performance optimization in complex business processes, making it popular in sectors such as supply chain management, finance, and healthcare. It is composed of:

- **Endorsing Peers:** These specialized peers validate and endorse transaction proposals. After receiving proposals, they simulate transactions by executing the requested chaincode to generate a read-write set without committing it. Following simulation, they validate results against business logic and endorsement policies, adding their digital signatures to approve transactions.
- **Proposer:** The proposer is the entity that starts a transaction. It constructs transaction proposals, sending them to endorsing peers for validation. Once endorsements are received, it assembles them to prepare the transaction for ordering.
- **Ordering Service:** This service is essential for sequencing transactions consistently. After collecting endorsed proposals, it organizes them into blocks and reaches a consensus on the transaction order. Once ordered, blocks are distributed to all peers to maintain consistent ledger states.

- **Validators:** Validators are responsible for reviewing the blocks received from the ordering service. They verify endorsements on each transaction and check that blocks comply with network policies and structure. Only transactions that meet all criteria are committed to the ledger.
- **Committers:** Committers finalize the transaction process. After receiving blocks from the ordering service, they perform a final validation on each transaction. Once approved, they commit the transaction to the ledger, marking the transaction as complete across the network.
- **Certificate Authority (CA):** The CA manages digital identities, ensuring only authorized participants interact on the network. It issues certificates, enabling identity verification and secure communication. It also provides tools for administrators to manage certificate renewals, revocations, and other identity maintenance tasks.

2.9.3 IOTA

IOTA represents a departure from traditional Blockchain structures by utilizing a Tangle, a Directed Acyclic Graph data structure. Designed specifically for the Internet of Things, IOTA's architecture eliminates the need for miners by having each new transaction confirm two previous transactions, creating a web of interlinked transactions rather than a linear chain. This unique setup theoretically enables IOTA to achieve higher transaction throughput as network activity increases, making it suitable for IoT applications where scalability and microtransactions are critical [49]. IOTA's architecture offers advantages in terms of scalability and energy efficiency, as it does not rely on energy-intensive mining processes.

Chapter 3

Research methodology

Research methodology encompasses the systematic approaches employed to solve a research problem, ensuring the collection, analysis, and interpretation of data is structured and reliable. In this study, two main methodologies were followed: a *Systematic Literature Review (SLR)* and a *Design and Development Research Methodology*, each suited to the respective phases of the research on Blockchain technology applied to agri-food traceability.

Research methodologies can broadly be classified into several types based on the nature and objectives of the research. These include:

- **Qualitative Research**

This approach focuses on understanding complex phenomena through non-numerical data, such as interviews, observations, and textual analysis. It is particularly suited for exploring the depth of a subject, though less focused on generalizability.

- **Quantitative Research**

Based on numerical data, this methodology is often used to quantify variables and assess statistical relationships. It allows for generalization from sample data to broader populations.

- **Mixed Methods**

Combining both qualitative and quantitative research, this approach offers a comprehensive perspective, allowing researchers to explore both the breadth and depth of a topic.

- **Empirical Research**

This methodology relies on direct or indirect observation and experience, often involving experiments or field studies to test hypotheses.

- **Systematic Research**

SLR is a structured methodology aimed at identifying, analyzing, and synthesizing all available research on a specific topic, ensuring that the study is based on existing evidence.

- **Design and Development Research**

This methodology is focused on creating and evaluating artifacts (such as models, platforms, or frameworks) that solve specific real-world problems, often through iterative design and testing.

In this research, two specific methodologies were employed:

- **Systematic Literature Review (SLR)**

To thoroughly explore the current state of Blockchain technology in the agri-food traceability sector, an SLR was conducted. This method provided a comprehensive understanding of the challenges, opportunities, and existing solutions in the domain, guiding the subsequent design phase of the research.

- **Design and Development Methodology**

Following the SLR findings, a real-world platform was designed and developed to address the practical needs of producers and consumers in the agri-food supply chain. This methodology involved iterative prototyping, implementation, and evaluation to ensure the platform's effectiveness in enhancing transparency and trust within the supply chain.

These methodologies ensure a balanced approach, combining theoretical analysis with practical implementation to address the research objectives.

3.1 Systematic Literature Review

The approach follows the guidelines of a systematic mapping process proposed in [50] and the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) guidelines. The authors outline a five-step workflow, as illustrated in Fig. 3.1: Definition of Research Questions (RQs), Primary Studies Search, Papers Screening, Keywording of Abstracts, and Data Extraction and Mapping of Studies.

- **Definition of Research Questions (RQs)**

RQs define the goals of a study and the outcomes desired from the research.

- **Primary Studies Search**

The objective of the second step is to define a search string to gather papers from online databases. This string can be composed using the Population, Intervention, Comparison, and Outcome (PICO) method [51].

- **Papers Screening**

Gathered papers are filtered through Inclusion and Exclusion Criteria, which include domain affinity, acceptance for publication in a conference, journal, or book, and the main language of the paper, among others.

- **Keywording of Abstracts**

Each paper abstract is categorized using keywords that lead to a classification schema. This schema is useful for better understanding a set of categories that represent the underlying population.

- **Data Extraction and Mapping of Studies**

In the final step, actual data extraction occurs. Here, the provided RQs are answered, and useful insights regarding the topic of interest are identified. Graphics and tables can be employed to highlight trends within the analyzed papers more effectively.

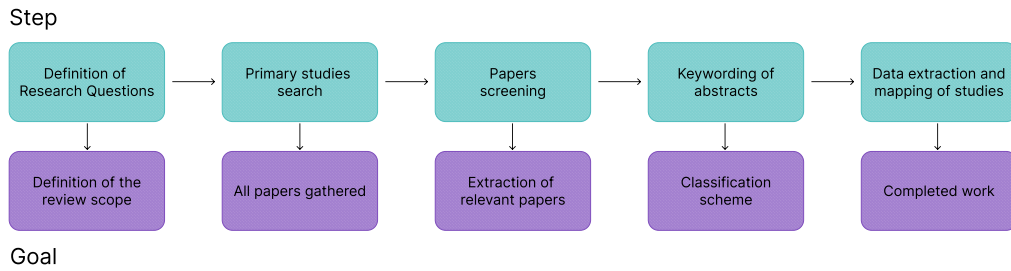


Figure 3.1: Systematic Mapping process

3.2 Design and Development

The second phase of this research focused on the design and development of innovative Blockchain-based architectures that aim to improve both consumer perception and producer transparency in agri-food traceability. This phase adhered to Software Engineering best practices to ensure that the developed platforms were scalable, secure, and user-friendly.

3.2.1 Architectural Modeling

To address the challenges identified during the SLR, several novel architectures were modeled, each focusing on different aspects of agri-food traceability:

- **Consumer Perception Enhancement**

A consumer-facing platform was designed to provide transparency regarding the provenance, handling, and quality of food products. This architecture relied on a public Blockchain to ensure that the information was immutable and verifiable, enhancing consumer trust. Through the use of smart contracts, key milestones in the supply chain were automatically validated, providing real-time updates to consumers.

- **Producer Transparency Improvement**

For producers, a private Blockchain-based architecture was developed to enable secure, transparent tracking of goods along the supply chain. This system allowed producers to monitor and document every step of the production process, ensuring accountability and compliance with regulatory standards. Some considerations on reward-based mechanisms to incentivize honest behavior and the timely sharing of information were also made.

Both architectures were designed using modular and scalable components to ensure ease of integration with existing systems, and to allow for future expansion as technologies evolve. The implementation phase followed a structured approach based on Software Engineering guidelines, including:

- **Requirement Analysis**

The functional and non-functional requirements of both consumers and producers were gathered through a combination of interviews, surveys, and analysis of existing agri-food traceability systems. Key requirements included high availability, data security, and ease of use.

- **Platform Modeling**

Various modeling techniques were used to depict the system architecture, data flow, and interactions between components. Unified Modeling Language (UML) diagrams, such as class diagrams and sequence diagrams, helped visualize relationships and behaviors within the platform. This ensured a clear blueprint for the development phase, outlining how modules interact, how data moves across the system, and how users interface with core functionalities.

- **Modular Design**

A modular architecture was chosen to allow for flexibility and scalability. This enabled the system to integrate with various complementary technologies, such as Internet of Things (IoT) devices for real-time data collection and different databases for handling large datasets.

- **Prototyping and Iteration**

A prototype of the platform was developed and iteratively refined based on feedback from potential users. This iterative approach ensured that the final implementation was both functional and user-centric.

- **Testing and Evaluation**

Rigorous testing was conducted to assess the platform's performance under different conditions, including stress testing to evaluate its scalability and security testing to ensure the integrity and confidentiality of data. Feedback from industry stakeholders was also incorporated to validate the platform's applicability in real-world scenarios.

An Agile development methodology was followed, allowing for continuous feedback and iterative improvements to the platform. This approach facilitated the integration of new features based on user feedback during the development process.

The design and development of these innovative Blockchain architectures provide a practical solution to the challenges of traceability, transparency, and trust within the agri-food sector. By adhering to Software Engineering guidelines, the platforms ensure scalability, security, and usability, offering an effective tool for both consumers and producers in managing agri-food supply chains.

Chapter 4

State of the Art analysis

In the agri-food domain, Blockchain can modernize the way food is traced throughout the Supply Chain: by using this technology, each step of the food Supply Chain, from production to consumption, can be tracked and recorded to be trustable from the consumer point of view [52]. This allows for a more efficient food control and safety: producers can improve their visibility too.

Furthermore, Blockchain technology can also be used to create digital identities for food products, including information such as origin, production method, and certifications. This would allow consumers to make more informed decisions about the food they purchase and also allows for better tracking of sustainability and ethical production methods. Overall, Blockchain technology has the potential to significantly improve the transparency and the security of the agri-food supply chain, and to increase consumer trust in the food system.

Therefore, a comprehensive evaluation of Blockchain-based traceability systems is lacking in the literature, both in terms of technical implementation and advantages and disadvantages. To that end, this chapter presents a literature review to identify and assess the level of maturity in the use of Blockchain technology to improve agri-food. Six Research Questions (RQs) are proposed, that aim to explore the role of Blockchain technology in supporting agri-food Supply Chains, both from the consumers and stakeholders point of views. The analysis is based on 183 main papers, after a process of data gathering and filtering through the PRISMA workflow [50]. An analysis of industries involvement in the process of adopting a distributed architecture together with some security aspects is conducted, with some considerations on open challenges and future research directions. Section 4.1 describes some related work, Section 4.2 describes the adopted research methodology, and Section 4.3 analyzes results. Section 4.4 draws conclusions and lists open challenges in the analyzed topic.

4.1 Related work

Several literature reviews have explored the use of Blockchain in supply chain management. Zhao et al. present a review of studies on Blockchain applications in supply chains up to 2019, dividing the research into four primary categories: manufacturing, sustainable water management, traceability, and information security [53].

Niknejad et al. focus on the integration of Blockchain with smart agriculture, specifically addressing traceability and IoT sensors, expanding the scope beyond previous literature to explore Blockchain's role in agri-food systems [54]. The study aims to examine the involvement of various industries and assess whether the benefits of decentralized applications surpass their limitations.

Bhat et al. provide insights into the integration of Blockchain and IoT technologies within supply chain management, highlighting advantages such as food traceability, composition monitoring, and security enhancements throughout the supply chain [55]. The paper also addresses key cybersecurity challenges in Blockchain-based supply chains, particularly regarding consumer trust and IoT device vulnerabilities.

Dasaklis et al. conduct a systematic literature review on Blockchain-based supply chain traceability solutions, emphasizing the limited discussion of practical solutions, especially in terms of cost and implementation feasibility in the reviewed literature [56].

Bhatiadigitalization [57] offers a taxonomy and content analysis of Blockchain-based frameworks and adoption models for various stakeholders, while Agnusdei et al. focus on sustainable agri-food supply chains with less emphasis on Blockchain-specific issues [58].

Additional studies analyze the benefits of Blockchain in agri-food traceability, including counterfeiting prevention, decentralized organization, enhanced quality control, and product traceability [59], [60]. These works also explore practical use cases and security considerations. Other studies investigate the adoption of Blockchain technology across different countries and its applications in traceability, information systems, and agriculture, noting that Blockchain remains in its early stages of development [61], [62].

Agarwal et al. explore the adoption of Blockchain in supply chain management through a SWOT analysis, identifying key opportunities such as reducing anti-counterfeiting risks, enhancing trust, and gaining competitive advantage. The study also highlights challenges such as the lack of industry standards and interoperability issues [63].

This review diverges from the aforementioned studies by addressing not only product traceability within the supply chain but also the impact of Blockchain on agri-food, security concerns, and the application of technologies beyond Blockchain and IoT. Furthermore, the review considers the role of industries in adopting this

new paradigm, along with an analysis of its advantages and limitations. A comparison of these reviews is provided in Table 4.1.

Table 4.1: Comparison between the related work and the present review

Reference	Blockchain based	IoT and other technologies	Industries involvement	Security aspects
[53]	Yes	Yes	No	Privacy
[54]	Yes	No	Yes	No relevance
[55]	Yes	Yes	No relevance	Infrastructure
[56]	Yes	No	Use cases	No relevance
[57]	Yes	Yes	No relevance	No relevance
[58]	Less importance	No	Yes	Infrastructure
[59]	Yes	No	Use cases	Superficial
[60]	Yes	No	Yes	Infrastructure
[61]	Yes	Superficial	No	Infrastructure
[62]	Yes	No	Yes	Infrastructure and Privacy
[63]	Yes	No	Yes	Privacy
This review	Yes	Yes	Yes with in-depth analysis	Infrastructure and Privacy

4.2 Research Methodology - Literature Review

This research adopts the guidelines for conducting a Systematic Literature Review as outlined by Kitchenham et al. [64], focusing on relevant literature published between 2016 and 2022. The review assists in identifying and mapping areas related to Blockchain technology in the agri-food sector, as well as uncovering potential research gaps. The process for identifying relevant studies is illustrated in Figure 4.1.

4.2.1 Definition of Research Questions

The objective of this study is twofold: (a) to identify the state of the art in Blockchain technology and the smart agri-food domain, and (b) to provide a foundation for highlighting gaps, trends, and future research directions in this field. To achieve these goals, the following Research Questions (RQs) are formulated:

- **RQ1: What are the Blockchain trends in the agri-food sector from 2016 to 2022?**

This question aims to examine publication patterns, including the year, mode, and type, in order to understand the progression of the field.

- **RQ2: What research themes have been addressed in studies on Blockchain technology and agriculture?**

This question seeks to identify key areas of study in the field and their contributions to the scientific community.

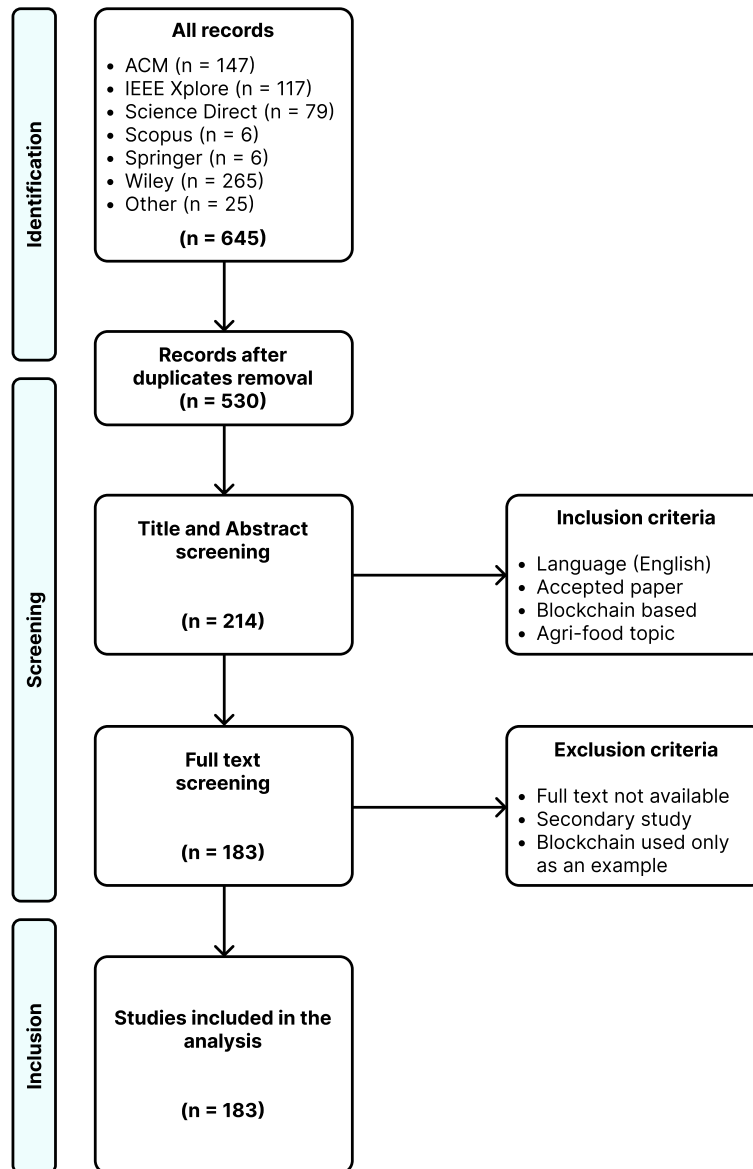


Figure 4.1: PRISMA search methodology

- **RQ3: What solutions can Blockchain provide to address stakeholder challenges across the agri-food chain?**

This question aims to explore the benefits of Blockchain in agri-food traceability on a large scale, with a particular focus on industry involvement.

- **RQ4: What information can stakeholders receive and integrate using Blockchain?**

This question aims to identify the types of product and technology information available for consumers and producers in product traceability.

- **RQ5: What are the current research gaps between the benefits of Blockchain technology and its limitations?**

This question aims to identify research gaps and trends, as well as examine existing open challenges.

- **RQ6: How is security addressed, and at what level?**

This question aims to assess the level of security provided, both in terms of implementation and infrastructure.

4.2.2 Paper Selection Strategy

Relevant databases were consulted to ensure that the information included in the review is comprehensive. A Population, Intervention, Comparison, and Outcome (PICO) framework was used to guide the search for keywords, categorized into two main groups:

- Population-related term: “agri-food”.
- Intervention-related terms: “Blockchain” and “traceability”.

The search string was constructed using binary logic:

“blockchain AND traceability AND (agri OR food OR agrifood)”.

This query returned 645 results from databases including ACM, IEEEExplore, ScienceDirect, Scopus, Springer, and Wiley, which was deemed sufficient for the scope of the investigation.

4.2.3 Inclusion and Exclusion Criteria

Once studies containing the search string’s keywords in their metadata (title, abstract, keywords) were identified, irrelevant studies were filtered out (i.e., studies that only superficially addressed the topic despite containing the relevant keywords). To enhance the reliability of the included studies, the following inclusion and exclusion criteria were applied:

Inclusion criteria:

- Studies published up to 2022.
- Studies written in English.
- Studies accepted for publication in conferences or journals.
- Studies focused on traceability in the agri-food supply chain.
- Studies that emphasize Blockchain methods and solutions.

Exclusion criteria:

- Studies with incomplete texts.
- Secondary or tertiary studies (e.g., surveys).
- Studies where Blockchain is not the primary focus, but used as an example.

After applying the screening procedure, 183 studies were included in the analysis¹. The extracted data was classified to answer the formulated Research Questions. The data extraction form is shown in Table 4.2.

Table 4.2: Research questions and their corresponding value

Data	Value	RQ
Publication year	2016 to 2022	RQ1
Search type	Method of analysis	RQ1
Research area	Type of study	RQ2
Focus	Software or knowledge-based	RQ2
Solution target	Approach to problem-solving	RQ3
Industry involvement	Involvement of industries	RQ3
Product information	Product aspects covered	RQ4
Other technologies	Use of additional technologies	RQ4
Benefit-boundary gap	Comparison of benefits and limitations	RQ5
Security focus	Level of security analysis	RQ6

¹A replication package is available at https://politecnicobari-my.sharepoint.com/:f:/g/personal/marco_fiore_poliba_it/Eimw3a8vD5lHsBgD39p-xEABYpmVV--Pe7WgpeQeN9evMQ?e=pe2ZyM

4.3 Results and discussion

This section presents the results of the literature review to answer the six Research Questions proposed above.

4.3.1 RQ1: What are the Blockchain trend issues in the agri-food sector from 2016 to 2022?

The analysis of Figure 4.2 shows an increasing number of papers during the years. Studies on the topic of Blockchain applied to agri-food increased over time and are expected to constantly grow. There is a slight decrease between 2020 and 2021, which can be attributed to the pandemic situation that shifted research perspectives. Practical approaches began to spread in 2022, emphasizing the importance of finding new ways to meet the increasing food demand due to the growing world population [65].

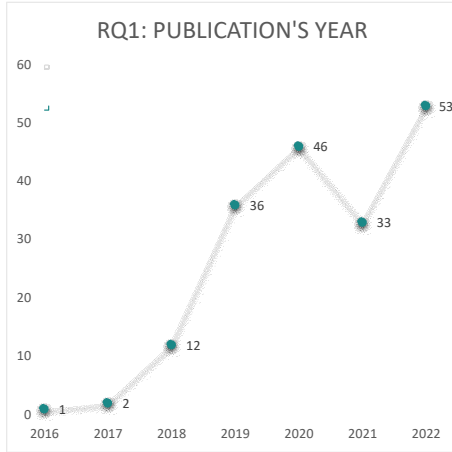


Figure 4.2: Distribution by pub year

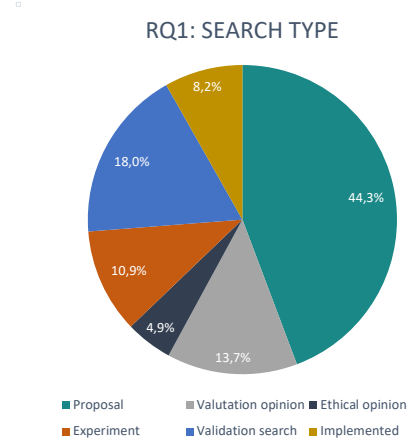


Figure 4.3: Distribution by search type

Figure 4.3 distinguishes between different search types: 43.8% of the analyzed papers are proposals, offering innovative solutions with systems that are not fully validated or implemented. Implementations cover 8.2% of the analyzed papers, indicating that producers are hesitant to adopt Blockchain systems, largely due to its immaturity. Other categories include 14.1% evaluative opinions, 17.8% validation research, and 10.8% experiments, reflecting the ongoing nature of practical evaluations. Ethical and philosophical discussions account for 4.9%, highlighting Blockchain as not just a technological innovation but also a transformative way of thinking.

4.3.2 RQ2: What research themes have been addressed in previous studies on Blockchain technology and agriculture?

Figure 4.4 presents the different research areas covered: 75 papers focus on technology, 38 on architecture, and 23 on performance. Since Blockchain is still a developing technology, researchers continue to explore new approaches to enhance its performance. Other areas include reliability (17 papers), business analysis (14), quality (8), bibliometrics (5), and philosophy (3), with transparency and data immutability recognized as crucial aspects for the adoption of Blockchain.

Figure 4.5 shows the distribution between software-based and knowledge-based publications. The two categories are nearly balanced, with 89 software-based and 94 knowledge-based papers, indicating that research into Blockchain’s architectural network and algorithms is progressing alongside software development and technological advancements.

Blockchain traceability solutions are being explored by companies and real-world scenarios, but as noted in [56], delivering commercial value is challenging due to factors such as Blockchain’s infancy, the diffusion of advanced traceability technologies, scalability issues, and the gap between platform research and real-world testing.

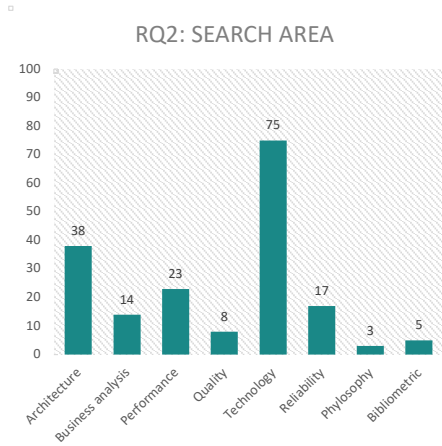


Figure 4.4: Distribution by search area



Figure 4.5: Distribution by papers base

4.3.3 RQ3: What solutions may Blockchain build to simplify the problems of stakeholders across the full agri-food chain?

Figure 4.6 shows that 62.3% of the proposed papers focus on product identification at various stages of the Supply Chain, system implementation, and traceability

aspects. Blockchain can identify products, track them through production and distribution, and manage the Supply Chain to ensure transparency and trust. Interoperability is a less-explored topic, with only 6% of papers addressing it, as integrating Blockchain into existing systems often requires significant architectural changes.

As shown in Figure 4.7, 138 papers reported no industry involvement. This lack of industry engagement is a key factor in the slow adoption of Blockchain as a traceability tool in agri-food. The success of Blockchain solutions requires the proactive participation of industries, which should lead the adoption of these technologies to improve product quality and supply chain efficiency.

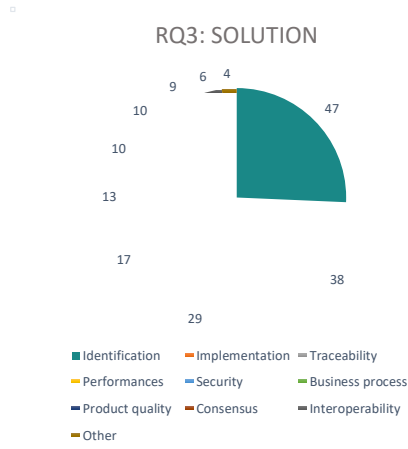


Figure 4.6: Distribution by solution

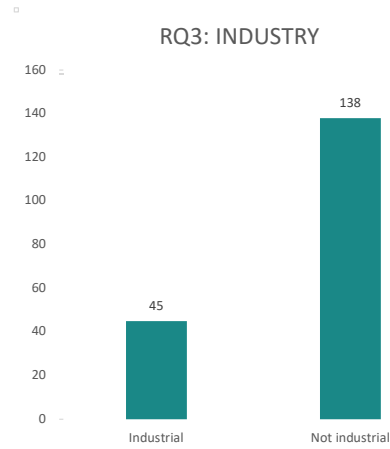


Figure 4.7: Industry involvement

4.3.4 RQ4: What kind of information could stakeholders receive and integrate using Blockchain?

The analysis of Figure 4.8 reveals that traceability information in the agri-food sector is largely focused on product origin, such as transport, storage, place of production, and processing. This information helps optimize logistical aspects. Quality-related papers focus on certifications like Hazard Analysis and Critical Control Points (HACCP), which help reduce counterfeiting and ensure the safety of products and production lines.

Figure 4.9 shows a growing use of IoT devices alongside Blockchain technology. IoT sensors are primarily employed for tracking environmental conditions like humidity and temperature during transportation and storage. Edge computing and data mining techniques are also increasingly used to optimize and secure interactions with consumers.

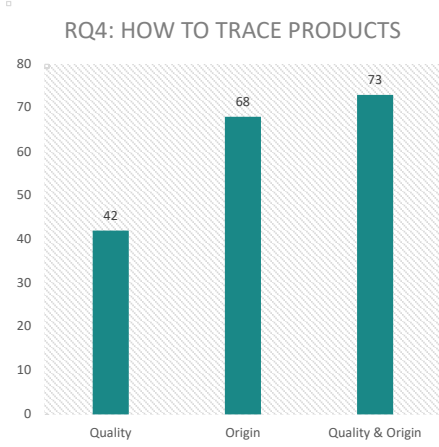


Figure 4.8: Traceability information proposed in papers

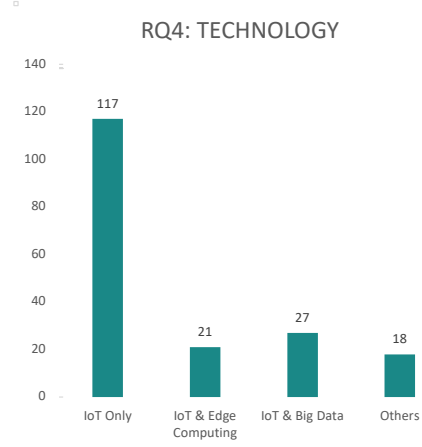


Figure 4.9: Technologies used in selected papers

4.3.5 RQ5: What are the present research gaps between the benefits of Blockchain technology and its limitations?

The literature highlights several benefits of Blockchain for the Supply Chain, such as the ability to trace products from cultivation to retail, identify defective batches quickly, and streamline information collection and storage [66]. However, several research gaps and limitations persist, including:

- Difficulty in scaling Blockchain for larger systems.
- Lack of industry-wide adoption due to the perceived risk and cost.
- Limited tools for developers to understand and implement Blockchain solutions.
- Insufficient integration with existing Supply Chain technologies.
- Initial financial investments required for adoption.

As noted in [67], stakeholders' willingness to adopt new technology is subjective and may slow down the transition to Blockchain-based systems. The lack of simple, user-friendly tools for implementing Blockchain also widens the gap between established businesses and start-ups, as the latter are often more agile in adopting Industry 4.0 technologies [68].

4.3.6 RQ6: Is the matter of security addressed, and if so, at what level?

As shown in Figure 4.10, security is a key concern in Blockchain research. 94 of the 185 papers address security, either in terms of infrastructure or traceability.

Blockchain’s distributed architecture offers enhanced security and fraud prevention for Supply Chains. The use of IoT devices further bolsters security by ensuring real-time data collection and tamper-resistant records.

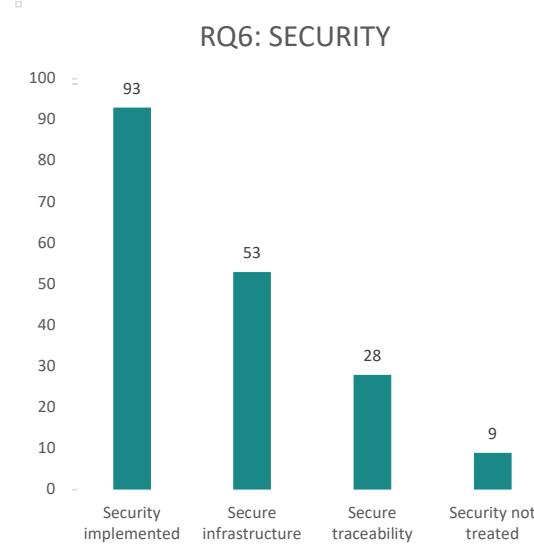


Figure 4.10: Distribution by treatment of security topic

4.4 Open challenges

This review evaluates the application of Blockchain technology to agri-food traceability, analyzing 183 out of an initial 645 references. These studies collectively form a robust foundation for assessing the state of the art in this field, highlighting both the technological advancements and the challenges that lie ahead.

From the analysis, it is evident that interest in Blockchain for agri-food supply chains began to gain momentum around 2018, with a shift in research focus from theoretical proposals to validations and practical implementations. Blockchain technology has been identified as a critical tool for enhancing transparency, trust, and traceability across supply chains. While more than half of the studies focus on the technological aspects of Blockchain, 60% of the reviewed literature emphasizes its potential to improve traceability in agri-food sectors.

However, despite these promising findings, the slow adoption of Blockchain in industrial applications highlights significant gaps, particularly in terms of industry involvement. The COVID-19 pandemic may have further delayed the technology’s promotion and adoption. Nevertheless, the use of Blockchain in agri-food supply chains presents numerous benefits. These include enhanced brand identity, improved sales for companies, and greater transparency for consumers, who can

verify the quality and origin of their products through QR codes and other means.

Several open challenges must be addressed to accelerate the widespread adoption of Blockchain in the agri-food sector. These challenges highlight the areas where future research and development efforts should be concentrated:

1. **Stakeholder Training and Awareness:** A lack of training for industries and stakeholders remains one of the major hurdles. Researchers should develop new approaches to educate stakeholders about Blockchain's characteristics and its applicability to agri-food supply chains. Practical training programs and guidelines are essential to ensure that stakeholders can grasp the technology's advantages and successfully implement it.
2. **Integration with Emerging Technologies:** To overcome the limitations of current Blockchain platforms, such as bandwidth and throughput constraints, future research should focus on the integration of Blockchain with complementary technologies like Big Data, Edge Computing, and IoT. These technologies can provide the scalability and reliability required for large-scale adoption, while also addressing the challenges of data management and system performance in distributed environments.
3. **Supporting Tools for Developers:** The absence of robust developer tools is another barrier to Blockchain adoption. There is a need for user-friendly tools and frameworks that can help developers differentiate between available Blockchain platforms and choose the most suitable one for their specific use cases. Such tools should provide guidance on technical compatibility, scalability, and cost-effectiveness, making it easier for developers to build and implement Blockchain-based solutions.
4. **Scalability and Standardization:** One of the key technical challenges that future research must address is the scalability of Blockchain systems, particularly for large and complex supply chains. In addition, interoperability between Blockchain platforms and existing systems remains a critical area for exploration. A standardized regulatory framework is crucial for fostering the adoption of Blockchain in agri-food supply chains.
5. **Incentivizing Industry Involvement:** Finally, future research should explore strategies to incentivize greater industry participation. Blockchain adoption can be driven by demonstrating tangible benefits to key stakeholders, including cost savings, improved operational efficiency, and enhanced consumer trust.

By addressing these open challenges, Blockchain technology can realize its full potential as a transformative tool for agri-food traceability, offering enhanced transparency, accountability, and efficiency across the global supply chain.

Chapter 5

Blockchain for Agri-food Traceability

The inner characteristics of Blockchain technology allow systems to be transparent and trustable. Traceability is easily achievable due to the immutability of data stored in a Blockchain. Traceability refers to the ability to reproduce the history of products from production to distribution [69]. By ensuring traceability, it becomes possible to identify the responsibilities of each actor involved in a supply chain, thereby fostering consumer trust in terms of food quality and safety. However, given the length and complexity of many supply chains, tracking products from raw materials to end consumers can be costly [70]. Consequently, a scalable and efficient system is required, which must also be reliable to maintain consumer trust [71]. Blockchain technology addresses these challenges with its intrinsic properties: (i) it is a distributed system, eliminating dependence on a single server that could be a point of failure, (ii) it offers data immutability, making it straightforward to track information and resistant to tampering, and (iii) it can be deployed as either a public or private ledger [72] [73], allowing it to adapt to specific use cases while still ensuring transparency and fraud prevention.

A common architecture that summarizes various approaches to agri-food traceability using Blockchain technology is illustrated in Figure 5.1. Most proposed architectures involve two key actors: the end consumer and the producer, which can be further extended to include the farmer, distributor, and retailer. Each actor functions as a node within the distributed system. The end consumer can access all immutable traceability information via their device, typically through a QR code or RFID tag [74]. The producer, in turn, inputs new data, which is managed by predefined smart contracts. These smart contracts are responsible for ensuring the accuracy of the data being added to the Blockchain. Additionally, data may be sourced from IoT sensors following a data-gathering process facilitated by a central unit. All transactions are recorded on the Blockchain and can subsequently be uploaded to the InterPlanetary File System (IPFS) [75].

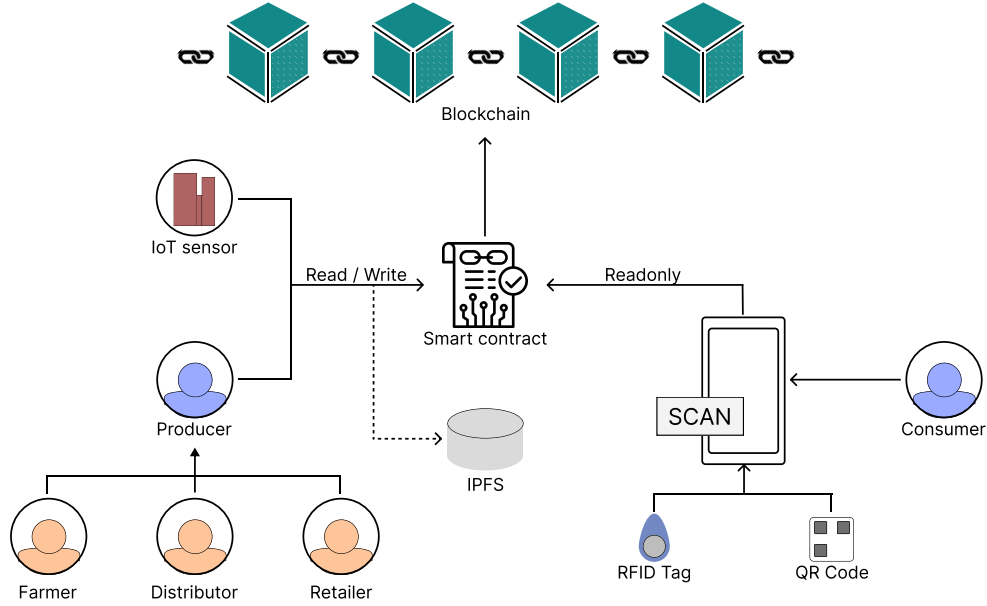


Figure 5.1: An architecture incorporating components presented in different works

This chapter explores the development of new platforms, based on the Software Engineering guidelines (e.g., requirements definition, UML diagrams, agile development), to connect producers and consumers in a Blockchain-based environment. An analysis of transparency and accountability enhancement is proposed in Section 5.1, while consumers perception of Blockchain-based platforms is described in Section 5.2.

5.1 Transparency and Accountability enhancement

Traceability is a handy tool for consumers seeking as much information as possible about a certain product. Businesses, on the other hand, consider traceability as a strategic marketing tool since it allows them to guarantee the quality of their products to clients in a transparent manner. The capacity to quickly obtain all information on an agri-food product is crucial for customer trust. Products' information can include where they were created, where they came from, how they arrived at the shelter, and so on. Transparency and accountability can be enhanced by using Blockchain technology: this is the main goal of the Tracecoop project. The aim of the proposed project is to apply the Blockchain system to the agri-food sector, with the ultimate goal of creating a platform for products traceability. The platform is based on the use of appropriate devices (smartphones, tablets, etc.) and must allow the general user (consumer, producer, etc.), at any time, to verify the origin and the product information, as well as the chemical-physical characteristics, the organoleptic properties of the product, and the varietal origin. It must also

guarantee to control and monitor the agri-food chain of the product itself thanks to the possibility of accessing information relating to the production phases, from sowing to sale, including all stages of any transformation. Specifically, the project proposal intends to experiment with the integration of Blockchain technology and therefore the real-time traceability of the information recorded on the history of the product, in order to guarantee the various stakeholders, from the agronomist to the final consumer, the certification of product safety to prevent scams and malicious events. The architecture of the system proposed in the project is shown in Fig. 5.2. It is composed of four main components: the front-end application for both the consumer and the producer, the private Blockchain for sensors, and the back-end application.

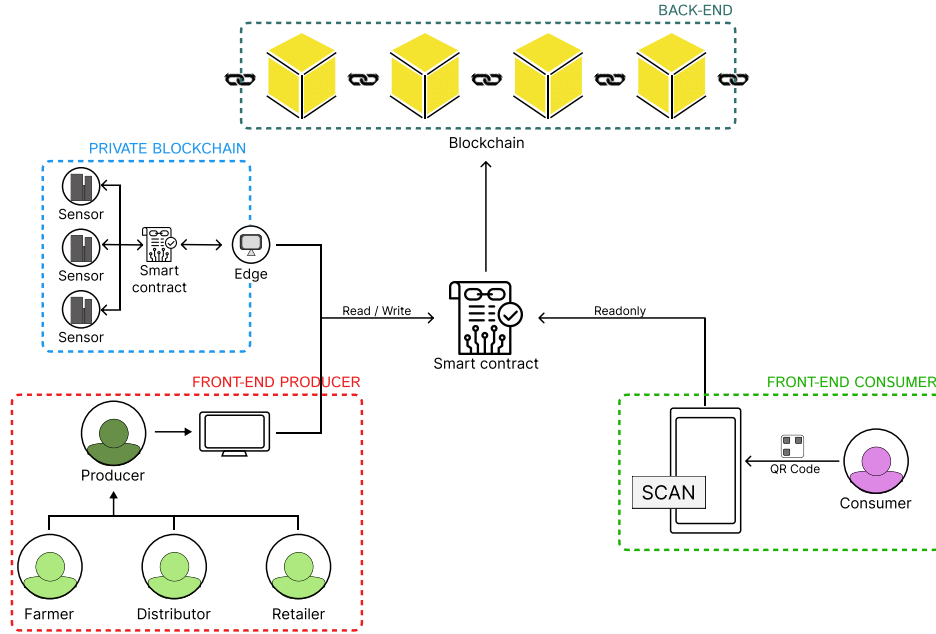


Figure 5.2: Architecture of the proposed system

- *Front-end for the consumer.* The front-end component is a web-based application. This app allows the consumer to scan a QR code placed on the product's label to access the back-end and read information about the chosen product. The main goal is to ensure that the information displayed on the platform is secure and transparent.
- *Front-end for the producer.* The front-end component for the producer enables various actors (i.e., the farmer, the distributor, the retailer) to add information not collected by IoT sensors. This functionality allows producers to establish a trust relationship with consumers: the more a consumer trusts a producer, the more likely they are to purchase that producer's products.

- *Private back-end.* Data from IoT sensors are not directly inserted into the main back-end; instead, they are gathered in a private local back-end responsible for the collection and conversion of information into value. An edge computing unit reads the information from the sensors and, after a defined period, extracts valuable insights and uploads them to the main back-end.
- *Back-end.* This component is responsible for storing information about agri-food products in a secure and immutable manner. Data stored in this component are accessible (with read-only permission) to customers who scan the QR code on the product's label.

The proposed architecture is the result of evaluating several relevant issues:

- The system must be available 24/7, as it will be used at various times throughout the day.
- Sensor data are constantly generated, so the system must support large volumes of information.
- The system must be scalable and optimized for different types of products, not just the test items.
- There should be the capability to add new functions without requiring downtime for the platform.

To satisfy the requirements described above, a Blockchain-based architecture was chosen. Blockchain technology makes the history of any digital asset unalterable and transparent through decentralization and cryptographic hashing. A Blockchain is a distributed database shared among network nodes, storing information electronically in digital representation. Blockchains are best known for their critical role in cryptocurrency systems like Bitcoin, where they maintain a secure and decentralized record of transactions. The innovation of Blockchain lies in its ability to ensure the integrity and security of a data record, fostering trust without the necessity for a trusted third party.

A typical scenario consists in a field composed by an agri-food product (i.e., pomegranates); IoT sensors gather both field and meteorological information and upload them into Hyperledger Fabric. An edge computing unit is responsible of converting this huge amount of data into valuable information, then it uploads the output of the processing to Ethereum using the available smart contract. Producers also upload some information about that product (i.e., where it is distributed, how it is transported from the field to the reseller). A consumer, looking at the pomegranate in a supermarket, decides to know more about that product. He opens the web-app and scans the QR code that he finds on the product label. He then access all relevant information about that lot of pomegranates, knowing the amount

of spared water, what chemical products have been used during cultivation, and when and where the product has been cultivated and transported. The scenario is shown in a UML sequence diagram in Fig. 5.3.

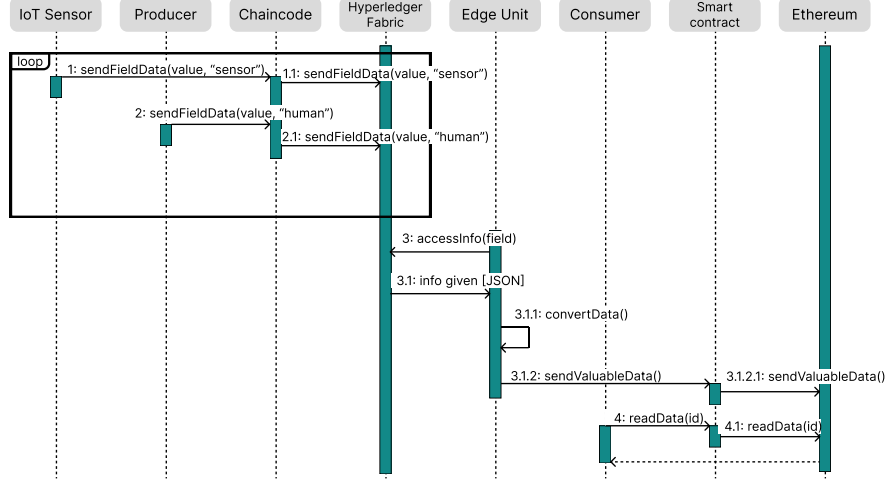


Figure 5.3: Sequence diagram showing a common scenario of the Tracecoop project

5.2 Consumers perception

Consumers side, the project aims to understand if users tend to trust producers more if Blockchain is used in a traceability platform. To do so, a choice experiment is conducted, together with an econometric data analysis.

The econometric data analysis was conducted using Nlogit software (version 5.0)¹, based on Lancaster utility theory. It was assumed that the consumer, by choosing between two products, A or B, would select the one with greater utility. Therefore, the choice of the product is influenced by its attributes and the preferences that distinguish consumers.

The utility function is described by a deterministic component (V), a function of observable attributes, and a stochastic component (ϵ) that represents measurement errors along with all unobservable attributes influencing the purchase choice. Thus, the utility function is determined as follows:

$$U_{nj} = V_{nj} + \epsilon_{nj} \quad (5.1)$$

where V_{nj} can be expressed by:

$$V_{nj} = \beta' x_{nj} = \alpha + \beta_1 x_{1n} + \beta_2 x_{2n} + \dots + \beta_m x_{mn} + \epsilon_{nj} \quad (5.2)$$

¹<https://www.limdep.com/products/nlogit/>

Here, x_{nj} indicates the attribute x of the alternative j selected by individual n , with the coefficients β' , whereby β_n represents the weight of the preference for each level of the attribute, while the coefficient α incorporates the heterogeneity of the sample of consumers/respondents.

The estimation of Willingness-to-Pay (WTP) reflects how much extra consumers were willing to pay as a price premium for a product based on Blockchain technology with a specific characteristic. The following formula was used for this estimation:

$$WTP_a = -\frac{\beta_a}{\beta_p} \quad (5.3)$$

where WTP_a is the willingness-to-pay for attribute a ; β_a and β_p are the estimated coefficients related to each attribute and price, respectively.

An online survey was conducted, lasting about four months (June - September 2022), which reached 327 valid respondents. Six attributes were considered, with their levels of variation within the choice experiment (CE) approach assigned as follows: (i) Attribute 1: BC technology and attached QR code (with 2 levels: absent, present); (ii) Attribute 2: Information on environmental sustainability (with 3 levels: absent, partial, complete); (iii) Attribute 3: Information on social sustainability (with 3 levels: absent, partial, complete); (iv) Attribute 4: Information on the quality and healthiness of the selected products (with 3 levels: absent, partial, complete); (v) Attribute 5: Information on business innovation (with 3 levels: absent, partial, complete); (vi) Attribute 6: Price (with 4 levels: about half of the average market price, average market price rounded, 2 times the average market price, 3 times the average market price). Concerning the levels, “absent” indicates that only the mandatory information is included on the label for consumer access. The “partial level” indicates that the consumer is informed that the agri-food product is sustainable, but no details are provided on the activities that make it sustainable. The “complete level” indicates that the consumer is informed that the agri-food product is sustainable, with detailed information available on the activities that allow the product to be classified as environmentally friendly.

5.2.1 Econometrics Results and Discussion

The multinomial logit model (MNL) analysis revealed that all estimated attributes were significant, and the alternative specific constant (ASC) for the opt-out option was negative and significant, indicating overall acceptance of the products included in the analysis. As expected, the price attribute had a negative coefficient, indicating that consumers were negatively influenced by price increases. All other attributes had positive and significant coefficients, indicating a positive influence on purchase decisions. Table 5.1 shows these results.

Furthermore, the attributes showed slight differences, indicating that consumers have varying preferences for different attributes. Overall, the highest WTP (€1.25)

was for the "Quality and Healthiness" attribute. This was significantly higher than the WTP for "Social Sustainability Information" (€0.59), "Environmental Sustainability Information" (€0.35), and "Business Innovation" (€0.31). The presence of Blockchain technology resulted in a WTP of €0.52 (Fig. 5.4). Results align with findings from other studies that highlight the potential of Blockchain technology in communicating credence attributes and empowering consumers [76].

Table 5.1: MNL coefficients estimate

Variable	Coefficient		Standard Error	z	Prob. z >Z*	95% Confidence Interval	
Price	-0.24196	***	0.01293	-18.71	0	-0.26731	-0.21661
BC Technology	0.1265	**	0.05425	2.33	0.0197	0.02018	0.23283
Environmental Sustainability	0.08398	***	0.02233	3.76	0.0002	0.04021	0.12775
Social Sustainability	0.14191	***	0.02115	6.71	0	0.10046	0.18336
Quality and Healthiness	0.30143	***	0.02311	13.04	0	0.25613	0.34674
Business Innovation	0.07462	***	0.01978	3.77	0.0002	0.03586	0.11338
ASC Opt-out	-1.04329	***	0.07546	-13.83	0	-1.19118	-0.8954

Note: ***, **, * ==> Significance at 1%, 5%, 10% level.

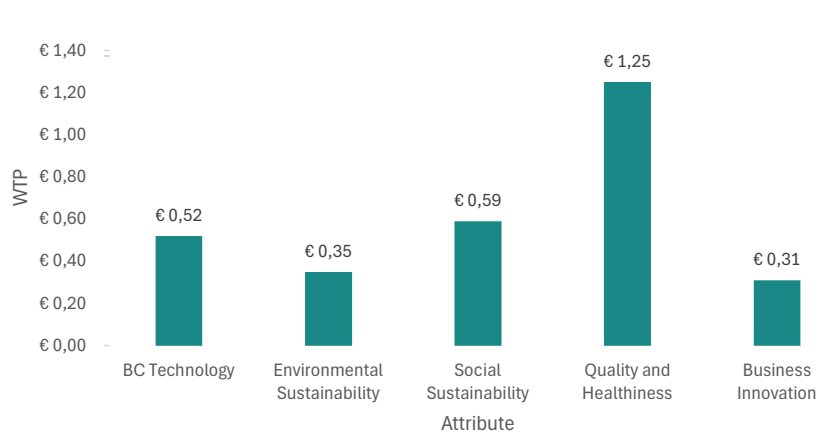


Figure 5.4: WTP estimate for the attributes

This study has practical implications and seeks to support Apulian (southern Italy) cooperatives or producers in implementing appropriate and efficient promotional and marketing diversification strategies, as well as determining the premium price of selected products. Additionally, it has public information implications in terms of supporting and urging the implementation of information labels (like QR codes) on product labels to influence consumption behavior and raise social awareness. Consequently, another added-value purpose of the present paper is to enrich the scientific literature on the choice modeling of sustainable agri-food consumers' perceptions. Possible developments of the study include differentiating the results for each product and segmenting the market using models that capture discontinuities in people's choices, such as latent class models.

The implemented system reflects the proposed requirements, to the ease of use for both producers and consumers, to the automatization of all aspects of the analyzed supply chain. The econometric data analysis shows a great interest from consumers in the traceability system. Moreover, this kind of research is relatively new in the agri-food market and could be relevant for companies interested in differentiating their products with this type of tracking, and, consequently, might represent an incentive for consumers to seek more information about it.

Chapter 6

Blockchain and Cryptography

The challenge of security and privacy has been analyzed in the context of Blockchain technology, focusing on the implications of quantum computing and the development of post-quantum cryptography. Quantum computing represents a transformative advancement in computational power, enabling the resolution of complex mathematical problems far beyond the capabilities of classical computers. However, this capability also poses significant risks to cryptographic algorithms, including those foundational to Blockchain platforms. The immutability and integrity of Blockchain, which are critical for applications in sensitive domains such as the agri-food sector, could be compromised without proactive measures.

To address these risks, this chapter examines the intersection of Blockchain and quantum computing. Section 6.1 provides an introduction to quantum cryptography, offering essential context for understanding the vulnerabilities of current cryptographic systems. Section 6.2 presents a state-of-the-art analysis, identifying key challenges and research gaps. Building on these insights, quantum-resistant solutions are proposed, including quantum-safe encryption algorithms in Section 6.3 and quantum-safe signatures in Section 6.4. Additionally, Section 6.5 explores secure biometric key-pair generation as an innovative approach to enhancing Blockchain security.

6.1 Quantum Computing

Quantum computing represents a significant paradigm shift from classical computing, leveraging the principles of quantum mechanics to solve complex computational problems more efficiently. At its core, the qubit (quantum bit) serves as the fundamental unit of quantum information, analogous to the classical bit. However, unlike classical bits, which can only exist in one of two discrete states (0 or 1), qubits exhibit the property of superposition, allowing them to exist simultaneously in a combination of both states.

6.1.1 Qubits, Superposition, and Entanglement

Each quantum state can be expressed as a vector in a Hilbert space, denoted by the Dirac notation $|\psi\rangle$. A general qubit state can be represented as a linear combination of the basis states $|0\rangle$ and $|1\rangle$, as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \{\alpha, \beta \in \mathbb{C}\} \quad (6.1)$$

where α and β are complex numbers representing the probability amplitudes of the qubit being in the states $|0\rangle$ and $|1\rangle$, respectively. The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ ensures that the probabilities sum to 1, highlighting the probabilistic nature of quantum measurements. In superposition, a qubit can represent both 0 and 1 simultaneously, making quantum computers capable of parallelism that vastly increases their computational power in specific applications.

Another important feature of qubits is entanglement, a phenomenon in which two or more qubits become linked in such a way that the state of one qubit directly influences the state of the other, regardless of the distance separating them. This "spooky action at a distance," as described by Einstein, is a hallmark of quantum mechanics and forms the foundation for advanced quantum algorithms and protocols.

6.1.2 Quantum States Representation: The Bloch Sphere

The state of a qubit can be visually represented using the Bloch sphere, a geometric model that maps quantum states to points on the surface of a sphere. The north and south poles of the Bloch sphere correspond to the classical states $|0\rangle$ and $|1\rangle$, respectively, while any point on the surface represents a possible superposition of these states. A general qubit state in spherical coordinates is given by:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (6.2)$$

Here, θ and ϕ define the position of the qubit on the Bloch sphere. Quantum gates, which perform operations on qubits, can be viewed as rotations on the Bloch sphere. This model helps to understand concepts such as decoherence, where the quantum state moves toward the center of the sphere, indicating a loss of quantum coherence.

6.1.3 Post-Quantum Cryptography

As quantum computing advances, concerns arise about its impact on cryptographic systems. Classical cryptographic algorithms, particularly those based on the difficulty of factoring large integers or computing discrete logarithms, are vulnerable

to quantum attacks. Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against classical and quantum adversaries.

Shor's and Grover's algorithms are two quantum algorithms that directly challenge current cryptographic security. Shor's algorithm allows quantum computers to factorize large integers exponentially faster than classical algorithms, posing a threat to widely used public-key cryptosystems such as RSA and ECC (Elliptic Curve Cryptography). On the other hand, Grover's algorithm offers a quadratic speedup for unstructured search problems, undermining the security of symmetric cryptographic systems by effectively halving the security strength of keys. Grover's quantum algorithm [77], formulated by Lov K. Grover in 1996, allows a search within an unstructured, unordered database with a polynomial computational complexity equal to:

$$O(\sqrt{n}) \quad (6.3)$$

Basically, by receiving as input a cryptographic hash value (e.g., digital signature) and the cryptographic hash function with which it was generated, the Grover algorithm can decrypt the data in a quadratically smaller number of attempts. Consequently, this acceleration leads to halving the security level of several security algorithms [78]. Table 6.1 shows a comparison between encryption algorithms security levels, in bit.

Table 6.1: Comparative table of encryption algorithms security levels

Encryption algorithm	Security level in bit (current)	Security level in bit (post-quantum)
SHA-256	256	128
SHA-3 256	256	128
Keccak-256	256	128
Keccak-384	384	192
Keccak-512	512	256
RIPEMD 160	160	80
AES-128	128	64
AES-256	256	128

6.1.4 Applications to Blockchain Technology

Quantum computing's potential to break classical cryptographic schemes extends to Blockchain technology, which relies heavily on cryptographic primitives for its security and integrity. A Blockchain system typically employs three cryptographic components: i) key-pair generation for user authentication, ii) transaction signatures for verifying the legitimacy of transactions, and iii) block hashes for linking blocks securely within the chain.

Quantum attacks, particularly those leveraging Shor's algorithm, could break public-key cryptography, allowing attackers to derive private keys from public keys. This compromises the integrity of transaction signatures (ii) and key-pair generation (i). However, the threat to block hashes (iii) is less severe because an individual

attacker could only manipulate their own local Blockchain, which would be rejected by the consensus of other nodes in the network.

The development of quantum-safe Blockchain systems focuses on integrating post-quantum cryptographic algorithms that resist quantum attacks. Quantum-safe key-pair generation and signature schemes ensure the continued security and reliability of Blockchain-based platforms in the quantum era, ensuring a smooth transition as quantum technologies mature.

6.2 Related Work

The advent of quantum computing poses a significant threat to the security of Blockchain systems. In response, several platforms are exploring post-quantum algorithms to counteract this risk. Bitcoin Post-Quantum¹ is an experimental extension of Bitcoin's primary Blockchain, incorporating quantum-safe digital signatures. This initiative aims to pave the way for the eventual implementation of quantum-safe cryptographic methods in Bitcoin's main network. Ethereum 3.0² intends to integrate quantum-resistant features such as zk-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge). Zk-STARKs are highly secure cryptographic proofs that leverage Zero Knowledge Proof principles to verify encrypted data without disclosing the underlying information and are inherently resistant to quantum computing, thus safeguarding its future security. Additionally, Abelian³, a Blockchain consulting and development firm, suggests employing lattice-based post-quantum cryptographic techniques to decrease operational costs. Finally, Corda⁴, a scalable permissioned peer-to-peer distributed ledger platform, is investigating post-quantum cryptographic methods such as SPHINCS.

In 2018, the authors in [79] introduced the concept of the post-quantum Blockchain and developed a secure cryptocurrency protocol capable of withstanding quantum computing threats. They employed the lattice basis delegation algorithm to derive secret keys by picking a random value and used the preimage sampling algorithm for message signing. The security of this approach is linked to solving the short lattice integer solution problem. Concurrently, [80] suggested a potential approach to addressing the quantum-era Blockchain challenge, demonstrated through an experimental implementation of a quantum-secure Blockchain platform incorporating quantum key distribution. Their findings indicate that quantum-secure Blockchains are both feasible and scalable for use in commercial and governmental settings.

¹<https://bitcoinpq.org/>.

²<https://ethereum.org/es/zero-knowledge-proofs/>.

³<https://abelian.tech/>.

⁴<https://corda.net/>.

In 2020, [81] conducted a study on the latest advancements in post-quantum cryptosystems and examined their application within Blockchain technologies. They also analyzed and compared the key features and performance of leading post-quantum Blockchain systems with a particular focus on the most promising post-quantum public-key encryption and digital signature schemes. Their findings highlighted the absence of post-quantum Blockchain algorithms that simultaneously offer compact key sizes, brief signature/hash dimensions, and rapid execution. Later that year, [82] pointed out that Blockchain does not significantly differ from other secure platforms concerning resistance to quantum attacks. They also emphasized the importance of planning a gradual transition by integrating existing initiatives and solutions like Quantum Key Distribution and post-quantum cryptography, as well as developing authentic quantum cryptographic mechanisms for encryption and digital signatures.

In 2021, researchers [83] aimed to identify and address quantum threats within Blockchain networks. They crafted and implemented a layer-two solution to protect the exchange of data between Blockchain nodes over the internet and introduced a secondary signature in transactions using post-quantum cryptographic keys. This solution was applied on the LACChain Besu Blockchain network. Additionally, another project⁵ involved deploying and setting up smart contracts for permissions on a Blockchain safe from post-quantum threats. Specifically, they carried out the implementation of a Falcon-512⁶ verification precompiled contract on the Hyperledger Besu network, with nodes operating on the LACChain.

In the past year, [84] conducted an updated survey on post-quantum digital signatures with unique advanced capabilities. Their research examined cryptographic signatures essential for Blockchain activities, including account management, consensus processes, enabling scriptless functionalities, and preserving privacy. Specifically, their analysis concentrated on multi-/aggregate, threshold, adaptor, blind, and ring signatures. Furthermore, the authors in [85] introduced a new method for handling cryptographic components within smart-contract-based ledgers. They utilized smart contracts directly on the ledger to manage these cryptographic protocols, allowing for rapid alteration of algorithms and parameters. The advantage of this method is its facilitation of adaptable post-quantum-based Blockchain designs. Generally, implementing new features or updates in a Blockchain can lead to forks, potentially causing significant issues. By employing smart contracts for Blockchain management, they can circumvent this problem, enabling the seamless introduction of new protocols or discontinuation of outdated ones without affecting existing data.

⁵<https://github.com/lacchain/pq-permissioning-setup>

⁶<https://falcon-sign.info/>.

6.3 Quantum safe algorithms in a Blockchain

Nowadays, computer security is based on the inability of processors to perform certain calculations in an acceptable amount of time. This inability is exploited by cryptographic functions that allow data to be encrypted with functions that cannot be reversed.

The functions that ensure the difficult exploits for traditional computers regard factoring integers into primes and solving a discrete logarithm, often implemented in elliptic curve cryptography. With the advent of quantum computers, it is possible to perform these calculations in reduced time through the Shor and Grover algorithms.

A survey has been conducted among NIST researchers regarding the likelihood of the development of a quantum computer that is powerful enough to break the RSA-2048 algorithm in just 24 hours, along with the presumed development time of the algorithm[86].

To quantify on a temporal level the impact that quantum computing will have in cryptography, it is possible to observe the inequality formulated by the deputy director of the Institute for Quantum Computing at the University of Waterloo Michele Mosca in 1999, known in the form:

$$D + T > Q_c \quad (6.4)$$

Where D presents the amount of time it takes for encryption to be considered secure, T the time it takes for infrastructure to be adapted by quantum-safe solutions, and Q_c the time it takes for quantum processors to reach a scale where they can breach existing encryption protocols.

From the standardization point of view, NIST launched a process in 2016 to standardize post-quantum cryptography algorithms [87]. Between 2022 and 2024, the standardization of the finalist algorithms is planned, proposing possible alternatives.

It is possible to group the candidate algorithms to be standardized as quantum-resistant cryptographic algorithms by NIST into two categories, shown in Table 6.2.

The categories shown above are explained as follows [88].

- Hash-Based

Using a cryptographic hash function the input message is converted into a sequence of bytes called “message digest”.

- Code-Based

Cryptosystem that inserts an error in the message to be transmitted and then corrects it through a corrective encoding on reception.

Table 6.2: Post-quantum cryptographic algorithms chosen by NIST in Round 3

	Category	Finalists	Alternatives
Public key algorithms	Hash-based	-	-
	Code-based	Classic McEliece	BIKE, HQC
	Lattice-based	CRYSTALS-KYBER, NTRU, SABER	FrodoKEM, NTRU Prime
	Isogeny-based	-	SIKE
	MPKC	-	-
Digital signature algorithms	Hash-Based	-	Picnic, SPHINCS+
	Code-Based	-	-
	Lattice-Based	CRYSTALS-DILITHIUM, FALCON	-
	Isogeny-Based	-	-
	MPKC	Rainbow	GeMSS

- Lattice-Based

Cryptography is performed through computational proofs that require solving problems using multidimensional algebraic constructs called "lattices".

- Isogeny-Based

The message is encrypted by establishing a secret key between the nodes present in the communication channel. This encryption is based on the pseudo-random crossing of a graph called "supersingular isogeny graph".

- MPKC

Multivariate Public Key Cryptography is a public key cryptography based on solving systems of polynomial equations.

As highlighted in the 2021 NIST survey results⁷, the problem still takes some time, but preventive action is needed.

The basic idea is to create an architecture with a modular encryption algorithm that connects with the same interface and that can change over time. In this way, multiple encryption algorithms can coexist in the Blockchain; every block header will contain a field indicating the algorithm used for the encryption, as shown in Fig. 6.1. This allows the Blockchain to not discard or readapt all validated blocks in order to switch to a quantum-safe algorithm, minimizing the left part of Mosca inequality.

The Blockchain becomes versionable from the encryption algorithms' point of view and some smart contracts will be used to store and read the *algorithm* field, to know the used encryption algorithm, in every block. The architecture proposed in Fig. 6.2 shows how a Blockchain can evolve and switch from a quantum broken chain (blocks #i-2 and #i-1) to a quantum safe one (blocks #i and #i + 1) without the need to discard all quantum broken blocks. Instead, the *version* field helps to

⁷<https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report>

manage different encryption algorithms and keep track of them, so the chain will not split after the introduction of new algorithms. This minimizes, following the Mosca inequality described in the chapter above, the time needed to adapt the infrastructure to the new technology.

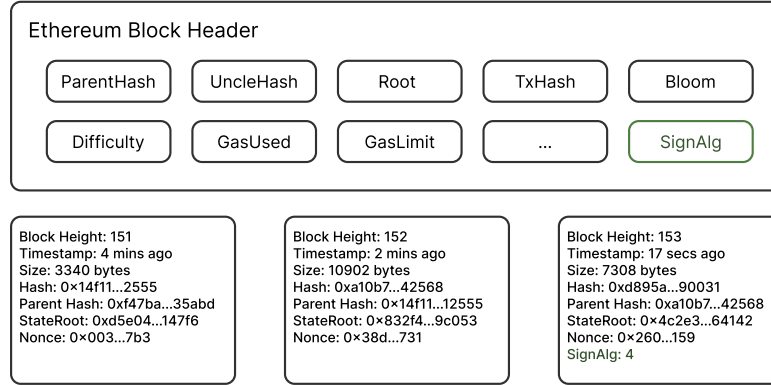


Figure 6.1: Ethereum block header with SignAlg field added

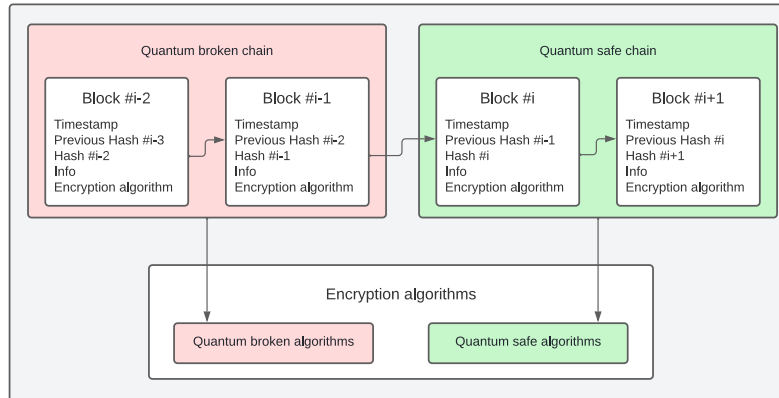


Figure 6.2: Proposed architecture overview

6.3.1 Workflow

The sequence diagram shown in Fig. 6.3a describes the operations required to add a new block to the chain. The first smart contract, responsible for adding a node, makes an add request to the *BlockCryptoAlgorithmCheck* smart contract, which verifies whether the block should be added to the chain using a quantum-broken or safe algorithm for the signature and optional data encryption. Then the first smart contract calculates the block hash and adds that block to the chain.

The sequence diagram shown in Fig. 6.3b describes how to get block information from the chain. The node makes a block request to the Blockchain using a

smart contract, that is responsible for the decryption (if needed) of the contained information using the correct algorithm. In this case, it gets the version field to understand what algorithm should be used, then decrypts the block information and gives them back to the node.

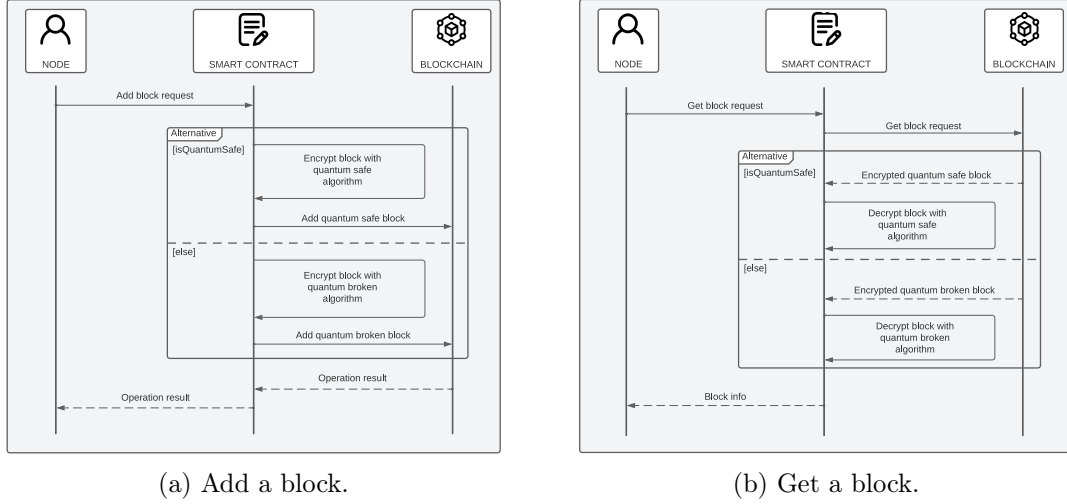


Figure 6.3: UML sequence diagrams for (a) adding a new block to the chain, encrypting it with a defined algorithm and (b) getting a block, decrypting it with the used encryption algorithm.

The smart contract is based on an enum, called *BlockCryptoAlgorithm*, which identifies if the encryption has been made through quantum-safe or not algorithms. External contracts can use this simple contract to set the used encryption algorithm using the first two functions; they can also get the actual algorithm of the block using the *getAlgorithm()* view function, to understand how to decrypt the information contained in that block or how to verify the block signature.

A practical implementation of this architecture is done in the Official Go implementation of the Ethereum protocol. The header has been extended with the *SignAlg* field, an integer number that contains the information about the used encryption algorithm (either a quantum-broken or quantum-safe one). The system makes a request to update that field during the block creation process using the smart contract described above, passing the corresponding number taken from the *BlockCryptoAlgorithm* enum. The block header now contains the information on the correct algorithm to use to decrypt it; the information can be used to access those block transactions. Fig. 6.1 shows the implementation in a local Ethereum network with three blocks: the first two blocks show the standard encryption, while the third block presents the *SignAlg* field with value 4, indicating that a different algorithm has been used. The smart contract will then convert the value 4 to the correct algorithm (e.g.: QuantumSafe2 based on the proposed smart contract).

6.3.2 Discussion

A modular likeness for the Blockchain technology permits users to have no constraints on specific algorithms, but they can let the system evolve over time adapting it to new signs of progress in research fields without the needing to discard old changes and information already stored. For example, in classic Blockchains, the architecture can be adopted for the transaction signature. All transactions made after a defined timestamp will be signed using a quantum-safe algorithm, while old transactions can still be verifiable using the old quantum-broken algorithm. The architecture fits also the chains where data are encrypted and not visible to anyone [89]: in this case, it is possible to correctly encrypt old and new data stored in blocks thanks to the coexistence of multiple encryption algorithms.

This architecture allows the creator of a Blockchain to minimize the left part of the Mosca inequality, letting NIST find all the possible encryption algorithms and adapting his own infrastructure to them. Blocks that have already been validated using older and quantum-broken algorithms will be kept alive in the chain without the need to adapt or discard them.

This kind of adaptation carries some limits to the platform. Older blocks will still be quantum-broken, so their stored information will not be part of the quantum-safe switch, even if the entire chain will still be resistant to quantum attacks. This can be seen as a physiological problem of the technology: what is done and validated can be attacked in the future if it is not adapted to new technologies.

6.4 Quantum safe signatures

This short proposal provides an interface for supporting different signature methods in the implementation of Go Ethereum nodes⁸. The Geth implementation is the most used one, so we decided to focus on its version v1.11.0 (Annos Basin), to analyze the code and develop our approach to support a quantum safe signature algorithm. We identify different paths and files to modify to switch from the use of ECDSA signature algorithm to multiple algorithms. The main folder to analyze is located in *go-ethereum/crypto*: in particular, we analyze the *crypto.go* and *signature_cgo.go* files.

To parameterize the methods contained in these files, we created *crypto_ecdsa.go* and *signature_cgo_ecdsa.go*. Each time a method is called in the go-ethereum code, the calling functions make a check on the used algorithm and call the right function with its inputs and expected outputs. The main constraint is to use an ECDSA-compliant algorithm, that is, an algorithm using the same dimensionalities (i.e.,

⁸<https://geth.ethereum.org/>

public and private key size, signature size, signature parameters) and formats of ECDSA. To overcome this issue, we plan to improve our interface further, considering only the main methods and making them accept byte-formatted parameters as input and output. The parsing functions will then be used to adapt the parameters to each signature algorithm used.

A node has been run and tested using the interface. The geth console is operational and correctly runs after generating a key-pair. Fig. 6.4 shows the details of the running modified node, and Fig. 6.5 shows the signature methods in action.

```
> admin.nodeInfo
{
  enode: "enode://
ebaeb62e122472c7988ad7e26255c16fd8527b7f15099d9325ccd2a3e35385fe7bc33625e4cb5cda3f76d6c9177f565722b8d8eeb79cd1e0441566906402e73@129.152.24.74:30303"
  enr: "enr:-Ka4QHeA8zsDe2nsDA_iMnRP8PIA-ytqlrWBgyeJel-
aUvK4RwwZgA91mdE3BZTPAgC_6b70IKzKsE67zcGeXuaomzaGAYar4xhgg2V0aMrJhPxk7ASDEYwwgmIknY0gmIwhjJGYGEqJc2VjcDl1Nmsx0QPr
rrYuEiRyx5IK1-JiVcFv2FJ7fxUJnZMizNKj410F_oRzbmFwwiNOY3CCdl-DdWRwgnZf",
  id:
    "27656ffe02b16f7df160bec014f5a1eb0247c4254df7ff2f2d6d9adb41ba59be",
  ip:
    "129.152.24.74",
  listenAddr: "[*]:30303",
  name: "Geth/v1.11.3-unstable/linux-amd64/go1.19.6",
  ports: {discovery: 30303, listener: 30303},
  protocols: {
    eth: {
      config: {
        arrowGlacierBlock: 13773000,
        berlinBlock: 12244000,
        byzantiumBlock: 4370000,
        chainId: 1,
        constantinopleBlock: 7280000,
        daoForkBlock: 1920000,
        daoForkSupport: true,
        eip150Block: 2463000,
        eip150Hash: "0x2086799aeebeae135c246c65021c82b4e15a2c451340993aacfd2751886514f0",
        eip155Block: 2675000,
        eip158Block: 2675000,
        ethash: 0,
        grayGlacierBlock: 15050000,
        homesteadBlock: 1150000,
        istanbulBlock: 9069000,
        londonBlock: 12965000,
        muirGlacierBlock: 9200000,
        petersburgBlock: 7280000,
        terminalTotalDifficulty: 5.875e+22,
        terminalTotalDifficultyPassed: true
      },
      difficulty: 17179869184,
      genesis: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      head: "0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3",
      network: 1
    },
    snap: {}
  }
}
> net.listening
true
> net.peerCount
11
```

Figure 6.4: Modified node running on Ethereum

```
marcofiore@10go-ethereum% ./build/bin/gethaccountnew--datadirmodular_chain

=====
You are using a method called by an interface to generate a key
=====

=====
You are verifying a transaction using a method called by the interface!
=====

INFO[03-02|11:10:20.439]Maximum peer count ETH=50 LES=0 total=50

Your new key was generated
Public address of the key: 0x76d7d8E20271D5240D9Ed53e206A606B4DD7c161
Path of the secret keyfile: modular_chain/keystore/UTC--2023-03-02T10-10-27.226351000Z--76d7d8e20271d5240d9ed53e206a606b4dd7c161
```

Figure 6.5: Signing and verifying transactions using the modified interface

6.5 Biometric key-pair generation

Biometric authentication systems have become increasingly prevalent due to their unique ability to identify individuals based on intrinsic physical characteristics. Biometrics, such as fingerprints, facial recognition, and iris scans, offer a highly secure alternative to traditional password-based systems by utilizing characteristics that are unique to each individual and difficult to replicate. Yet, despite their advantages, biometrics introduce challenges regarding privacy and data security, particularly when it comes to sensitive biometric data being misused or compromised.

Combining Blockchain with biometrics offers an intriguing solution to the dual problems of secure identity management and privacy protection. Two projects have been proposed to implement fingerprint-based and iris-based key-pair generation in a Blockchain platform.

6.5.1 Common background

A short background is presented for both proposals.

Biometrics

Biometrics refers to the measurement and statistical analysis of people's physical and behavioral characteristics. Biometric authentication is commonly used in various security systems to identify individuals based on unique physical attributes such as fingerprints, facial structure, or iris patterns.

Key-Pair Generation

Key-pair generation is a fundamental process in Blockchain systems, where each user is assigned a public key and a private key. This cryptographic mechanism, known as asymmetric cryptography, ensures that the private key, which is kept secret, can be used to sign transactions, while the public key can be used by others to verify the signature. The use of key-pairs guarantees that transactions can be securely authenticated without revealing the identity of the user.

The process of generating key-pairs is enhanced by incorporating biometric data as the seed for the cryptographic algorithm. Seeds are values from which cryptographic key-pairs can be deterministically generated. Using biometric data as a seed increases security because the biometric data is unique and bound to a specific individual. The key-pair derived from this seed allows the user to sign and verify transactions within the Blockchain, without compromising the privacy of their biometric data.

Feature Extraction Algorithm

Feature extraction is a critical step in biometric systems, as it involves processing biometric inputs to extract distinctive features that can uniquely identify an individual. The use of feature extraction algorithms offers a high level of accuracy and robustness in distinguishing between individual users, which is essential in biometric-based authentication systems. By leveraging the power of deep learning, this approach ensures that the biometric data is processed efficiently, resulting in high-quality cryptographic keys for use in Blockchain-based platforms.

6.5.2 Fingerprint-based generation

The functionality of the proposal is represented in Fig. 6.6. The user scans his or her fingerprint in order to generate a new key-pair. A Principal Component Analysis (PCA) is applied to the result of the scan to identify some characteristics of the fingerprint, then these characteristics are hashed using a secure hash function to ensure that the fingerprint information is not accessible by anyone. For security reasons, the system only hashes the fingerprint features and does not collect the whole fingerprint data. The novelty introduced in this architecture is about the obtained hash value, indeed it is used as a seed to generate the key-pair, composed by a public key and a private key.

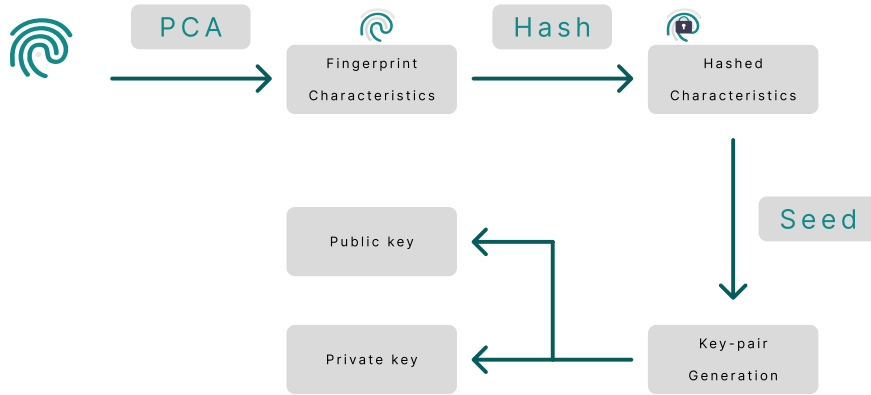


Figure 6.6: Architecture of the proposed fingerprint-based system

This kind of approach allows developers to design Blockchain-based platforms without the worry of sybil resilience, ensuring that every user can create a limited number of accounts – that is, one for each finger. Some approaches can be considered to further limit the number of wallets per user, for example recognizing the fingerprint and allowing the index finger only – 2 wallets per user.

There are several applications of the Blockchain technology, and in some cases it is mandatory to unambiguously identify the user to ensure that he or she does not create multiple wallets. Thanks to this biometrical approach, the proposed system

is able to reduce the number of wallets binding their creation to user fingerprint data. Differently from other approaches, several advantages can be obtained using the fingerprint data combined with the hash function in order to generate the seed for the key-pair generation. Since fingerprint data are not directly used for the authentication and they are not stored in the Blockchain, the anonymity of the user is guaranteed. Further studies will be done to understand how to further limit the number of wallets, for example scanning all 10 fingers, mixing their features to ensure anonymity, to get a wallet; another approach could be to identify only one finger per hand, limiting the number of wallets to 2 per user.

6.5.3 Iris-based generation

The architecture of the proposed system is designed to securely handle biometric data, particularly iris scans, for the purpose of generating a seed used in key-pair generation within a Blockchain platform. The architecture consists of several interconnected modules responsible for different stages of enrollment, authentication, and key generation. Each module is designed to ensure data integrity, security, and privacy while maintaining a decentralized approach through the use of Blockchain.

The system architecture is divided into three primary modules, as depicted in Fig. 6.7: (i) the Template Generation module, which extracts features from the submitted iris scan, (ii) the Enrollment Request (Sign-Up) module, which handles user registration and ensures that each user is uniquely enrolled, and (iii) the Authentication Request (Sign-In) module, which verifies that the user's biometric data matches the enrolled profile. Each of these modules communicates with the Blockchain network for secure storage and retrieval of the relevant biometric data.

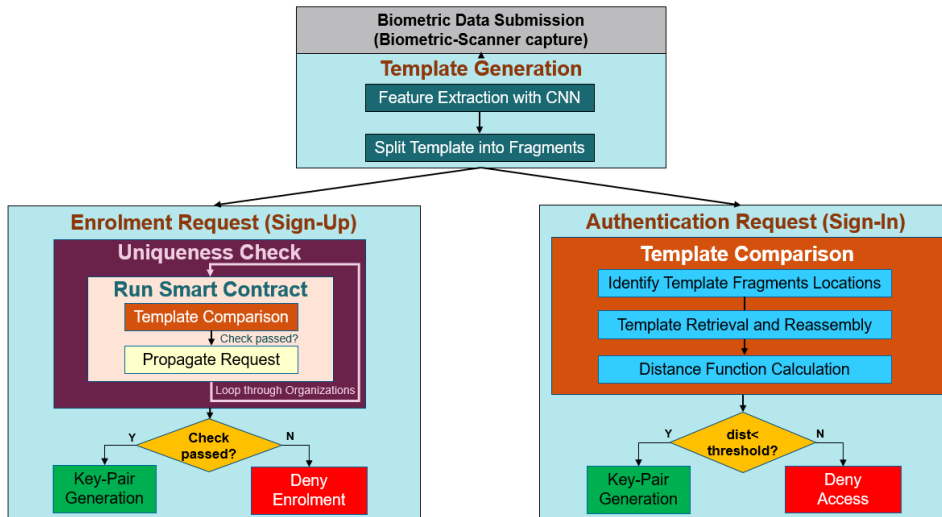


Figure 6.7: Architecture of the proposed approach

The primary objective of the architecture is to securely generate and manage key-pairs by using iris scans while distributing the biometric data across multiple nodes in the Blockchain. This decentralized approach increases security by ensuring that no single node has access to the complete biometric template, thus minimizing the risk of data theft or compromise.

The data flow in the system begins with the user submitting their iris scan through the client-side application. This data is passed through the Template Generation module, where a Convolutional Neural Network (CNN) extracts the unique features of the iris. The resulting feature vector is then hashed using a cryptographic hash function, such as SHA-256, to generate a non-reversible and secure representation of the biometric data.

Once the feature vector is processed, the Enrollment Request module handles the registration of the user in the Blockchain. If the user is enrolling for the first time, the system checks the uniqueness of the submitted biometric data by comparing the feature vector to the stored fragments in the Blockchain. The system ensures that no two users share the same biometric signature, thus preventing duplicate enrollments. Once the uniqueness is confirmed, the system generates a key-pair based on the hashed feature vector.

During the authentication process, the user submits their iris scan again, which is processed similarly to the enrollment phase. The Authentication Request module compares the newly submitted feature vector with the stored fragments in the Blockchain. If the comparison yields a match, the user is authenticated, and access is granted.

A critical aspect of the system's architecture is the distributed storage of biometric data. To enhance security and fault tolerance, the extracted feature vector from the iris scan is divided into multiple fragments, which are stored across different nodes in the Blockchain network. Each fragment is stored in random nodes, ensuring that no single node holds the complete biometric template.

This fragmentation and distribution of biometric data significantly reduce the risk of data breaches, as an attacker would need to compromise multiple nodes to reconstruct the full feature vector. Furthermore, each fragment is stored with replication to ensure redundancy and fault tolerance. The system uses a consensus mechanism to guarantee that data fragments are securely and consistently stored across the network.

The decision to adopt a distributed architecture ensures that the system remains highly available and scalable. Even in the event of node failures, the redundant storage of fragments across multiple nodes allows the system to continue operating without data loss or disruption.

For the management of the enrollment and authentication phases, the adopted distributed architecture guarantees the requirements of (a) reliability of the entire

system without relying on a central point, (b) availability of the network at any given moment, (c) robustness and fault tolerance: no single point failures and (d) scalability. The solution adopts a logical subdivision of the network into organizations characterized by two types of nodes called superpeers and peers, as shown in Fig. 6.8.

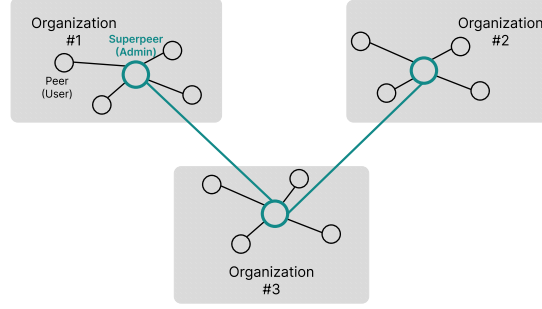


Figure 6.8: Distributed architecture organization

The architecture incorporates several fault tolerance mechanisms to ensure the system’s reliability. Each fragment of the biometric data is replicated across multiple nodes, ensuring that if one node fails, the data can still be retrieved from other nodes. This redundancy is crucial for maintaining the system’s availability, especially in a decentralized network where individual nodes may go offline.

In addition, the architecture uses a Byzantine Fault Tolerance (BFT) consensus mechanism to ensure that even if some nodes behave maliciously or unpredictably, the system as a whole remains secure. This consensus model is particularly suited for permissioned Blockchain networks like Hyperledger Fabric, where trust between participants is necessary but cannot always be guaranteed.

The redundancy and fault tolerance features allow the system to handle node failures, network partitioning, and other potential disruptions without compromising the security or availability of the biometric data or the key-pair generation process.

Security is a critical concern in the proposed architecture, particularly given the sensitive nature of biometric data. Several layers of security are incorporated into the design to mitigate potential risks:

- **Data Encryption:** All biometric data, including the feature vector fragments, are encrypted before being stored in the Blockchain. This ensures that even if an attacker gains access to a node, they cannot reconstruct the original biometric data.
- **Decentralization:** By distributing biometric data across multiple nodes, the architecture reduces the risk of data breaches. No single point of failure

exists, and attackers would need to compromise a significant portion of the network to access complete biometric information.

- **Sybil Attack Prevention:** To prevent Sybil attacks (where malicious actors control multiple nodes in the network), the system requires nodes to authenticate themselves using cryptographic keys and membership certificates issued by a trusted Certificate Authority (CA) in the Hyperledger Fabric network.
- **Smart Contract Security:** All enrollment, authentication, and storage operations are handled by smart contracts deployed on the Blockchain. These smart contracts ensure that biometric data is handled securely and that no unauthorized modifications are made to the stored data.

These security measures are designed to protect the integrity of the system while ensuring the privacy of the users.

Smart contracts play a vital role in managing the enrollment and authentication processes. During enrollment, the smart contract verifies the uniqueness of the submitted biometric data and stores the template fragments across different nodes. It also logs the user's key-pair in the Blockchain ledger, ensuring transparency and immutability.

For authentication, the smart contract retrieves the relevant template fragments and compares the newly submitted biometric data to the stored templates. If the match is successful, the contract grants access to the user and updates the ledger with the authentication transaction.

Smart contracts are written in Go and deployed on the Hyperledger Fabric network. These contracts are essential to the system's operation, providing the business logic necessary to manage user data, process transactions, and ensure the secure handling of biometric information.

System Workflow

The complete system workflow, from enrollment to authentication, can be summarized in the following steps, as shown in Fig. 6.9:

1. User submits an iris scan via the client-side application.
2. The scan is processed by the Template Generation module, which extracts a feature vector using a CNN.
3. The feature vector is hashed and divided into multiple fragments, which are stored across the Blockchain network.
4. During enrollment, the system verifies that the biometric data is unique and generates a key-pair for the user.

5. During authentication, the user submits another iris scan, which is processed and compared to the stored fragments.
6. If the biometric data matches, the user is authenticated, and access is granted.

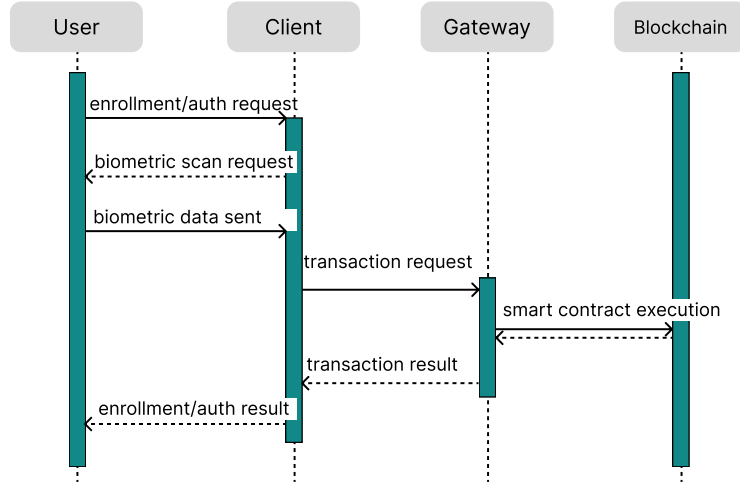


Figure 6.9: UML Sequence diagram

This workflow ensures that biometric data is handled securely at every stage, from initial submission to key-pair generation and user authentication.

A Web Application named Iris-Chain has been developed to handle the user's biometric data, the connection to the permissioned Blockchain to perform the enrollment or authentication tasks, and the generation of the user's key-pair starting from the submitted biometric material and the subsequent registration of the performed transaction in the Distributed Ledger. The languages and technologies adopted to implement the proposed architecture are: a) biometric materials: iris; b) client-side application: ReactJS framework; c) server-side application: NodeJS; d) template generation: PyTorch; e) feature extraction: ResNet18 CNN; f) distance function: cosine distance; g) hash function: SHA256; h) Blockchain: Hyperledger Fabric; i) signature algorithm: EdDSA; j) smart contracts: GO.

The client-side of the web application has been developed using JavaScript and the React framework. The user first has to authenticate to access the Iris-Chain platform, which means signing in if the enrollment step has already been completed or signing up in the case of first access. In both cases, the platform will require the user to provide his username and submit the biometric material. Then, the username and the iris image are fetched from a peer in the network through an HTTP POST request.

After the server-side calculation is complete, the user will be forwarded to a page that displays the result of the enrollment/authentication request.

The server-side of the web application has been developed using JavaScript and the Node.js framework. Its main function is to receive the biometric material from the client and compute the feature vector by performing a feature extraction using the last convolutional layer of “ResNet18” Convolutional Neural Network (CNN) from the PyTorch framework. The resulting feature vector, which consists of 262144 float64 values, is then divided into 3 fragments. Regardless of the request type, the network node needs to check first whether the submitted username is already present in the ledger. Then, if the request type is a sign up, the submitted username must be new to the ledger; if the request is a sign in, the username must already be present in the ledger. The smart contract “searchUser” has been developed to perform this query. The next operations that are carried out differ based on the request type. If a user wants to enroll, the peer checks the uniqueness of the submitted biometric material by comparing the feature vector extracted from the submitted image with the feature vectors of all the users currently enrolled in the platform. The information regarding which node of the network stores a Template Fragment for a certain user is included in the ledger. To retrieve these locations, the smart contract “searchTemplate” has been developed. For a given user, the output of this task is an extract of the ledger, providing the assets related to the storing locations of their template fragments (i.e., the address of the storing peer, its port number, and the identification number of the fragment it stores), as shown in Fig. 6.10.

```
Search template location for User1, function returns Location, Port and FragmentNumber
Result: [
  {
    AssetID: 'asset11',
    Location: 'peer1.org1.trischain.com',
    Port: 7051,
    FragmentNumber: 1
  },
  {
    AssetID: 'asset13',
    Location: 'peer1.org2.trischain.com',
    Port: 9051,
    FragmentNumber: 2
  },
  {
    AssetID: 'asset15'
    Location: 'peer1.org3.trischain.com',
    Port: 11051,
    FragmentNumber: 3
  }
]
```

Figure 6.10: “Search template” smart contract output

The feature vector of an enrolling user is compared to the templates of every

user already enrolled in the network. If the cosine distance of the submitted feature vector is equal to or above the defined threshold, access to Iris-Chain is granted to the enrolling user. The submitted biometric material is stored on randomly selected peers of the network, with each Template Fragment having n replicas to ensure fault tolerance. In the event that the user successfully enrolls/authenticates, a key-pair for asymmetric cryptography is provided. An elliptic-curve cryptography method has been used to generate key pairs with the Edwards-curve Digital Signature Algorithm (EdDSA). The complexity of the implemented method, used to detect whether a submitted iris image belongs to a certain individual or not, is kept to a simple level with the usage of cosine distance. In any case, being extremely unrealistic to have two perfectly identical acquisitions of the iris of one individual, and with it therefore two perfectly identical feature vectors, our approach is capable to provide to the same person a novel key-pair at every access.

The pseudocode for identifying template fragments locations is shown in Algorithm 1, the pseudocode for the authentication request is shown in Algorithm 2, while the pseudocode for the enrollment request is proposed in Algorithm 3.

Algorithm	1	Identify	Template	Fragments	Locations:
------------------	----------	----------	----------	-----------	------------

```

searchTemplate(ledger, user)
    ledger ← connection instance to HyperLedger
    user ← provided Username
    userInfo ← []
    for asset in ledger do
        if user == asset.userID then
            info = [asset.Location, asset.FragmentNumber]
            userInfo.append(info)
        end if
    end for
    return userInfo

```

The Hyperledger Fabric platform of the Linux Foundation was chosen for the creation of the Blockchain. Furthermore, unlike other Blockchain systems, Hyperledger Fabric is private and authorized. Rather than an open, permissionless system that allows unknown identities to join the network, members of a Hyperledger Fabric network sign up through a service provider membership (MSP). This feature is essential for certifying biometric information. The topology implemented for our purposes is shown in Fig. 6.11.

The infrastructure of the Blockchain network consists of the R1, R2, R3, and RO organizations that interact through the C1 channel. Channel C1 features the CC1 configuration, agreed upon by all organizations, which includes definitions for all organizations and policies that define each organization's roles. In particular, in this implementation, the organizations R1, R2, and R3 will take care of joining the peers

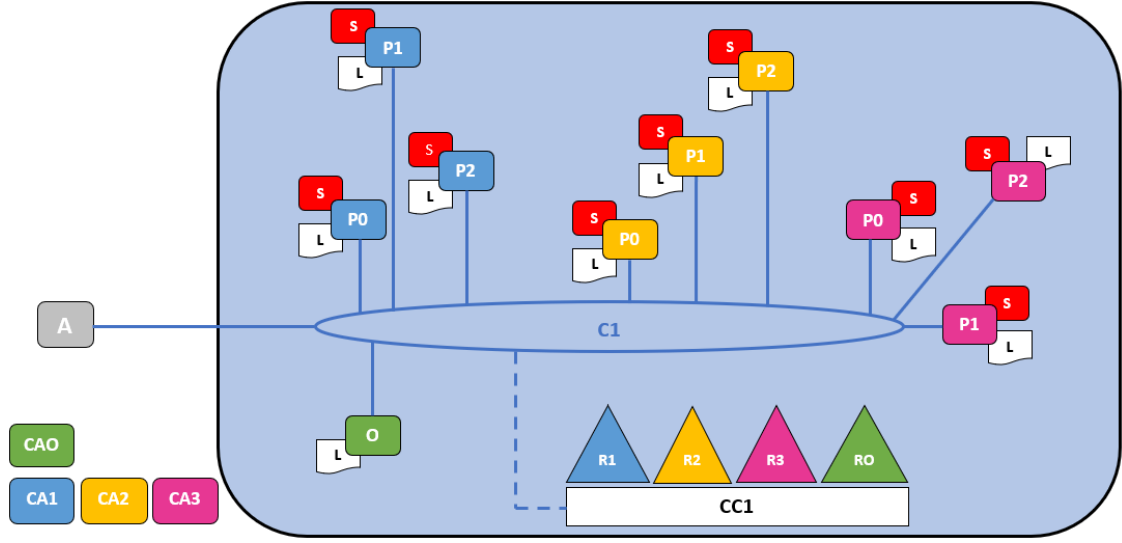


Figure 6.11: HyperLedger Fabric network topology

Algorithm 2 Authentication Request: $authenticate(ledger, user, biometric)$

```

Import:  $searchTemplate$ 
 $ledger \leftarrow$  connection instance to HyperLedger
 $user \leftarrow$  provided Username
 $biometric \leftarrow$  feature vector extracted from
    submitted biometric material
 $template \leftarrow$  empty
 $userInfo \leftarrow searchTemplate(ledger, user)$ 
if  $userInfo.length > 0$  then
    for  $fragmentNum.unique$  in  $userInfo$  do
         $fragment = GET(userInfo.Location[fragmentNum])$ 
         $template.concatenate(fragment)$ 
    end for
    if  $cosineDistance(biometric, template) < threshold$  then
         $keyPair \leftarrow generateKeyPair(SHA256(biometric))$ 
         $ledger.storeTransaction$ 
        return  $keyPair$ 
    else
        // Authentication denied
         $ledger.storeTransaction$ 
    end if
else
    // User not enrolled, authentication denied
     $alert("User not enrolled")$ 
end if
    
```

to the network, while RO owns O, the ordering service for the channel. The decision to implement a network with 3 peers per organization is in line with the decision to segment the features of the scanned iris into 3 segments so as to have a multiple of 3 peers. Peers P^* and ordering node O will contain a copy of the channel ledger (L), which is the structure where transactions are recorded. P^* peers represent the physical point with which organizations connect to the channel and through which they interact with the channel by carrying out transactions. The business logic that governs the transactions is implemented in the smart contract (S), which, according to the Hyperledger Fabric life cycle, has undergone the following phases: (i) packaged in a chaincode, (ii) installed on every peer in every organization, (iii) approved by every organization, and (iv) committed to the channel. The ordering service (O) collects approved transactions and sorts them into transaction blocks, which are then sent to peers to record the transaction and update their local copy of the ledger. Organizations interact with the channel through the client application (A), which interacts with the network through the Fabric Gateway. All organizations have a Certificate Authority (CA) that generates the necessary certificates for their organization's nodes, administrators, organization definitions, and applications.

Validation

Represented scenarios are a) an individual, whose biometric material is not present in Iris-Chain, chooses an available username; b) an individual, whose biometric material was submitted to Iris-Chain before, tries to enroll again choosing another available username; c) an individual tries to enroll using an already taken username; d) an individual, already enrolled in Iris-Chain, submits their biometric material using the correct username; e) an individual submits his biometric material using a username belonging to another individual; f) an individual submits his biometric material using an username not registered in the ledger. The proposed implementation recognizes all tested use-cases.

1. Individual, whose biometric material has not been submitted to Iris-Chain before, chooses an available Username so that result must be:
 - User successfully enrolled
 - Private Key provided to user
2. Individual, whose biometric material was submitted to Iris-Chain before, tries to enroll again choosing another available Username so that result must be
 - Enrollment denied
3. Individual tries to enroll choosing a Username already taken so that result must be:

Algorithm 3 Enrollment Request: *enroll(ledger, user, biometric)*

```
Import: searchTemplate
ledger  $\leftarrow$  connection instance to HyperLedger
user  $\leftarrow$  provided Username
biometric  $\leftarrow$  feature vector extracted from
    submitted biometric material
template  $\leftarrow$  empty
index  $\leftarrow$  0
flag  $\leftarrow$  False
userInfo  $\leftarrow$  searchTemplate(ledger, user)
if userInfo.length > 0 then
    alert("Username already registered in the Blockchain")
else
    while flag == False do
        userInfo  $\leftarrow$  searchTemplate(ledger, index)
        for fragmentNum.unique in userInfo do
            fragment = GET(userInfo.Location[fragNum])
            template.concatenate(fragment)
        end for
        flag  $\leftarrow$  cosineDistance(biometric, template) < threshold
        index  $\leftarrow$  index + 1
    end while
    if flag == False then
        keyPair  $\leftarrow$  generateKeyPair(SHA256(biometric))
        POST(biometric)
        ledger.storeTransaction
        return keyPair
    else
        alert("User not enrolled")
    end if
end if
```

- Enrollment denied
 - Suggestion to choose another Username (in case of new users) or to sign-in (in case of enrolled user mistakenly signing-up again) provided to user
4. Individual, who's already enrolled in Iris-Chain, submits their biometric material using the correct Username so that result must be:
- User successfully authenticated

- Private Key provided to user
5. Individual submits their biometric material using the Username belonging to another individual so that result must be:
 - Authentication denied
 6. Individual submits their biometric material using a Username not registered in the Ledger so that result must be:
 - Authentication denied
 - Suggestion to check the submitted Username (in case of enrolled user mistakenly typed their Username) or to sign-up (in case of new users) provided to user.

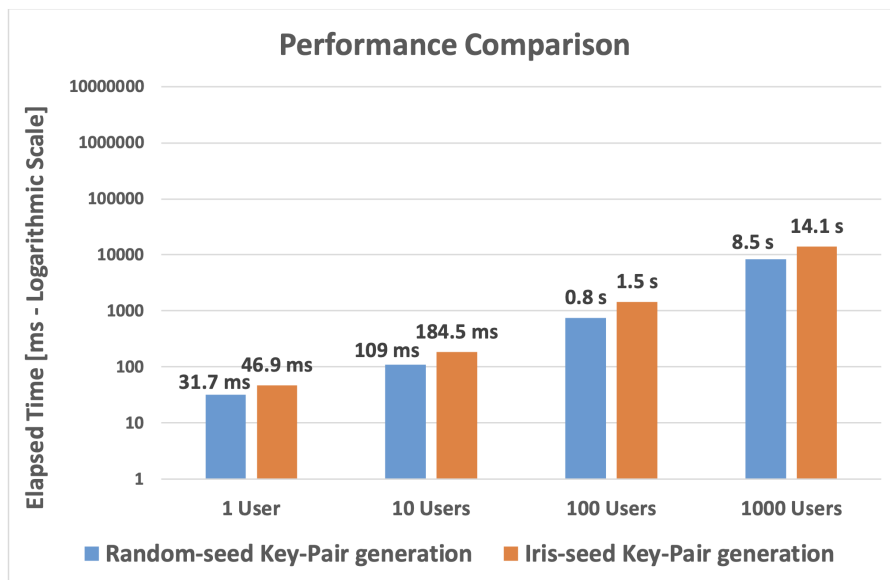


Figure 6.12: Required time comparison to generate 1, 10, 100 and 1000 simultaneous key-pairs

A comparison between the key-pair generation with EdDSA cryptographic algorithm using a random seed and a iris-based seed has been run to evaluate the performances in both methods. The comparison between the average time needed to generate an EdDSA Key-Pair using a random 32-Byte seed versus an Iris feature vector 2-Mbyte seed shows a little increase in time in the second case, as visible in Fig. 6.12. For a single user, the time increase is of 15 ms, so it is not considered a performance issue. A stress test has been conducted for the simultaneous generation of 1000 key-pairs: in this scenario, the time required to perform the operation increases from 8.5 s to 14.1 s. This is still considered an acceptable value because of the rareness of the event of 1000 simultaneous generations happening on the same device, being the generation of a key-pair an operation that happens client-side.

Table 6.3: Validation scenarios and effects

Action	Enrollment	Effect
Individual, whose biometric material has not been submitted to Iris-Chain before, chooses an available Username	User successfully enrolled	Private Key provided to user
Individual, whose biometric material was submitted to Iris-Chain before, tries to enroll choosing an available Username	Enrollment denied	Enrollment denied
Individual tries to enroll choosing a Username already taken	Enrollment denied	Suggestion to choose another Username (new users) or to sign-in (enrolled user mistakenly signing-up again)
Individual, already enrolled in Iris-Chain, submits his biometric material using the correct Username	User successfully authenticated	Private Key provided to user
Individual submits his biometric material using the Username belonging to another individual	Authentication denied	Authentication denied
Individual submits their biometric material using a Username not registered in the Ledger	Authentication denied	Suggestion to check the submitted Username (in case of enrolled user mistakenly typed their Username) or to sign-up (in case of new users)

Chapter 7

Blockchain Architecture

This chapter presents a range of Blockchain architectures developed and explored in published works, each tailored to specific application areas and requirements. Section 7.1 explores a hybrid private and public blockchain platform, combining security and transparency. Section 7.2 discusses blockchain implementation on IoT devices, addressing resource limitations. Section 7.3 introduces a hybrid blockchain and NoSQL platform for efficient data management. Section 7.4 examines blockchain sustainability from a smart contracts deployment point of view, while Section 7.5 presents a reward-based architecture. Finally, Section 7.6 proposes an architecture tailored for smart city applications.

7.1 Hybrid private and public Blockchain platform

To understand how Blockchain relates to agri-food traceability, an update on current literature is needed. There are several approaches that can be analyzed towards Blockchain-based traceability architectures, ranging from agri-food [90, 56, 91, 92, 93] to healthcare [94, 95, 96] and smart cities [11]. Most of the analyzed architectures propose an approach that takes advantage of Internet of Things (IoT) devices [97, 98]: in these cases Blockchain and Distributed Ledger Technology ensure availability and traceability of data exchanged and stored in the Supply Chain. Other implementations consider just one kind of Blockchain architecture, either public [99] or private [100, 101], even in conjunction with the Inter Planetary File System (IPFS) [102].

A common issue in these approaches is to guarantee high performance even though the usage of devices having a small amount of memory and poor performance. A Blockchain system requires devices with good memory, but no implementations are proposed on the application of a private Blockchain together with a public one to correctly manage data coming from sensors. Consistency of data is

Here, the interaction between different Blockchains is highlighted. The main system is based on Ethereum¹, to guarantee all the benefits of using a public Blockchain: transparency, data immutability, reliability. The Ethereum nodes consist of some edge computing units, responsible for management of all the internal low-memory devices. These devices will not rely on some NoSQL databases as described by authors of papers [103, 104] to communicate and store data: they use a containerized private Blockchain, in particular we use Hyperledger Fabric² but to this purpose any private Blockchain can be used. This approach provides modularity and scalability to the platform. Each edge computing unit is at the same time an Hyperledger peer and an Ethereum node: from Hyperledger side, it can obtain data from IoT sensors, manage and convert them into valuable data; from Ethereum side, it can upload the output of the computation (i.e. the mean and standard deviation of monthly data) lightening the Blockchain load. Due to their limited memory and computational power, IoT sensors can only benefit from the application of our methodology: sensor's ledger is less expensive than the Ethereum one, because they only keep track of the information collected inside their container. The behaviour of a container is independent of all others, thus ensuring modularity and scalability to the platform.

Smart contracts are used to manage the public and private Blockchain. On Hyperledger side, they are developed following a context-aware approach: they can receive any kind of input data from sensors and insert them into the database using a JSON format. Fig. 7.2 shows the JavaScript chaincode for updating data or adding new information to an array.

¹<https://ethereum.org/en/>

²<https://hyperledger-fabric.readthedocs.io/en>

```
async updateDocData(ctx, id, oldData, updatedData) {
  const old_data = JSON.parse(oldData);
  const updated_data = JSON.parse(updatedData);

  const updatedDoc = {
    ...old_data,
    ...updated_data,
  };

  await ctx.stub.putState(id, Buffer.from(JSON.stringify(updatedDoc)));
  console.log(updatedDoc);
}

async addData(ctx, id, oldData, category, newData) {
  const new_data = JSON.parse(newData);
  const doc = JSON.parse(oldData);

  if (!Array.isArray(doc[category])) {
    throw new Error(`Given category is not of Array type!`);
  }
  doc[category].push(new_data);
  await ctx.stub.putState(id, Buffer.from(JSON.stringify(doc)));
}
```

Figure 7.2: Hyperledger Fabric chaincode written in a context-aware approach

Fig. 7.3 shows the output of such functions in a food traceability system with an updated value (Plant density) and a new information inserted in the Cultural Operations array. The edge computing unit reads the inserted data, converts them in valuable data and sends the final information to Ethereum. In this way, thanks to the applied algorithm, the amount of data sent to Ethereum and stored in Hyperledger Fabric subsystem is reduced. Consistency of data is not a problem in this approach, because a common interface is used: information between platforms is exchanged using a JSON format, that is managed by the JavaScript chaincode and by the Solidity smart contract.

```
"Cultivated_species": "POMEGRANATE",
"Cultivated_variety": "WONDERFUL",
"Plant_density": "500 p/ha", // This
value has been updated through the
updateDocData function, previous value
was 300 p/ha
"Alternate_land": "No",
"Cultural_operations": [
  {
    "Progressive_number": 1,
    "Date": "10/09/22",
    "ID_lot": 1,
    "Operation": "Pruning",
    "Type": "Manual",
    "Hours": "10 h/Ha"
  },
  {
    "Progressive_number": 2,
    "Date": "18/10/22",
    "ID_lot": 1,
    "Operation": "Chopping",
    "Type": "Mechanic",
    "Hours": "2 h/Ha"
  },
  // Following object has been inserted
  through the addData function
  {
    "Progressive_number": 3,
    "Date": "20/11/22",
    "ID_lot": 1,
    "Operation": "Suckering",
    "Type": "Manual",
    "Hours": "5 h/Ha"
  }
]
```

Figure 7.3: Execution of the Fabric chaincode in a Blockchain-based traceability system

7.1.2 Scenario

The proposed system has been implemented following a scenario: design and development of a traceability system for agri-food supply chain. Our schema is different with respect to the approaches described in papers [105, 106, 107].

The scenario proposes five different fields, each of them covering an agri-food product: asparagus, pomegranate, almond, tomato and durum wheat. The system is split into three main parts: collecting data, transforming data into value, sending value to the public Blockchain.

Collecting data

Data collection is possible thanks to some IoT sensors in the field that measure temperature and humidity and meteorologic parameters, ranging from the rain percentage during the day to the wind speed. These data are not valuable if considered standalone, but they should be gathered to extract useful information. Furthermore, these big data occupy lots of memory, so it would be impossible for a low memory device to obtain an exhaustive storage of the information coming from all the sensors. By creating a local private Blockchain, devices can easily manage smaller amounts of data. The usage of a private Blockchain, with respect to a general database such as MongoDB, grants immutability of data even in this phase of the process. No one can alter data, so counterfeiting is avoided.

Transforming data into value

Each field is gifted with an edge computing unit, that is responsible of reading every information that the sensors store in the private Blockchain. These units take data and convert them into value, performing some preliminary analysis on the importance and priority of the gathered information. The output of this process is a lightweight set of information that can be stored in the public Blockchain, to make them accessible by anyone.

Sending value to the public Blockchain

Every edge computing unit is a peer in the private Blockchain and a node in the public one. Only these units can upload new information to the public Blockchain, so only the final reports of each field is accessible to people. This process makes the traceability system transparent and generates trust in the final user. The consumer, before buying an agricultural product in the supermarket, can read information about a product by scanning a QR code to know where the product has been produced, the temperature of the field, the number of cultural operations.

Strengths and limitations

The proposed architecture is simple to implement in new and existing systems, because it requires few hardware elements to work correctly. A single edge computing unit is enough to create the platform, because it can be connected to both Hyperledger Fabric (for IoT devices) and Ethereum (for data uploading). Modularity is intrinsic in the platform: each set of IoT devices can create a new Hyperledger Fabric image, using container-based approaches such as Docker. This method allows high performances and scalability in scenarios involving many IoT devices. Also security is important: in this architecture IoT devices do not contain any sensitive information, even though they are frequently and easily subject to attacks. In fact, data processing is performed by the edge computing unit.

In addition to this, thanks to smart contracts, it is possible to provide controls that automatically exclude from the analysis and the processing phase out-of-scale values due to malfunction or tampering with the IoT sensors.

Sensitive data are generated by the edge computing unit and inserted directly into Ethereum: this procedure ensures transmission security due to the Blockchain, but at the same time makes this unit become a point of failure of the architecture. Anyway, the addition of an edge computing unit allows data redundancy and avoids malfunctions especially if located in a different place. From the security point of view, it is possible to reduce the number of accesses to the system to a minimum and to avoid human suspicious accesses.

Blockchain, as explained before, is an add-only storage solution, but we are using it in a scenario composed by low-memory devices. Table 7.1 shows the memory occupied by transactions in the private Blockchain and the time needed to add a new batch of 100 transactions. To pursue our goal, the private Blockchain (Hyperledger Fabric) can gather data in a limited amount of time (i.e., a month), then perform a dimension reduction to collected data, upload it in Ethereum and discard old information (i.e., resetting the private ledger). This is not an issue for our proposal because data is still present in the system: its value has been already uploaded in the public Blockchain, so single data are not needed anymore.

Table 7.1: Memory needed to store transaction in the Blockchain and time needed to upload 100 new transactions

Transactions in Blockchain	Occupied storage (MB)	Time needed to add 100 transactions [sec]
0	0,219	0
5	0,272	0,36
10	0,339	0,84
50	0,635	4,44
100	0,892	8,46
500	2,5	40,26
1000	6,3	86,46
5000	32,4	421,26
10000	64,5	912,66
50000	335,7	5508,66

7.2 Blockchain implementation on IoT devices

The rise of the Internet of Things has introduced new challenges related to data security and transparency, especially in industries like agri-food where traceability is critical. Traditional cloud-based solutions, while scalable, pose security and privacy risks. This project proposes a decentralized architecture using Blockchain technology to address these challenges. We deploy IoT sensors connected to a Raspberry Pi for edge processing and utilize Hyperledger Fabric, a private Blockchain, to manage and store data securely. Two approaches were evaluated: computation of a Discomfort Index on the Raspberry Pi (edge processing) versus performing the same computation on-chain using smart contracts. Performance metrics, including latency, throughput, and error rate, are measured using Hyperledger Caliper.

One of the key features that makes Blockchain particularly well-suited for IoT applications is its ability to execute code directly on the network. Ethereum [24] pioneered this concept with smart contracts, which have since become widely used for managing transactions and data, as well as for generating digital assets like Non-Fungible Tokens (NFTs) and cryptocurrencies. Recent works, such as the one proposed in [8], implement context-aware smart contracts, focusing on employing Blockchain to securely store data in formats like JavaScript Object Notation (JSON). Additionally, strategies involving smart contracts for managing smart grid infrastructures are discussed in [108], while [109] presents a Blockchain-based payment system for IoT devices via the Ethereum Virtual Machine (EVM).

This paper explores the use of Blockchain and smart contracts as an alternative to traditional centralized cloud solutions, with a specific focus on monitoring air quality. Air quality is influenced by several environmental factors, with temperature and humidity being two critical determinants. These parameters are particularly important in sectors like agriculture, where maintaining optimal environmental conditions is essential for both crop yield and product quality. As a case study, we focus on the real-time monitoring of temperature and humidity data to assess air quality, leveraging the decentralized nature of Blockchain to ensure secure, tamper-proof data storage and analysis. In this context, we compare two different approaches on a Blockchain platform, namely Hyperledger Fabric, evaluating their performance and suitability for IoT-based air quality monitoring applications.

Current literature shows some proposals on the use of Blockchain technology for air quality monitoring. Benedict et al. [110] model an architecture based on Blockchain technology to monitor air in smart cities. They show some results based on execution times and connection to the Blockchain. Sofia et al. [111] implement a hybrid system composed by a centralized database for data computation and a public Blockchain, namely Ethereum. They optimize the data sent to the Blockchain in order to reduce transactions costs. However, data can be tampered in the centralized database phase, so there could be potential loss of information

in the workflow. De Tazoult et al. [112] and Hassan et al. [113] also propose architectures in which Ethereum is used as a Blockchain. Even in these cases, the information is not secure from start to finish, with the risk for it to be altered from malicious actors. The novelty of our proposal is the absence of intermediate databases, together with some considerations on the effective usefulness of which data should be inserted in the Blockchain for improving trust in the final user, like the consumer in an agri-food traceability platform.

7.2.1 Proposed architecture

This paper considers a scenario where IoT sensors are deployed in an agricultural setting to monitor environmental conditions, such as temperature, humidity, soil moisture, and sunlight exposure. These sensors play a vital role in ensuring optimal growing conditions for crops and provide critical data for traceability in the agri-food supply chain. The conventional approach would involve transmitting this data to a centralized cloud service for storage and analysis. However, this centralization poses security risks, including potential data breaches, unauthorized access, and loss of control over sensitive agricultural data [93]. To mitigate these risks, we propose a decentralized architecture that combines IoT devices, edge computing, and Blockchain technology. Instead of relying on the cloud, the IoT sensor data is first processed locally by a device such as a Raspberry Pi, which is connected to a private Blockchain network built using Hyperledger Fabric. This architecture ensures that data remains secure, traceable, and immutable throughout the supply chain without relying on a third-party cloud provider.

The proposed architecture is shown in Fig. 7.4 and consists of the following key components:

- **IoT Sensors:** Deployed in the field to continuously gather data on environmental conditions. These sensors collect crucial information that impacts the quality and growth of crops.
- **Raspberry Pi (Edge Device):** Acting as a local processing unit, the Raspberry Pi collects data from the IoT sensors and performs initial computations. This reduces the dependency on centralized cloud resources and enables faster, real-time decision-making at the edge.
- **Private Blockchain:** The processed data from the Raspberry Pi is transmitted to a private Blockchain network via a smart contract. In this scenario, Hyperledger Fabric serves as the underlying Blockchain platform. Its permissioned nature ensures that only authorized participants in the agri-food supply chain can access the data. Fabric's modular design allows for the creation of custom

chaincodes (smart contracts), which facilitate secure data transmission and storage.

- Chaincode: Smart contracts are employed to automate the data handling process. The chaincode is responsible for securely recording sensor data onto the Blockchain and triggering specific actions based on predefined rules.

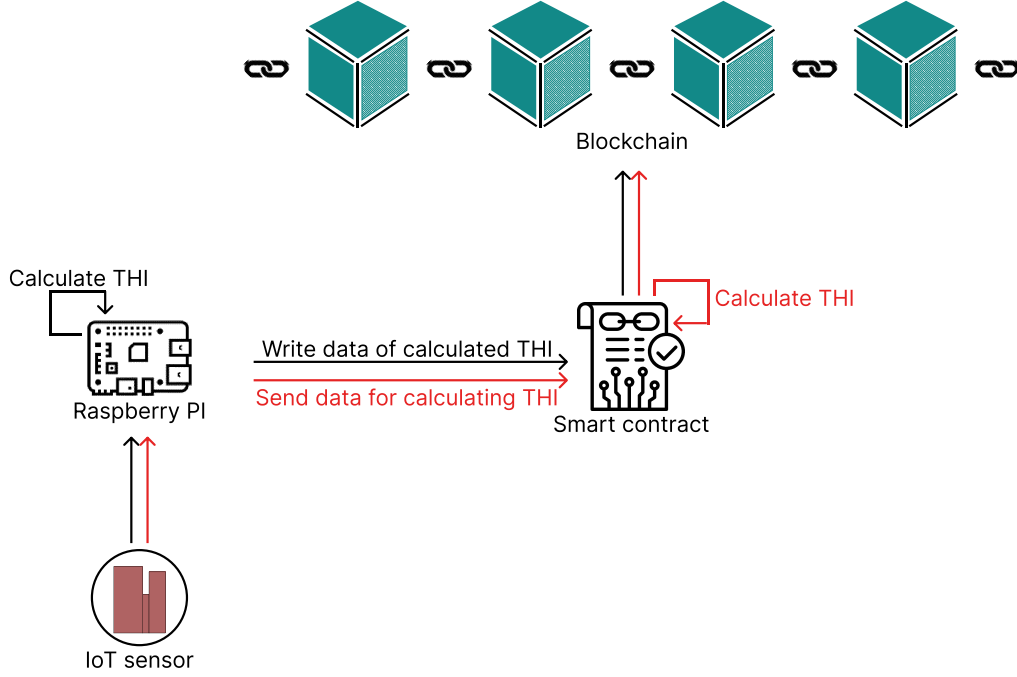


Figure 7.4: Architecture showing two different approaches for calculating THI

The DHT 11 sensor, taking into account the sensor specs, has an 8 bit resolution, a temperature range of 0°C to 50°C, and a precision of $\pm 2^\circ\text{C}$. Relative humidity readings have an accuracy of $\pm 5\%$ and a range of 20%-90%, according to the standard. Monitoring comfort and discomfort of interior environment in relation to a specific temperature and humidity combination has been the main focus. The Temperature Humidity Index (THI) [114] is used to aggregate the sensed temperature and humidity. Also referred to as the Discomfort Index, it provides some context for the potential implications of the detected data. The calculation of the THI is as follows:

$$THI = (1.8 * T - ((1 - RH/100) * (T - 14.3))) + 32 \quad (7.1)$$

where T is the temperature in Celsius and RH is the relative humidity. As seen in Table 7.2, various assessments of the discomfort can be made based on the value the index assumes.

In the proposed implementation, only the computed THI is uploaded to the Blockchain, rather than the raw temperature and humidity data. This approach reduces the amount of potentially unuseful information stored on the Blockchain, which is important given that Blockchain is an add-only storage solution. By focusing on the THI, we streamline the data stored, improving efficiency and ensuring that only relevant, trust-enhancing information reaches the end user, such as consumers in an agri-food traceability platform. To evaluate the flexibility and efficiency of this architecture, we propose two different test cases. The first one regards a computation on the Raspberry Pi: it processes the raw sensor data locally and computes the THI. Once computed, the Raspberry Pi transmits the final value to the private Blockchain, where it is recorded and made available for stakeholders. This approach takes advantage of edge computing, reducing the computational load on the Blockchain and enabling real-time analysis. The main benefit here is that the Blockchain is used purely for storage and validation, while the computation is offloaded to the edge device.

Table 7.2: Discomfort Considerations

THI Values	Considerations
$65 \leq THI < 68$	Possible discomfort
$68 \leq THI < 72$	Little discomfort
$72 \leq THI < 75$	Discomfort
$75 \leq THI < 79$	Alert
$79 \leq THI < 84$	Danger
$THI \geq 84$	Emergency

In the second test case, instead of performing the computation on the Raspberry Pi, the raw sensor data is sent directly to the Blockchain. A chaincode deployed on Hyperledger Fabric and shown in Alg. 7.1 is responsible for computing the THI. This allows for greater transparency and trust in the calculation, as the logic is executed directly on the Blockchain, ensuring that all participants can verify the computation process.

Listing 7.1: Hyperledger Fabric chaincode

```

async thiCalculus(ctx, id, temp, hum){
  let msg;
  let thi = (1.8*temp -((1-(hum/100))
              *(temp-14.3)))+32;
  if (thi >= 65 && thi < 68){
    msg = "Possible discomfort";
  }else if (thi >= 68 && thi < 72 ){
    msg = "Slight discomfort";
  }else if (thi >= 72 && thi < 75){

```

```

        msg = "Discomfort ";
    }else if (thi >= 75 && thi < 79 ){
        msg = "Alert ";
    }else if (thi >= 79 && thi < 84){
        msg = "Danger ";
    }else if (thi >= 84){
        msg = "Emergency ";
    }else{
        msg = "Do Nothing ";
    }
    return msg;
}

```

This method fully leverages the distributed nature of the Blockchain, as all calculations are performed within the network. While this adds to the transparency and immutability of the data, it may introduce performance overhead, as Blockchain networks are generally slower at processing compared to local devices [115].

By testing these two scenarios, we aim to assess the trade-offs between edge processing and Blockchain-based computation.

7.2.2 Results and discussion

Tests have been run on a Fedora 40 machine, powered by a 12th Gen Intel Core i7-12700 processor, 32 GB of RAM, NVIDIA RTX 3070ti graphics card, and 1 TB of disk space. The two Fabric configurations have been benchmarked using Hyperledger Caliper, a tool used to calculate performance metrics of Blockchain platforms. Table 7.3 shows obtained results.

Table 7.3: Benchmark report in Hyperledger Caliper

Approach	# Transactions	Input TPS	Error rate (%)	Max L (s)	Min L (s)	Avg L (s)	Throughput
THI at edge	100	50	0	0.21	0.07	0.13	50.6
	500	50	0	0.19	0.06	0.12	50.2
	1000	50	0	0.19	0.06	0.12	50.1
	100	100	0	0.13	0.06	0.10	98.3
	500	100	0	0.13	0.06	0.09	99.6
	1000	100	0	0.15	0.06	0.09	99.9
THI in Blockchain	100	50	0	0.19	0.06	0.13	50.5
	500	50	0	0.20	0.06	0.13	50.1
	1000	50	0	0.18	0.06	0.12	50.1
	100	100	0	0.13	0.06	0.09	98.6
	500	100	0	0.14	0.06	0.10	99.3
	1000	100	0	0.13	0.06	0.09	99.8

Each approach was tested under different loads, with varying numbers of transactions (100, 500, and 1000) and input transaction rates (50 TPS and 100 TPS).

Latency

Edge Processing: The latency values in this approach are consistently lower compared to the Blockchain-based computation. The average latency (Avg L) ranges from 0.09 to 0.13 seconds across all transaction volumes. This lower latency is expected since the computation occurs locally on the Raspberry Pi before submitting the results to the Blockchain, reducing the overhead associated with Blockchain consensus.

Blockchain Processing: In contrast, the average latency for computing THI on the Blockchain is slightly higher but still in a similar range, from 0.09 to 0.13 seconds. However, the overhead of performing the calculations on-chain doesn't significantly increase the latency in this case, showing the efficiency of the Hyperledger Fabric platform in handling the computations.

Throughput

Edge Processing: Throughput values for edge processing closely match the input TPS, with near-perfect consistency in achieving the targeted throughput. For instance, with an input of 50 TPS, the system achieved a throughput of around 50 transactions per second, and at 100 TPS, throughput reached nearly 100 TPS. This high throughput is indicative of the Raspberry Pi handling the computational load efficiently and sending the results to the Blockchain without delays.

Blockchain Processing: Similarly, the throughput in the Blockchain-based computation approach is comparable to the input TPS, reaching nearly 100 TPS when tested at that rate. The ability of the Blockchain to handle high transaction volumes without significant degradation in throughput is notable, but it's worth mentioning that this approach might experience scaling challenges as more complex calculations are performed on-chain.

Error Rate

Both approaches displayed a 0% error rate across all tests, demonstrating the stability and reliability of the system. This suggests that neither edge computation nor Blockchain-based computation encountered any failed transactions or errors during the benchmarking, indicating robustness in the proposed architecture.

Max/Min Latency

Across both approaches, the maximum and minimum latency values are relatively consistent, with the maximum latency hovering around 0.19 to 0.21 seconds and the minimum around 0.06 seconds. These results indicate stable and predictable performance, with minimal variation between transactions in both processing scenarios.

While both approaches perform well across all key metrics, the edge processing method has a slight edge in terms of latency and throughput consistency, particularly under heavier loads (1000 transactions at 100 TPS). This is likely due to the local processing capabilities of the Raspberry Pi, which reduces the load on the Blockchain and speeds up overall transaction handling. The Blockchain-based computation, on the other hand, provides additional transparency and trust since all computations are done directly on-chain. However, it incurs a slightly higher processing overhead compared to edge computing, as expected from performing smart contract-based calculations on a distributed ledger.

In conclusion, the results show that edge processing offers superior performance in terms of latency and throughput, while Blockchain-based computation ensures greater transparency and trust. This study highlights the potential of Blockchain as a viable alternative to centralized cloud systems in IoT environments and suggests future research in scalability, hybrid architectures, and energy efficiency.

7.3 Hybrid Blockchain and NoSQL Platform

The main advantages of Blockchain regard data immutability, transparency, and the possibility to execute transactions between two parties in an untrusted environment. However, scalability and throughput are considered major challenges when it comes to the use of this technology [2]. Centralized databases can achieve better results than Blockchain in terms of speed and latency. This work puts forward a novel hybrid architecture making use of both Blockchain and NoSQL characteristics to enhance the system's performance [9]. On one hand, NoSQL platforms are very often used by enterprises looking for distributed approaches and ways to reduce downtime of their internal systems. On the other hand, several industries choose to adopt Blockchain in their existing database structure because of its data immutability feature. This leads to the creation of hybrid architectures leveraging the advantages of both technologies. In such case, two database layers are used: *i*) the first layer uses a lightweight-distributed consensus protocol that ensures some integrity level while providing good performance for querying, *ii*) the second layer uses a Proof of Work-based Blockchain to store evidence of the first layer's database operations.

Using NoSQL in a Blockchain application allows to handle different types of data, namely on-chain data coming from transactions in the Blockchain and off-chain data related to the Blockchain but not stored directly within the blocks - NoSQL can provide additional security and privacy to off-chain data.

7.3.1 Related Work

In this section we review the state-of-the-art techniques to enhance the Blockchain throughput.

Authors of papers [116, 117] investigate performance bottlenecks in Blockchain and present an efficient high-performance system for caching the Blockchain data in the FPGA Network Interface Controller (NIC) with the aim of improving scalability and throughput of Blockchain applications.

In [118], authors propose a Blockchain relational database involving all features provided by existing Blockchain platforms and with better support for complex data types. After separating the concerns of concurrent transaction execution and decentralized ordering of blocks of transactions, they make use of Serializable Snapshot Isolation (SSI) to concurrently execute transactions and validate each transaction in a block to obtain a serializable order that will be identical across all untrusted nodes.

Authors of paper [103] explain that hybrid Blockchain databases are decentralized systems that have three key components: *i*) a shared database that uses a storage engine, *ii*) a shared ledger replicated via a consensus mechanism, and *iii*) a user interface that usually supports a simple key-value store. They also review all the existing frameworks already implementing hybrid architectures.

Different tools and online systems can be also taken into consideration:

- **BigchainDB** [119] is a decentralized and immutable data storage system which leverages MongoDB as storage engine and Tendermint for consensus among the nodes. BigchainDB introduces two optimizations: *i*) Blockchain pipelining allows nodes to vote for a new block while the current block of the ledger is still undecided, and *ii*) parallel validation on multiple CPU cores.
- **BlockchainDB** implements a distributed database on top of a classic Blockchain. It is different from the other systems because it partitions the database into few shards so that the overall storage overhead is reduced.
- **Couchbase** allows to implement both of the data handling components usually used in Hyperledger systems. The two handling components are: *i*) operational transactions that verifies, creates and logs all transactions and *ii*) world state, another data view that maintains the current account values.

The state-of-the-art review reveals that hybrid architectures mixing Blockchain properties (e.g., decentralization, immutability, owner-controlled assets) and database properties (e.g., high transaction rate, low latency, indexing, querying of structured data) are a valuable solution to overcome limitations of the Blockchain technology. However, to the best of the authors' knowledge, no existing framework is able to perform data management in a completely context-agnostic manner, thus deciding at runtime where to store data in an automatic way.

7.3.2 System description

The goal of this work is to design a hybrid architecture able to *i*) automatically manage data in a distributed heterogeneous database and *ii*) handle data belonging to different user types in a context-agnostic and unstructured manner. Such system allows greater data security, without losing in performance speed.

This section explains how the overall architecture is organized, the roles of each component, and how the different parts are interconnected to create the workflow. The whole system consists of a three-layered architecture.

- **Data Layer**

Relies on a Firebase NoSQL database and an Ethereum Blockchain system. Firebase's key-value paradigm simplifies the process of working with unstructured data: each incoming information can be formatted into a key-value format. Moreover, to enter personal data into an Ethereum Blockchain, ad-hoc smart contracts are typically needed. If all data is represented using the same structure, a single general-purpose contract can be used instead.

- **Back-end layer**

Holds the whole logic, ranging from basic functions allowing user-system interaction to the logic leading to how the system reacts to a specific data request.

The content parser is the core element of the system because it bridges the gap between the logic layer and the data layer. Given a set of information from a user, the content parser decides whether the set of information should be stored either in the NoSQL database (fast transaction but not immutable) or in the online Blockchain (slow transaction but immutable). To do so, the idea is to classify users' data as sensitive or non-sensitive. Nevertheless, training a DL model to perform such task would require a large dataset comprising samples from different use cases to account for generalization, but no appropriate dataset is currently available.

Data Loss Prevention (DLP) services are essential for ensuring the protection of sensitive data within organizations, adhering to privacy and trust policies. DLP solutions offer more granular control over sensitive data, allowing organizations to monitor and protect data in real-time. Various solutions can be analyzed in this topic. For instance, Forcepoint DLP offers advanced protection with features like data discovery, classification, and monitoring, but it can be complex to configure and manage. Spin, on the other hand, might not offer the same depth of protection and could have limitations in terms of scalability, such as the ability to handle a large volume of data and limited integration with other systems. Google Cloud DLP is designed to discover, classify, and protect sensitive data across various environments, including databases, text-based content, and images. It offers advanced de-identification techniques

such as masking and tokenization, which help in maintaining data privacy while ensuring compliance with regulations like GDPR. Additionally, Google Cloud DLP provides real-time data protection and seamless integration within the Google ecosystem, making it easier to manage and enforce security policies. For these reasons, Google Cloud DLP has been chosen as reference model.

- **Front-end layer**

By interacting with the remote server, the web application provides the users with all the data-related functionalities: data storage, retrieval, and visualization. The realization of a web application allows to achieve portability, making the system independent from all sorts of platforms.

Fig. 7.5 shows the whole information flow within the system.

The DLP module analyzes the information and looks for sensitive data. At this point, if no critical record is found, the flow is redirected towards the NoSQL database. If sensitive data is detected, an online transaction is created in the Blockchain first and a tuple linking user ID and transaction ID is finally stored in the NoSQL database to keep track of every user's operation.

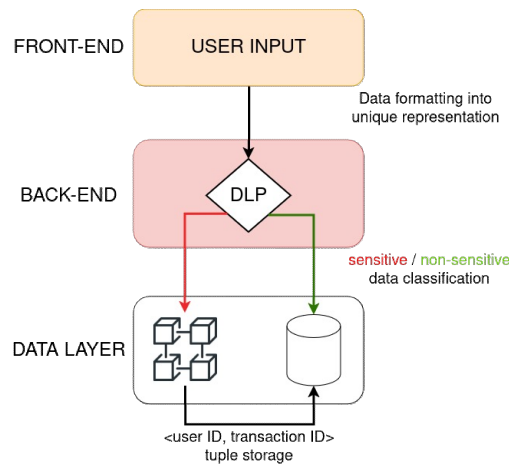


Figure 7.5: Hybrid system layered architecture and information flow

To speed-up basic operations, the core application logic (login, registration, etc.) runs on top of the NoSQL database, where all user-related information (IDs, passwords, etc.) is stored. The same happens to non-sensitive data that is organized and retrieved via the user's unique ID. To retrieve user-specific data from the Blockchain, all user's transactions IDs are first gathered from the NoSQL database (via user's ID) and then used to query the Blockchain system.

7.3.3 Experimental results

To evaluate the performance of the proposed system architecture, a fully working prototype has been realized. The Python Flask library has been used to develop the front-end web application, as it allows to easily manage key-value structured data while rapidly develop and test the server logic without needing to deploy the server on a public infrastructure. The Ganache framework is used to build up the Blockchain architecture, while an online Firebase DB has been created to host the NoSQL data.

In this preliminary stage, the objective is to gather data about the performance of the overall system in order to assess the validity of the idea. The implemented architecture works therefore in an offline setting. To show the capabilities of the framework, four use cases have been targeted: *i*) sensors' data from IoT networks, *ii*) medical records, *iii*) bank transactions, *iv*) school records from different universities.

The goals are: *i*) to check whether the Google DLP engine is able to perform the above-mentioned data classification by capturing sensitive information and *ii*) to measure the data management time difference between the NoSQL and the Blockchain systems. To carry out the first test, fac-simile data adherent to real-world structures were submitted to the prototype application. No specific dataset has been used in this stage. A custom dataset has been realized instead by generating, for each scenario, 200 samples. For instance, in the case of a bank transaction, the application requires to insert the bank account number of both the payer and the payee. Starting from the structure of a classical bank account number, the tool is then able to generate real-world data with plausible bank account numbers, while fake records contain random strings. The same happens for Social Security Numbers and so on. The generated dataset has finally been used to test the DLP module.

The DLP basic module allows to handle the selected case scenarios because it already provides built-in detectors for all the sensitive information potentially linked to each case. Even though no additional training has been performed on top of the model, some custom detectors based on regular expressions have been developed to extend the model detection capabilities. Before deploying the application, the likelihood threshold of each detector has been fine-tuned so as to reduce the number of both false positives and missed detections.

All the tests carried out show that Google DLP is able to perform the task of discriminating sensitive and non-sensitive information, thus redirecting the first towards the Blockchain and saving the latter in the NoSQL database. To ensure the validity of the tests, some constraints were fixed for each use case (e.g., a doctor was asked to insert the Social Security Number of the patient when saving a medical record or the bank coordinates had to be specified for each transaction).

The capabilities of the platform have been extended to automatically measure and store the time needed to carry out each task. This study particularly focuses on comparing the speed of both architectures during data storage and data retrieving. These execution times are therefore measured while a user is interacting with the platform and saved in the NoSQL database for further analysis.

Fig. 7.6 shows the performance comparison when new data is being permanently saved. Due to the creation of an immutable transaction in the ledger, the Blockchain average memorization time is much higher when compared to that of the NoSQL.

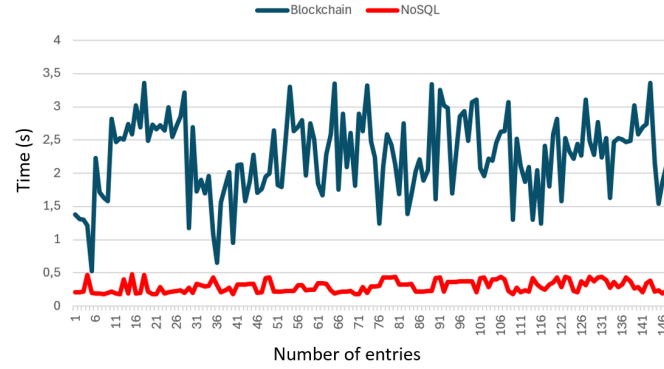


Figure 7.6: Time comparison (in seconds) during data storing activities

In Fig. 7.7, the time required to retrieve data is compared. Retrieving data directly from a NoSQL database is faster due to the direct access nature of key-value stores, where the data is retrieved using a unique key. On the other hand, Blockchain retrieval is a multi-step process that involves first obtaining the transaction ID from the NoSQL database, then using this ID to query the Blockchain. Although this process is slower, it offers the added advantage of transparency and traceability, which are crucial in environments where data integrity and auditability are essential. Table 7.4 compares saving and retrieving times in both approaches.

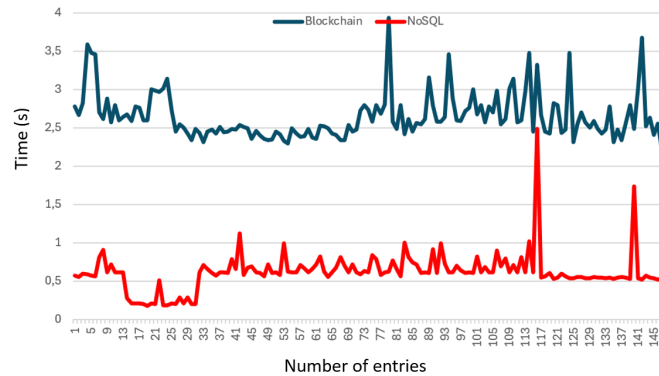


Figure 7.7: Time comparison (in seconds) when performing data retrieving

Results show that the proposed architecture successfully enhances the throughput of a Blockchain-based application. While state-of-the-art architectures enhance the performance speed by using parallel and distributed data sources, the proposed architecture achieves the objective by saving only data actually requiring immutability constraints in the distributed ledger. This is done by leveraging a parallel NoSQL database and Blockchain platform, and a DL-based decision pipeline to manage all data. The DL system relies on Google DLP model to perform a binary classification between sensitive and non-sensitive information. After classification, critical data is stored in the Blockchain to satisfy immutability constraints, while the NoSQL hosts all non-sensitive information.

Table 7.4: Retrieving and saving time comparison

	Retrieving Time			Saving time		
	Max [s]	Min [s]	Avg [s]	Max [s]	Min [s]	Avg [s]
Blockchain	3.93	2.23	2.63	3.36	0.53	2.14
NoSQL	2.48	0.18	0.47	0.48	0.18	0.25

7.4 Blockchain sustainability

Blockchain technology, as explained above, is based on the use of smart contracts. These contracts are written in different programming languages, which determine their complexity, and consequently, the transaction’s cost. The work presented in [13] analyzes the topic of cost considering smart contracts based on different Blockchains and various programming languages. This analysis helps identify which of the Blockchains is the most economical and sustainable in terms of energy for those who execute them and the environment.

7.4.1 Related Work

BLOCKBENCH [120] was introduced in 2017 as the first evaluation framework for analyzing private Blockchains in a fair and in-depth manner. The framework enables a better understanding of various system design choices and enables an objective comparison between different platforms. Integrating any private Blockchain into BLOCKBENCH is a simple process which can be accomplished via its APIs. BLOCKBENCH provides performance evaluation, measuring overall and component-wise performance in terms of throughput, latency, scalability and fault tolerance. The authors used BLOCKBENCH to comprehensively evaluate three major private Blockchains: Ethereum (as a solidity Blockchain), Parity, and Hyperledger Fabric. The results suggest that there is still significant room for improvement before these systems become viable replacements for current database systems

in traditional data processing workloads. Furthermore, the assessment highlights performance gaps among the three systems attributed to the design choices at different Blockchain software stack levels.

In [121], the authors have used a benchmarking approach in their research and shared the preliminary results for the Python Ethereum client running on a Mac. The study reveals that there can be significant differences in the reward per CPU second for functions in Ethereum's most popular contracts, which can result in misaligned incentives that impact the dependable operation of the Blockchain. Additionally, the research highlights that contract creation, done once for each new contract, can be more lucrative than the regular execution of contract functions.

In 2019, [122] presents a comparative analysis of various distributed ledger technology (DLT) platforms in a diplomatic and unbiased manner. The selection of platforms is based on their popularity, current market share, and evolving trends and approaches. The platforms selected for the analysis are Ethereum, EOS, Hyperledger Sawtooth, and NEO. The comparison is done from both development and performance perspectives to provide a comprehensive understanding of their strengths and limitations. The analysis reveals that Sawtooth offers significant customization capabilities that may affect performance, while EOS maintains stable throughput under varying network scales and loads.

[123] objectively evaluates and compares different smart contract functions. The article suggests using multi-criteria analysis (MCA) to assess and compare functions based on multiple criteria to ensure a fair evaluation process. The study provides a comprehensive review of the current state-of-the-art in the field by considering various criteria used in the selection process, such as security, scalability, and performance. It also highlights the challenges associated with critical criteria for smart contract selection, including security, privacy, efficiency, scalability, and regulatory concerns. However, the article stresses that the process is complicated by challenges such as the lack of standardization and difficulty comparing platforms. The article emphasizes the need for further research on smart contract platforms' long-term performance and scalability and more comprehensive and objective evaluation methods for MCA of smart contract selection while acknowledging the complexity of the subject matter.

The authors of [124] have proposed a multi-objective test selection technique for smart contracts that aims to balance three crucial objectives: time, coverage, and gas usage. They comprehensively evaluated their approach using five solidity smart contracts based on data collected from GitHub and State of the DApps³. They compared their results with various test selection methods in traditional software systems. Through statistical analysis of their experiments, which utilized benchmark Solidity smart contract case studies, the authors have demonstrated

³<https://www.stateofthedapps.com>.

that their approach significantly reduces the testing cost while maintaining acceptable fault detection capabilities. These findings have been compared to random search, mono-objective search, and the traditional re-testing method that does not employ heuristic search.

With respect to current state of the art, this paper analyzes different public Blockchains and programming languages, with the final goal to understand the impact of a language on energy consumption requirements.

7.4.2 Proposed approach

This study examines smart contracts implemented on multiple Blockchains using a variety of programming languages to assess their associated costs. The goal is to pinpoint the most economical and environmentally friendly Blockchain for its users and the ecosystem it operates within. Additionally, we investigate how different programming languages affect the gas transaction cost on various Blockchains, determining which ones are more economical. In terms of sustainability, we factor in the environmental impact of these Blockchains, specifically their electricity usage and CO2 emissions. The programming languages chosen range from high-level to low-level, facilitating a comparative analysis, thereby leading to the selection of the relevant Blockchains. All the analyzed Blockchains are permissionless, irrespective of the programming languages employed in smart contract development.

Private Blockchains are not included in the analysis because they are not accessible to individual users without authorization.

The chosen Blockchains are summarized below.

- **Ethereum and Solidity**

Ethereum, created by Vitalik Buterin in 2013, revolutionized Blockchain with its programmable smart contracts. Operating as a permissionless public Blockchain, Ethereum has transitioned to a Proof of Stake consensus protocol in 2023. Its native token, ETH, fuels platform activities and facilitates value exchange. Ethereum's pivotal role extends beyond cryptocurrency, powering the burgeoning decentralized finance (DeFi) sector. Advantages include a deflationary token supply, a robust community fostering demand, passive income opportunities through staking, and serving as foundational infrastructure for emerging projects like Non-Fungible Tokens (NFTs). Solidity, a high-level programming language primarily for Ethereum, facilitates smart contract development. Inspired by C++, Python, and JavaScript, Solidity interfaces seamlessly with the Ethereum Virtual Machine (EVM). Developers leverage Solidity to craft smart contracts governing various functionalities, including voting mechanisms and multi-signature wallets. Solidity programming necessitates Solidity compilers, such as Remix and npm, tailored for Linux and MacOS environments.

- **Tezos and SmartPy**

Tezos, introduced in 2014, offers innovative features surpassing traditional Blockchains like Ethereum. Its Liquid Proof-of-Stake (LPoS) consensus protocol allows for decentralized smart contract execution and governance through a voting mechanism. Tezos adaptability enables dynamic adjustments to its protocol parameters, enhancing security through formal methods. The native cryptocurrency, XTZ, fuels transactions within the ecosystem. Tezos architecture comprises multiple layers, with a peer-to-peer layer ensuring network connectivity and a subsequent layer treating the network as a distributed database. Blocks are extracted, modified, and passed to the economic protocol layer, responsible for consensus enforcement. SmartPy, a Python-like high-level language, simplifies smart contract development on Tezos. It offers a user-friendly syntax and a secure programming environment. Initially, smart contracts on Tezos were coded in Michelson, a low-level language focused on security and precision. SmartPy's compiler seamlessly translates code into Michelson for testing and deployment onto the Blockchain, enhancing developer efficiency and contract reliability.

- **Polkadot and Rust**

Polkadot, established in 2017, revolutionizes Blockchain interoperability with its Nominated Proof of Stake (NPos) consensus mechanism. The network features a primary relay chain governing inter-chain communication and numerous user-created parachains operating autonomously within the Polkadot ecosystem. Polkadot boasts a throughput capability of 1,000 transactions per second. Rust, developed by Mozilla Research, epitomizes modern systems programming by seamlessly blending low-level performance control with high-level convenience and robust security assurances. It excels in speed and memory efficiency, making it suitable for critical performance services and embedded systems, while its advanced type system and ownership model ensure memory and thread safety, minimizing bugs at compile time. Renowned for its eco-friendly attributes, Rust stands out as one of the most environmentally sustainable programming languages in use today.

- **Solana and C++**

Solana, introduced in 2018, stands out as a Blockchain platform optimized for widespread adoption, catering to diverse sectors such as finance, NFTs, payments, and gaming. Operating as a global state machine, Solana is distinguished by its high-performance architecture, open nature, and decentralized ethos. Its native cryptocurrency, SOL, drives transactions within the ecosystem. Solana's innovative Proof of History (PoH) consensus mechanism ensures verifiable event order and time intervals, fostering trust without reliance on external entities or synchronized clocks. C++, renowned for its versatility and efficiency, serves as an ideal programming language for Solana.

development. Combining low-level capabilities with high-level functionalities, C++ enables seamless integration with system libraries, making it a preferred choice for video game development, AR/VR applications, IoT devices, and operating systems. Notably, C++ boasts exceptional energy efficiency attributed to its minimal storage usage, further enhancing its appeal for Solana development.

7.4.3 Smart contracts definition

Analyzing functions in smart contracts is crucial for effective comparison. The diversity among programming languages complicates the task of defining executable programs, as some languages lack specific high or low-level functionalities, object-oriented capabilities, or other features. Consequently, we decided to employ very simple projects to ensure a comprehensive understanding.

The chosen functions, ordered by increasing complexity, are as follows.

- Sum of two numbers: we test how different programming languages manage the sum of two integers number, being it a mathematical primitive in equations. This primitive is shown in [124].
- Conversion of an integer into a string: we aim to analyze the behaviour of each Blockchain to a cast operation, as indicated in [120].
- Creation of a personal data record for a hospital patient: the goal of this contract is to verify the reaction of tested platforms with the management of a structure composed by strings and integers. Healthcare is between the main applications for evaluating smart contracts, as highlighted in [123].

Each function has been implemented in a smart contract written for every analyzed Blockchain. A total of 12 smart contracts have been written and tested.

7.4.4 Tests and results

This Section will show all the tests conducted on the selected Blockchain and the related results.

Ethereum - Solidity In conducting test cases for the Ethereum Blockchain, Remix IDE was employed because it provides a GUI and eliminates the need for configuration, making it ideal for developing smart contracts. It supports seamless deployment for users of all skill levels on any preferred chain. The testing process used virtual cryptocurrencies within a testnet environment provided by Remix IDE, which ensured a controlled setting for the experimentation and verification of smart contracts on the Ethereum Blockchain.

Tezos - SmartPy For the Tezos Blockchain, SmartPy IDE was selected. SmartPy IDE provides a comprehensive online environment for developing, testing, and deploying smart contracts on the Tezos Blockchain, all within the familiar Python syntax. Simulation was conducted on a test network called Ghostnet, which is popular for testing contracts without spending real cryptocurrencies.

Polkadot - Rust For evaluating Polkadot, a platform akin to Remix for Ethereum, known as Substrate, was utilized. Substrate facilitates the creation of Blockchain applications by equipping developers with a versatile toolkit that transcends the typical limitations found in other platforms. Unlike inflexible systems with set structures, Substrate presents a flexible and modular design, allowing developers to customize the Blockchain architecture specifically for their project's requirements. Substrate's flexibility arises from its emphasis on adaptability and customization. Its modular framework permits developers to easily integrate and modify components, facilitating the straightforward implementation of complex features. By adopting Substrate, developers can accelerate the development timeline, cut down on costs, and boost the scalability and interoperability of their Blockchain solutions.

Solana - C++ A local testing environment has been developed for Solana analysis. The tool used for tests was SolanaLabs, a local framework-like tool that enables the evaluation of various aspects of a contract for development and configuration. For the testnet, SolanaTestnet, provided by Solana, proved to be ideal for smart contracts testing and development. Lastly, Mathwallet, a local wallet, was used. It was populated with SOL currency using the SolanaDevnetFaucet.

7.4.5 Collected gas fees

We collect the spent gas for deploying each contract in a Blockchain. Results are summarized in Table 7.5.

Table 7.5: Results of contracts execution, in gas, in each chosen Blockchain

Blockchain	Smart contract language	Integers sum	Cast operation	Healthcare scenario
Ethereum	Solidity	328	1910	11681
Tezos	SmartPy	367	1033	9112
Polkadot	Rust	903	2416	13006
Solana	C++	299	4591	17467

Fig. 7.8 shows the gas fee comparison between the analyzed platforms. The trend depicted in the figure is nearly linear across all languages. Costs are significantly low when dealing with the sum smart contract. This can be attributed to the minimal gas required for the transaction since only a few low-level functions are used, resulting in low gas consumption.

Upon closer inspection, intersections of graphs are visible, particularly in the case of the sum contract. This can be attributed to the nature of programming languages. C++, being a low-level language, enables operations directly on memory, thus requiring minimal gas for execution on the Blockchain. The scenario changes when considering the cast smart contract. Here, high-level languages like SmartPy and PyTeal prove to be more cost-effective as they possess built-in syntax, commands, and functions for converting an integer to a string with just a single line of code. Conversely, low-level languages incur higher costs due to multiple and resource-intensive register operations. For the healthcare smart contract, the overall cost trend becomes clearer. Here, creating a Patient object creates some differences in different languages. Low-level and hybrid languages like Rust need to rely on external or more complex functionalities, leading to higher resource consumption on the chain.

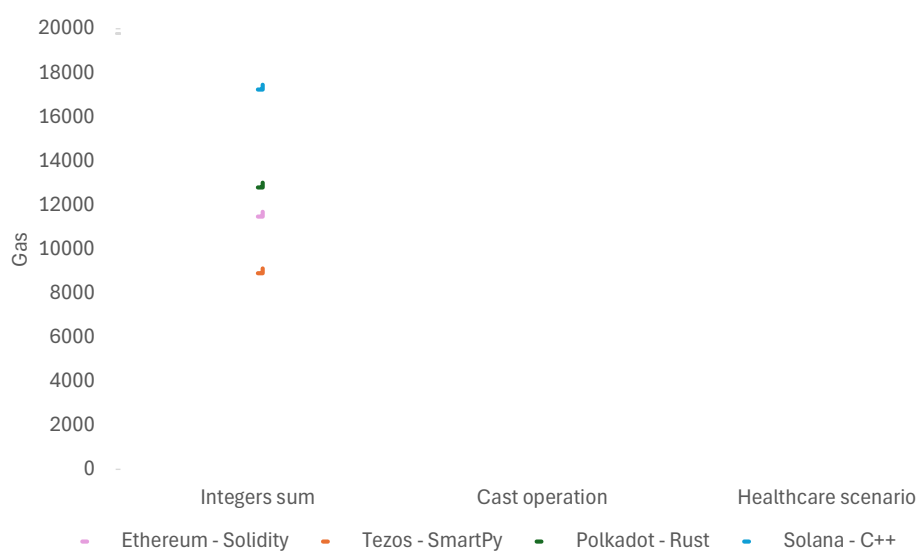


Figure 7.8: Gas spent for each Blockchain

7.4.6 Sustainability analysis

This section provides an examination of different Blockchain networks focusing on their yearly transaction volumes, energy usage, and the energy cost associated with each transaction.

Table 7.6 presents the results of the analysis. Numerous factors significantly impact all parameters, especially the consensus protocol, which, while based on PoS, has several variations affecting emissions. Power consumption figures fluctuate considerably, owing to the popularity of each Blockchain; increased usage leads to higher energy consumption. Correspondingly, CO2 emissions data can be inferred but vary greatly based on the energy sources powering the chain's nodes.

Thanks to official data gathered from different sources⁴, it is possible to create a graph regarding emissions per transaction, as shown in Fig. 7.9. Some values were instead calculated by knowing the number of transactions and the total estimated emission for the year 2022. A clear difference in ecological impact data can be observed.

Table 7.6: Analysis of CO2 emission for each analyzed Blockchain

Blockchain	Txs per year	Power consumption [GWh]	CO2 emission [kg]
Ethereum	4.9e10	7.210	2784143
Tezos	1,2e8	1.010	302461
Polkadot	3,1e6	0.473	122275
Solana	3,3e8	5.961	2228750

Tezos distinguishes itself as a Blockchain with reduced CO2 emissions. Its minimal carbon impact enables developers and users to focus on innovation while maintaining sustainability. Crafted for evolution through its on-chain governance, Tezos' efficiency is intentional. This adaptable design equips the Blockchain to meet future demands and evolve as per users' needs. Indeed, Tezos has boosted energy efficiency per transaction by at least 70%, with its energy consumption per transaction in 2021 estimated at less than 30% of that in 2020⁵. The analysis of Polkadot's resource use involved determining its daily transaction count via multiple block explorers and then computing a yearly average. This measurement encompasses transactions on both the relay-chain and parachains. Polkadot aims to support the forthcoming surge of web advancements while avoiding the significant energy requirements of traditional proof-of-work Blockchains. Its novel consensus mechanism requires only a minimal amount of energy compared to traditional Blockchains⁶.

Solana and Ethereum, the latest Blockchains, demonstrate nearly identical energy consumption rates. Ethereum has long scrutinized its energy usage, prompting a significant shift known as the 'Merge', where it altered its energy-heavy and high-carbon-emitting consensus mechanism from PoW to PoS. On the flip side, the Solana Foundation is devoted to assessing its Blockchain's impact, making its findings public, and taking steps to reduce its environmental footprint to zero. Solana distinguishes itself as the first Layer 1 smart contract Blockchain with ongoing energy emission tracking, allowing global access to network emission data right down to the validator or RPC specifics⁷.

⁴<https://etherscan.io/>, <https://indices.carbon-ratings.com/>, <https://greenpolkadot.io/>, <https://www.theblock.co/data/crypto-markets/spot>, <https://indices.carbon-ratings.com/>

⁵<https://tezos.com/carbon>

⁶<https://polkadot.network/features/technology>

⁷<https://solana.com/environment>

The in-depth analysis conducted on smart contract dynamics reveals a complex landscape where programming languages play a significant role, especially when it comes to low-level languages. These languages can directly influence the efficiency and optimization of operations performed by smart contracts on a Blockchain. Although they are faster, do not require compilers, and use minimal memory, they rely on external functionalities that compromise the final cost. Another significant contribution comes from the efficiency of the Blockchains on which smart contracts operate. Regarding the actual costs incurred for executing a smart contract on a Blockchain, these are still influenced by the Blockchain itself: governance policies and resources employed by the operating logic make prices vary significantly. The intrinsic characteristics of the Blockchain and the adopted consensus protocol play a predominant role in determining the environmental footprint. The decentralized and diversified nature of consensus protocols can substantially impact energy consumption and CO₂ emissions associated with smart contract execution. Although careful programming can contribute to optimizing smart contract efficiency, it is the fabric of the Blockchain itself and the consensus rules that predominantly influence carbon emissions.

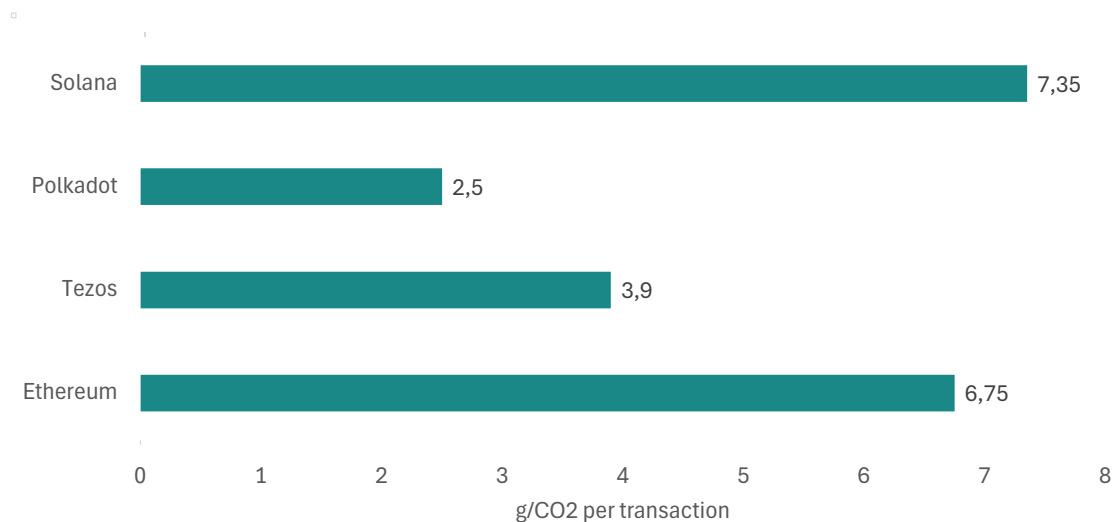


Figure 7.9: CO₂ emission per transaction for each analyzed Blockchain

In summary, while programming languages play a significant role in the internal optimization of smart contracts, the broader context of the Blockchain structure and the consensus protocol largely dictates the environmental impact of smart contract-related activities. Additionally, considerations must be made regarding the cryptocurrency market and its daily fluctuations, influenced by global stock markets. Prices and consumption are just some of the aspects to consider when developing a decentralized project or application. For a comprehensive overview,

perspectives on the project's Blockchain growth, upcoming implementations, and community support should also be evaluated to ensure foresight and backing from the community. Nearly all platforms analyzed, regardless of the programming language for smart contracts, are exploring and testing substantial changes to align with global emission reduction programs.

7.5 Reward-based Architecture

Cryptocurrencies are meant to generate a new kind of richness in an untrusted environment and without the need of a centralized third party. One way to generate new coins is through mining, as seen in Chapter 2: with the Proof-of-Work consensus protocol, miners can receive a reward in coins when they accomplish their goal, that is to find a correct hash for the new block. Nowadays, this procedure has become computationally expensive: if a user doesn't have enough computational power, he can not take benefits from the mining process. This paper aims to overcome the difficulties of starting from a non rich situation, thus spreading a meritocratic concept of a Blockchain network. In the proposed platform, all users start with the same initial amount of coins that can be used to buy goods and services from other users. In this way, the more the user sells his own services, the more he can obtain in terms of coins. All users start with the same purchasing power and it is responsibility of the single participant to stay alive in the network. No coins will be mined or be exchanged with real money.

7.5.1 Related work

The authors of paper [125] propose a novel economic system to exchange goods without the need of money, using Blockchain as the underlying technology. This proposal avoids the use of Proof-of-Work consensus protocol and is focalized on exchanging goods. However, it does not take into account the possibility to share services and to generate new forms of richness. Compared with this approach, our proposal aims to use coins that do not derive from mining but from offering someone's service. Decathlon brand has created a Blockchain-based rewards program. It was launched in March 2019 in some test nations (Slovenia, Croatia and Serbia) with the name of Decathlon Team. Here's an example of how the program works: A customer enters a Decathlon store to buy products, for example some football shoes. By the time she leaves the store, she can check her profile on the store app that runs on Blockchain on her smartphone to see how many medals (virtual coins) she has earned and the total number of medals credited to her account. As soon as she has enough medals, she can redeem some of her medals to receive a benefit, let's say, a two-hour lesson with a football instructor. That instructor earns the

medals from the customer and can spend them to buy football-related goods from a Decathlon store. This implementation is similar to our proposal, but, due to its industrial focus, it is based on spending real money to earn coins, so the starting point cannot be equal for anyone because it depends on how much money a customer can spend. This approach will not follow the main goal of the proposed platform, that is, no real money will be spent during the entire process.

7.5.2 System design

The main idea of our proposal is described hereby. The user who wants to join the Blockchain can register to the platform, using a username to guarantee the pseudonymity of the Blockchain. It is important to reach sybil resilience, so to use a mechanism to ensure that the same user will not create more than one account, otherwise he or she will get more coins than thought. A possible approach is to use a unique identifier such as the Social Security Number in America or the eIDAS ID in Europe [126], or by using the biometric techniques [127]. During the registration process, the user receives a certain amount of coins to start buying basic services. The coins available in the network depend on the number of users joining that network following the equation:

$$T = M * N = \sum_i c_i \quad (7.2)$$

where T is the total available coins in the platform, M the number of registered users, N the number of initial coins per user and C_i the coins of user i . The mean of coins per user will be equal to the number of starting coins in the platform. Fig. 7.10 shows a sample platform with $M = 10$ registered users, each one starting with $N = 100$ coins.

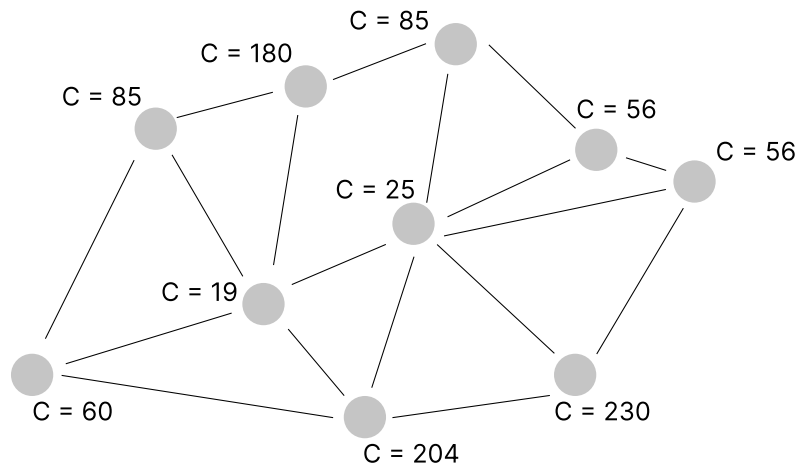


Figure 7.10: Network example with 10 nodes, each one starting with 100 coins

When a user buys a service, he or she makes a transaction in the chain that will be encrypted using the user's key. The transaction is then signed and sent to the network. Anyone can see that this transaction has been done and that the amount of coins needed for the service will be sent after the service is done. The user cannot buy or mine new coins, so his computational power has no effect on the network; he can instead sell some goods or services to earn new coins and buy new services. This mechanism can prevent rich users from increasing their wealth in a short time or users with expensive hardware platforms from becoming richer.

7.5.3 System analysis

A workflow sample is presented in Fig. 7.11. User A (the buyer) makes an offer on some good or service to User B (the seller). They can use an in-app text chat to communicate, make offers and counter offers, until they reach an agreement on the price (in coins) of the selected product. After the agreement, the seller makes a request to the app to make the transaction and sign it in the Blockchain platform. The app forwards the request to the Blockchain that uses some predefined smart contracts to execute the transaction and takes the defined amount of coins from the buyer. The result of the transaction is sent to the app and back to both the buyer and the seller. After that, User A receives the good or service, she/he can declare to the app that the transaction can be completed successfully. The app will communicate with the Blockchain that will release the taken coins and give them to the buyer. The transaction is now concluded and registered to the platform.

Ideally, participants in the network can also be the miners in the Blockchain; the more participants are in the network, the more the system becomes decentralized and, therefore, secure.

7.5.4 Economics considerations

From an economic point of view, some doubts could emerge on the value of a coin in the platform. Two main approaches have been identified to address this problem:

Stablecoin approach [128]. Stablecoins are cryptocurrencies that follow the real world market, so there is no risk of speculation and no alternative markets with prices that differ from a real world situation. These kind of coins exist in the Blockchain topic; the most well-known one is Tether, a coin mainly used for payments.

Self-leveling market approach. The more challenging way is to not impose a value on a platform coin, but to let people organize by themselves on how much a coin is worth. The market will stabilize by itself after a certain number of successful transactions: this approach will avoid to fix the price of a service (that is a consequence of fixing a starting value for a coin) and it will carry new results in

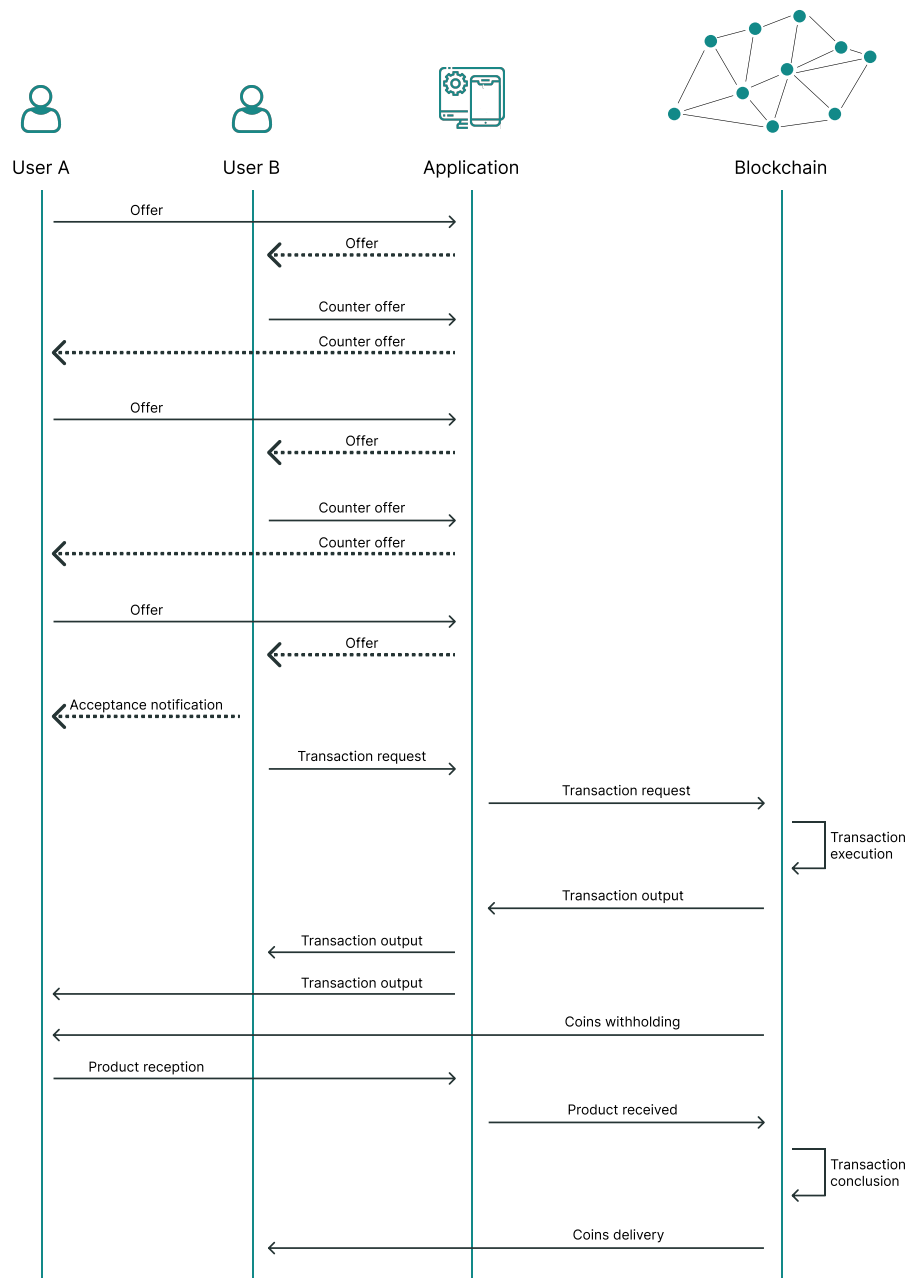


Figure 7.11: Workflow of the system

the market. This self-leveling market approach at a starting point will make people sell and buy under or overpriced services, anyway this situation has a drawback.

The stablecoin approach is the simpler and safer one, but it's less innovative and challenging than the second proposal. For this reason, it could be more interesting (and risky) to follow the second idea and analyze the market transformation as quickly as customers increase. Obviously, people could sell and buy under or overpriced services in a first time, but there always is a limit at this situation. For example, for the first two customers in the whole platform, every actor knows that the other one has a maximum amount of, let's say, 100 coins, so he would never try to sell a service for 100 coins or more, because it would be unacceptable by the other user.

From an economic point of view, the objective is to understand how the digital society will react to a kind of market similar to what was available centuries ago, when money did not have a fixed value. For this reason, validations will be analyzed after a certain number of transaction has happened in the developed platform.

7.6 Architecture proposal in a smart city

The rise of emerging technologies defines new and improved software processes. The modeling of an architecture is the first step to adapt a process based on specific needs defined by functional and non functional requirements. It is necessary to design some innovative approaches during the definition of the architecture to create a solid and scalable system. Among various innovative topics in Software Engineering, we focus on smart cities improvement. The smart city trend is constantly growing as new and emerging technologies help its spreading. A smart city goal is improving the quality of life for citizens, as well as making operations easier and more efficient. To make a smart city desirable, the network should be reliable and with high performances; moreover, privacy and encryption of data should be guaranteed and the concept of trust should be a solid foundation of the entire process.

A typical problem in smart cities development is modularity: new applications must be contextualized and developed having that smart city in mind. Actually, there are no standards and guidelines that can adapt to every smart city.

Our proposal is based on the use of Blockchain technology to improve our ability to develop, manage and apply new software and system applications for smart cities. To illustrate the main aim of this paper, let us consider a sample scenario: suppose we would develop a system that provides smart city services, using a single distributed database enabled for accessing city-related information for citizens. Traditional cities can become smart without using new systems, but simply interfacing with existing ones and with distributed databases used by other smart cities. Hence, as shown in Fig. 7.12, a smart city actor must have a single interface to

gather different data and to use the database; this means that the interface and the implementation of an object can vary independently being separated from one another. The implementation can be realized just once and be compliant to every other smart city that implements the proposed interface.

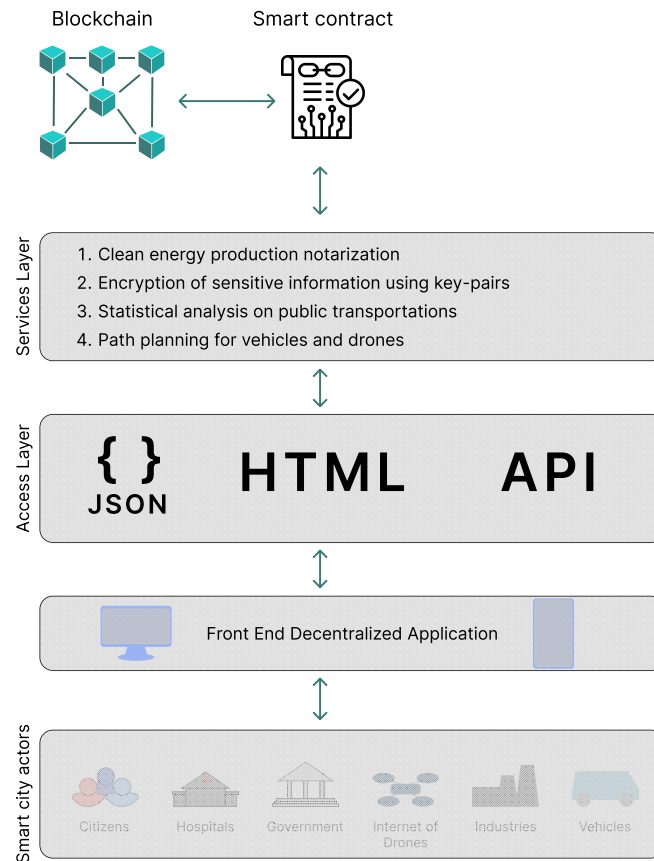


Figure 7.12: Layers of the system showing a single interface in the access layer

7.6.1 Related work

Different reviews show the role of Blockchain in smart cities, with some focus on smart healthcare, smart transportation, supply chains [129]. They also underline the combination of Blockchain and other technologies such as Internet of Things and Machine Learning [130]. Blockchain can help smart cities in being more sustainable thanks to its peculiarities: a) it is immutable, so every information added to the chain cannot be modified, b) it is anonymous, meaning that everyone can join the network without worrying about privacy, c) it is trustable even if people don't know each other.

Authors of paper [131] focus their research on Blockchain smart contracts in smart real estate. They propose a conceptual framework for the adoption of such topic in smart cities. The real estate process becomes more immersive and user-friendly, in line with Industry 4.0 requirements.

Blockchain can help smart cities development [132] both from performance and security sides. The distributed nature of this technology makes architectures more scalable and with less point of failures: as soon as one node is active, the entire network is up. Data sharing takes advantage of this approach: education, healthcare, buildings can communicate using a single common interface. Artificial Intelligence intervenes in data management and analysis [133]: deep learning techniques can enrich the green energy production [134, 135], while neural networks can improve road management [136].

Traceability characteristic of Blockchain is helpful for waste management [137] thanks to notarized documentation, compliance with laws and fleet management. It is also useful with respect to public emergency services [138]: it can help security workers to manage different anomalies, from fires to crimes. A state-of-the-art summary is shown in Table 7.7.

The analysis of such publications raises some open challenges: a) Sustainability is an important aspect in the topic of Blockchain applied to smart cities. It is the furthest research topic from most of the analyses [130]. b) There is the need of a single interface to the Blockchain, to create a bridge between different actors in the smart city and a single, common distributed database. c) Security and privacy should be underlined[139]: Blockchain preserves privacy and ensures that only authorized nodes can access sensitive information. d) Costs to deploy a complete Blockchain network in a smart city are not yet known. It is difficult to perform a cost prediction in the deployment of a Blockchain in a smart city [129]. e) Regulations are needed to correctly share information: smart contracts can come in hand in this topic.

This paper analyzes topics b) and c), solving them by creating a common interface to the Blockchain for different stakeholders and by analyzing the role of each stakeholder to grant access to sensitive data to the owner of those data.

Table 7.7: State of the art analysis

Paper	Topic
Xie (2019)[129]	Survey on the literature involving Blockchain technology applied to smart cities
Rejec (2022)[130]	Trends and research directions for Blockchain applied to smart cities
Ullah (2021)[131]	Usage of smart contracts in smart real estate environment
Shari (2022)[132]	Survey of Blockchain applications for data management in smart cities
Sharma (2021)[133]	Integration of Blockchain and Artificial Intelligence for sustainable smart cities
Ahmad (2021)[137]	Usage of Blockchain for waste management in smart cities
Kumar (2022)[138]	Protection of life and properties from fire damage in smart cities using Blockchain
Ghazal (2022)[139]	Protection of smart cities using Blockchain as a distributed database

7.6.2 Our approach

We envision a scenario in which Blockchain is the foundation of smart cities processes. Each process can be easily added to the system thanks to a common interface that embraces every aspect of the city. Information can be exchanged using JSON format, so the communication between a front end decentralized application and the Blockchain is context-aware. Blockchain technology has the potential to play an important role in the development of smart cities. It can provide multiple advantages in many topics:

- Supply chain management: Blockchain can be used to track goods and materials through a supply chain, thus increasing transparency and reducing the risk of fraud.
- Sustainability: Blockchain can be used to manage and track the use of renewable energy. A sustainable smart city can be obtained if actors reduce their carbon footprint and promote green approaches.
- Authentication and identification: Blockchain can be used to verify identities in a secure and decentralized way, making it easier for citizens to access services and participate in civic life.
- Public records: Blockchain can be used to store and manage public records, such as property titles or licenses.
- Transportation: Blockchain can be used to manage and track the use of public transportation, helping cities optimize their transportation systems and reduce congestion. Transports side, Blockchain can be used to gather information to improve paths, waiting times and overall services.

Overall, the role of Blockchain in smart cities management is to improve different aspects, from sustainability (i.e., notarization of clean energy production) to hijacking avoidance (i.e., guaranteeing the path of a bus or a taxi, making statistical analysis for public transports, identifying passengers). The ultimate goal is to improve quality of life for citizens.

7.6.3 Clean energy production

Smart buildings must be energy efficient and incorporate clean energy production technologies. The ways to accomplish this goal are different: a) solar panels can be installed on the roof of a building to capture sunlight and generate electricity, b) wind turbines can convert wind speed to electricity, c) storage systems, such as batteries, can store excess clean energy produced during low demand times. Blockchain technology can support the production of clean energy in multiple ways: a) it can

track and verify the energy production, to ensure that a building is sustainable; b) it can help the trading of energy, notarizing transactions between a building with enough energy in its storage and a building with less energy than requested; c) it can help people understand if a building is really sustainable and green (i.e., showing a building carbon footprint), thus letting people choose and prefer smarter and more efficient buildings.

7.6.4 Encryption of sensitive information

Citizens side, information should be encrypted to ensure privacy and anonymity. The encryption process can be both symmetric or asymmetric. In this proposal, we follow an asymmetric key encryption scheme, that takes advantage of the key-pair already present in every Blockchain architecture. In this way, everyone can encrypt any kind of message using the recipient public key, thus guaranteeing that only the recipient can decrypt the message using his or her own private key.

In the case of public services requests, it is possible to use smart contracts to make the process secure and transparent. The authentication and request process is shown in Fig. 7.13.

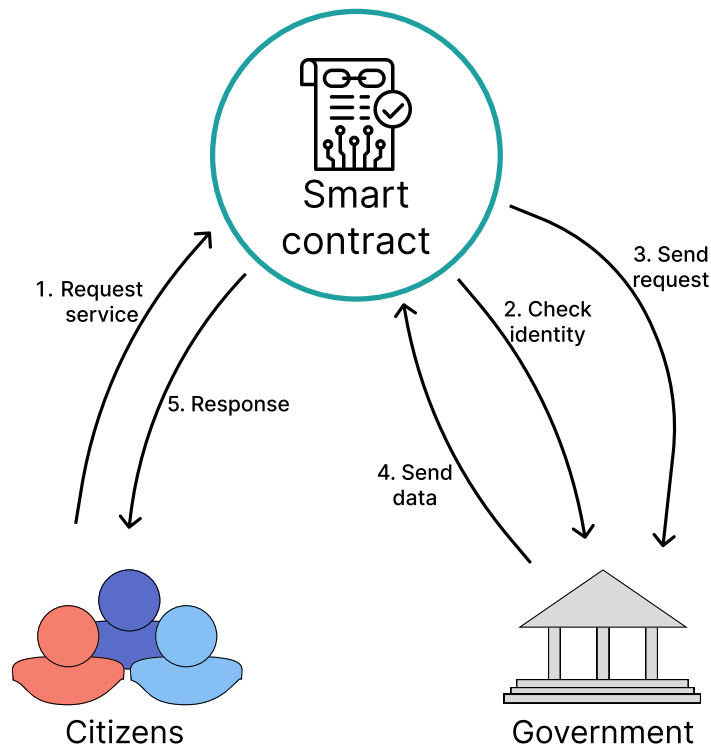


Figure 7.13: Sample process for a citizen requesting a service to government institutions

1. The citizen requests a service to the institution (i.e., a certificate of residence). The request is managed by a smart contract. It is also possible to directly upload documents to the InterPlanetary File System (IPFS) [140], but due to lack of regulations and laws, we decided to let institutions keep sensitive documents.
2. The smart contract, together with the institution, authenticates the citizen and ensures that the requested certificate is obtainable.
3. The smart contract requests the document to the institution.
4. The institution gives back the requested service using the same smart contract.
5. The citizen receives the requested service or document. The process, thanks to smart contracts intervention, is transparent, secure and fast.

7.6.5 Statistical analysis

The use of a distributed database such as Blockchain lets people read public records, that are stored in the chain and accessible to anyone. These data are stored anonymously, meaning that any information can be related to a public key (wallet), but there is no way to link that wallet to a person. In this way, data can be used to make some statistical analysis to understand how to improve services offered to citizens. Public transports can easily understand if there is a lack on the offer and improve it, knowing exactly where to act. Furthermore, the potential applications of statistical analysis extend beyond public transport. Other sectors, such as healthcare, energy, finance, and logistics, can leverage the insights gleaned from Blockchain-stored data to optimize their operations, identify trends, and develop innovative solutions. The possibilities are vast, as the Blockchain's transparent and secure infrastructure provides a solid foundation for making informed decisions based on reliable and unbiased data.

7.6.6 Path planning

The process of determining one optimal route for a vehicle to travel from one location to another is defined as path planning. This approach can be used to avoid traffic congestion in smart cities [141] or to quickly intervene in case of disasters [142]. Path planning can be used for vehicles, drones and people. With Blockchain technology, it is possible to avoid hijacking: in the Internet of Drones (IoD) field, various approaches have been proposed [143, 144, 145]. They all share a common point of view: everytime a drone approaches a new Point of Interest (PoI), it writes a new information on Blockchain to notarize its position. In this way, every attempt

of hijacking can be identified in short time. The same approach can be considered for Autonomous Guided Vehicles (AGVs) in a smart city: AGVs can read from the Blockchain where they have to go, then they can create an optimal path and notarize the time of arrival. These information can further be used for statistical analysis, as underlined before.

7.6.7 Proposed architecture

Our contribution regards the design of an architecture where every actor in a smart city can benefit from using Blockchain as a back end of the system. The main goal is the development of a common interface to communicate with the database, so everyone can join the network in a secure and fast way. Smart contracts can receive any kind of data in a JSON format: new actors just need to upload JSON-formatted information. Data are then managed by the contract, that gathers them and converts them into value, thus uploading them in the Blockchain. An architecture showing different actors is proposed in Fig. 7.14.

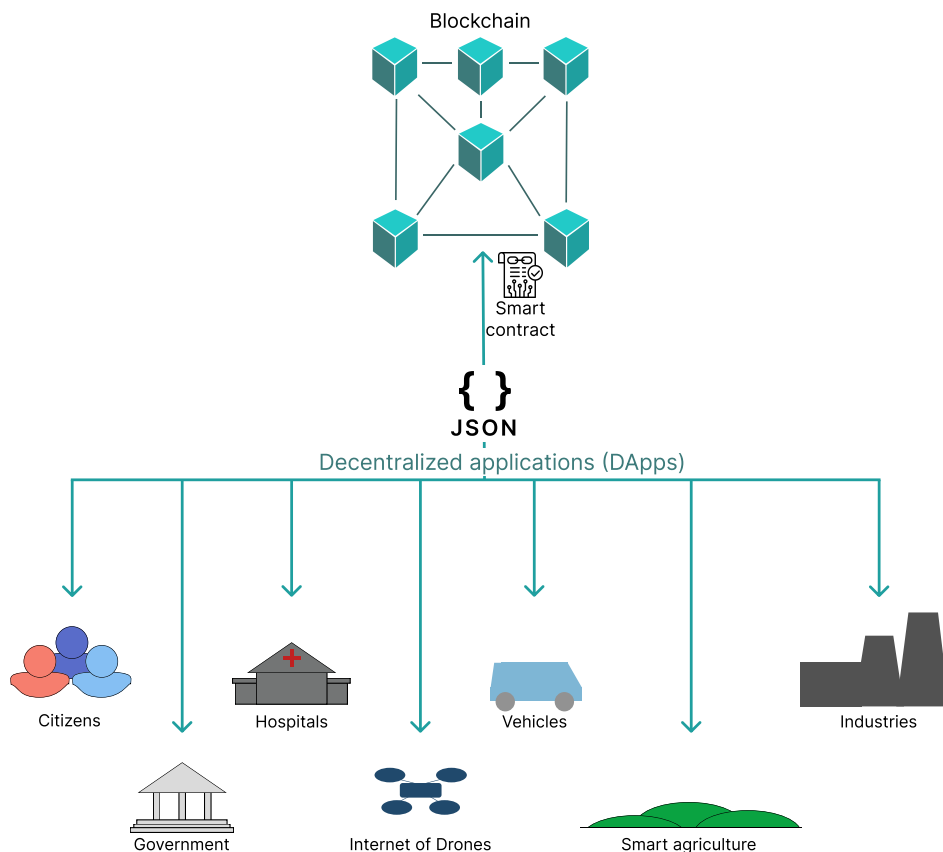


Figure 7.14: Architecture of the proposed Blockchain-based smart city

In our scenario, each actor uses a Decentralized Application (DApp) to connect to the Blockchain. DApps are designed to be distributed and to run on multiple nodes, rather than being controlled by a single entity. Some applications of such architecture can be summed up as follows:

- *A. Clean energy production.* To reach sustainability purposes, clean energy production can be notarized in Blockchain. Everyone can ensure that the energy used in a building comes from renewable sources.
- *B. Encryption of sensitive information.* Sensitive information can be encrypted using nodes key-pair. Autonomous shared vehicles (i.e., taxis) can use this sign to authenticate passengers and ensure that only the passenger who paid for the ride can use that vehicle.
- *C. Statistical analysis.* Public transportation can make statistical analysis (i.e., preferred destination, waiting times, etc.) to improve the offer, still guaranteeing anonymity.
- *D. Path planning.* Path planning is possible to avoid hijacking. In the Internet of Drones topic, this can be a useful approach to ensure that the path followed by a drone is correct and there is no tampering [146, 145].

Besides, every actor in the smart city can feel as part of a community, easily accessing any public information in the Blockchain and exchanging messages with other actors in a transparent way.

The architecture respects requirements for building a system process with modularity and scalability in mind, thus ensuring high performances and reliability that are guaranteed by the presence of Blockchain.

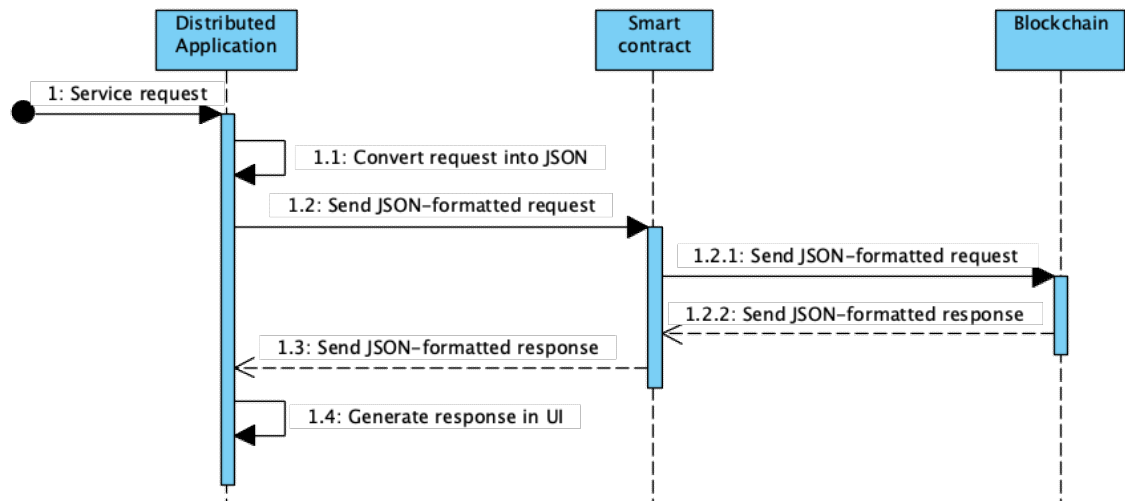


Figure 7.15: Sequence diagram for a smart city service request

To upload JSON information to the Blockchain, some context-aware smart contracts are designed. These smart contracts take the input, make some checks on the correctness of data and then upload them to the Blockchain. The specific front-end distributed application can manage the JSON output to show the information requested by the user. The described process is shown in Fig. 7.15: steps 1.2 to 1.3 are independent from the front-end distributed application.

Chapter 8

Additional technologies

As Blockchain platforms continue to evolve, integrating additional technologies has become crucial to enhancing functionality and expanding application areas. The conducted research explored these intersections across various fields. Section 8.1 investigates AR applications, while Section 8.2 examines the Metaverse’s role in digital tourism and education. Section 8.3 highlights the relevance of LLMs in code generation tasks.

8.1 Augmented Reality

The growing demand for products that are ethically sourced, eco-friendly, and safe has driven the growth of traceability systems. Consequently, industries have implemented advanced tracking solutions to oversee every production and distribution stage. At the forefront is Blockchain technology, whose decentralized and unchangeable ledger significantly enhances traceability systems by ensuring data integrity and transparency through the recording of each transaction and event in the supply chain. Although complex supply chains can create complicated data structures, posing challenges for consumers seeking clear insights, future end-users will increasingly engage with their environment immersively via Augmented Reality (AR) applications. Emerging headsets, like the Apple Vision Pro and Meta Quest Pro, are set to revolutionize everyday activities such as supermarket shopping. Presented at the IEEE VR 2024 conference [17], this paper investigates Blockchain-integrated traceability systems and uses AR to make these platforms more accessible. It allows consumers to scan a QR code and conveniently access the necessary traceability information in a visually optimized manner. The product is displayed to users with a 3D model that alters its shape based on specific quality metrics, boosting their trust in the manufacturer.

Augmented Reality is a transformative technology that overlays digital information, such as virtual objects or contextual data, onto the real world, enhancing

users' perception and interaction with surroundings. QR codes and markers have redefined AR interactions, while Blockchain technology assures data integrity and transparency. Integrating these technologies in AR enhances information dissemination and user engagement. The current literature lacks deep analysis on AR and Blockchain technology in the traceability field. Some architectures based on decentralized platforms have been proposed in different topics, from face-to-face collaboration using a web based XR framework [147] to the creation of virtual environments using Metaverse [148]. Blockchain and AR applications can be combined in various domains: education and training, advertising, tourism, virtual experiences [149]. The main contribution of the presented paper regards the possibility to give useful information about a product in an immersive way, giving consumers the possibility to scan a QR code and understand its quality simply by using their smartphone.

8.1.1 Architecture

The architecture of the platform is shown in Fig. 8.1. The consumer scans a QR code on the product label and the front-end distributed application sends a request to load the 3D model of the scanned product that is visualized in AR using Vuforia Engine. At the same time, a request is sent to the public Blockchain (through a smart contract) to access the traceability information regarding that product. The obtained data is shown to the consumer on top of the generated 3D model.

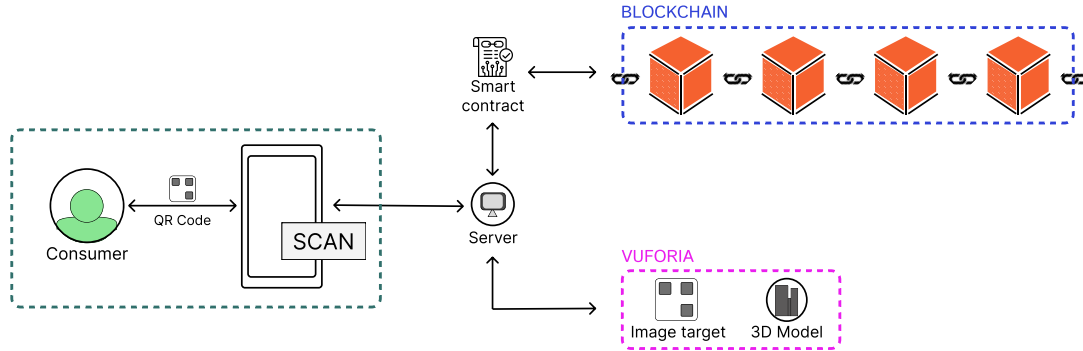


Figure 8.1: Architecture of the proposed platform

By using QR codes and Vuforia markers as entry points to Blockchain-hosted content, developers can ensure data security and immutability. Vuforia markers can initiate dynamic AR displays of Blockchain-verified information, while QR codes could lead users to transaction histories or supply chain details stored on the Blockchain. The combination of QR codes and Vuforia markers can happen in different ways. One approach is to insert a marker inside the QR code. Different tracking techniques can lead to this goal: Vuforia gives the opportunity to use a

VuMark that can be used to ensure a high number of feature points. However, this approach can lead to issues if two products are scanned simultaneously, because of the impossibility to distinguish between different products using the same marker. An alternative way is to directly use the QR code as a marker: it has lots of unique points and it can distinguish between two products. However, this scenario will require one QR code for each product uploaded in the Vuforia engine, so it could heavily affect the performance of the platform. The second scenario is chosen, due to the possibility to use Vuforia Cloud Recognition service to manage a huge number of image targets. Vuforia also grants the possibility to directly scan a QR code inside its environment using the Barcode Scanner service. This method is not compliant to the goal of the paper because it is limited to 2D objects, and it will not be possible to load 3D models on top of a scanned QR code.

8.1.2 Sample scenario

The platform has been tested in Unity. The sample scenario regards a traceability platform based on Blockchain technology, combining the benefits of both a public and a private Blockchain [4]. The platform must enable the general user to check the product origin, information, chemical-physical properties, and varietal origin [3]. Additionally, it must ensure that the product's agri-food chain is controlled and monitored by having access to data about the production phases, from seeding to selling, including all phases of any transformation. The project proposal specifically aims to experiment with the integration of Blockchain technology and, as a result, the real-time traceability of the information recorded on the history of the product.

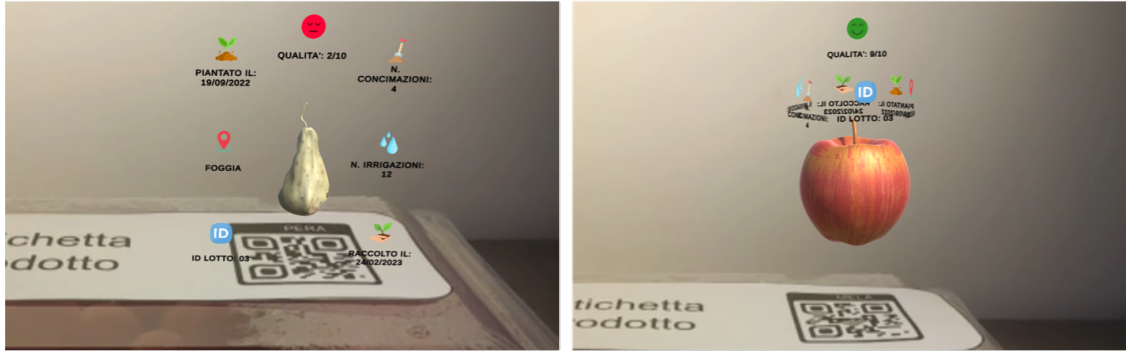


Figure 8.2: Two alternative graphical interfaces. (a) a pear, with quality 2/10, is surrounded by the attributes gathered from the Blockchain. (b) an apple, with quality 9/10, has its attributes rotating on top of it.

First results show that the platform correctly reads the required information and shows them to the final user, together with the product quality shown on top of the gathered data. Additionally, the product changes its shape by following the given quality: the higher the quality, the better it will be seen by the final

user. Fig. 8.2 shows two different ways to implement the graphical interface of the platform: one with fixed information around the product, all on the same plane; another one with animated information rotating on top of the product.

The increasing popularity of traceability systems in supply chains reflects the evolution of consumer expectations towards transparency and ethical consumption. Blockchain's integration in these systems brings immutable records and heightened trust. However, the challenge of enabling easy access to and comprehension of product information for consumers remains hard to accomplish. The possibility to use AR techniques helps in bridging this gap, giving consumers the possibility to easily read information thanks to immersive interfaces and platforms.

8.2 Metaverse

The metaverse is frequently characterized as the internet's successor, in which users can interact with each other and with digital objects in three dimensions rather than simply browsing websites or using social media platforms. It provides a variety of new opportunities for entertainment, social interaction, education, and commerce, thank to its direct effect on users satisfaction [150]. Between the different applications of metaverse, we want to focus on smart cities and in particular smart tourism.

Authors of paper [151] raise three main questions with respect to the application of metaverse in tourism area: what could be the staging experiences in the metaverse, how consumers behavior will change, and what business strategies can be developed in this approach. A metaverse tourism ecosystem is defined in [152]: travelers and suppliers are connected in both the digital and the physical world. The metaverse can provide mirror worlds to virtualize real life experiences. The technology most linked to tourism and metaverse topic is Mixed Reality (MR) [153], in particular in the topic of visiting cultural heritage. MR helps Generation Z people to feel more involved in tourism, creating more engaging adventures from industries.

Our proposal aims to develop a metaverse platform to support tourism in Apulia, Italy. In particular, we take advantage of MR technology to let tourists visit Bari, an Apulian city, discovering cultural places and activities. Suppliers can also join this platform to recreate their activities and sponsor them to the public, creating more engagement in visitors. Finally, touristic guides can use their avatar to easily connect to tourists and let them discover the city in a new and entertaining way.

Our scenario

Our scenario is explained below. The back-end of the architecture is a metaverse platform that allows sharing three-dimensional spaces, usable by different users in real time via devices such as computers, smartphones and virtual reality headsets.



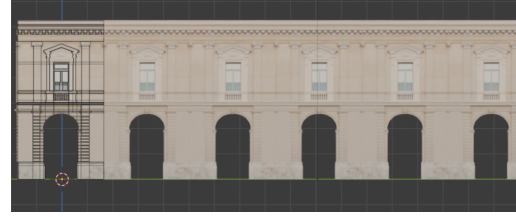
(a) Real photo of Piazza del Ferrarese



(b) Intermediate phase, without textures



(c) Final phase, with textures and details



(d) Detail of a building

Figure 8.3: Development steps for the metaverse platform

The front-end is an immersive virtual space, built with 3D graphics programs and then programmed and loaded into the metaverse. The environment is programmed to possess precise details of real environments, with the addition of extra information elements such as texts, graphics or completely additional 3D objects, available to users under certain conditions to enhance their experience.

Users accessing the platform are either consumers and providers. Consumers are visitors of the platform: they enter the space, attracted by an event inside the platform and then become intrigued by the reproduction of the real space. Furthermore, they have the opportunity to learn and increase their knowledge of the place in an organic way thanks to extra information elements present in the space for advertising, decorative and informative purposes. Providers create the three-dimensional reproduction of the space, and focus on populating the space by organizing cultural themed events in it, promoting the place of interest with exhibitions, historical anecdotes and details interesting geographical locations, thus ensuring the loyalty of passing visitors. Examples of providers are:

- **Touristic guides** who could get in touch with potential tourists and visitors directly from the virtual space, thus following them in detail on any potential question or curiosity.
- **Commercial activities** present in the virtual reproduction of the real world, such as a bar or restaurant, which could have special conventions for those who complete certain challenges inside the space [154, 155] or use the advertising space in the classic way.
- **Cultural promotion associations** could use virtual spaces to promote a municipality or locality far beyond its territorial borders, easily reaching the

international scale but without sacrificing real events held in presence. This approach guarantees an hybridization of real activities with virtual ones via VR headsets [156].

Implementation design

Various steps of implementation are proposed in Fig. 8.3, from the real photo of Piazza del Ferrarese in Bari (Fig. 8.3a) to an intermediate representation of the location (Fig. 8.3b), to the final implementation (Fig. 8.3c). The manufacturing process consists in taking a series of photographs so that the geometry of the object is centered and as straight as possible. We import the image as a plane in Blender¹ and, with the edge looping technique, we underline the salient reliefs of the photograph which are then extruded. To optimize structures with a repeated pattern, an array is used as shown in Fig. 8.3d. Preliminary results show a complete platform in the metaverse to explore with or without an headset, thanks to the characteristics of the chosen back-end platform, Spatial².

The proposed project will bring a great impact to the tourism market, which has always been looking for new innovative ways to attract the attention of millions of potential tourists every day via web-based social platforms. The main issue with such approaches was the lack of social and human aspects, such as the sociability between people and the sense of discovery. Users who discover a place through a virtual experience, whether it is actually existing or not, can reach a level of immersion that generates true memories equal to those of a visit to a real place. Furthermore, this experience has the additional element of sociality, which allows people in the same space to meet and make friends, chat and therefore encourage networking.

8.3 Large Language Models

Generative AI is a type of artificial intelligence that includes various techniques and models used to generate data or content. These models can create new content from scratch, often without the need for direct human input or based on specific prompts. LLMs, on the other hand, are a type of Generative AI that uses Neural Networks trained on vast amounts of textual data from different sources, such as online blogs, code repositories, open data, and media content. Their training aims to enable them to understand and produce human language. In November of 2022,

¹<https://www.blender.org>

²<https://www.spatial.io>

a sophisticated chatbot called ChatGPT³ was launched. Developed by OpenAI⁴, the chatbot utilizes advanced deep learning algorithms to generate human-like responses to natural language inputs. The model has been trained on a vast and diverse dataset of text and is capable of comprehending and generating text on various topics. ChatGPT's versatile capabilities make it a suitable solution for several applications, including customer service, content creation, and language translation. Since its release, ChatGPT's popularity has grown exponentially, surpassing even the likes of TikTok, the current record-holder⁵. Within two months of its launch, ChatGPT boasts an impressive user base of 100 million. ChatGPT's success moves the discussion on the LLM and their ability.

In this paper we review all existing work about LLMs used to generate code and programs. This is a first step towards the development of an LLM to automatically generate smart contracts in Blockchain platforms.

8.3.1 Background

Generative AI is a broad category of artificial intelligence that encompasses various techniques and models designed to generate data or content [157]. These models are capable of creating new content from scratch, often without direct human input or based on specific prompts. LLMs are a subset of Generative AI: they are Neural Networks trained on vast amounts of textual data, gathered from different sources, from online blogs to code repositories, from open data to media content. Their training aims to let them understand and generate human language. These models have demonstrated remarkable capabilities in a wide range of natural language processing tasks, including text generation [158], translation [159], summarization [160], and more. They can be considered as an evolution of chatbots [161], born in 1966 with ELIZA [162], a computer-based psychotherapist answering user's questions.

A survey conducted by [163] shows the evolution of LLMs, starting from GPT-1 in 2018. The diffusion of different LLMs starts at the end of 2022, with different producers showing their products. Fig. 8.4 shows the distribution of LLMs divided by producers.

Their interest grew exponentially after the born of ChatGPT on November 2022, the first application of LLMs open to public domain. A research on Google Trends confirms this trend, as shown in Fig. 8.5.

³<https://chat.openai.com>

⁴<https://openai.com>

⁵<https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note>

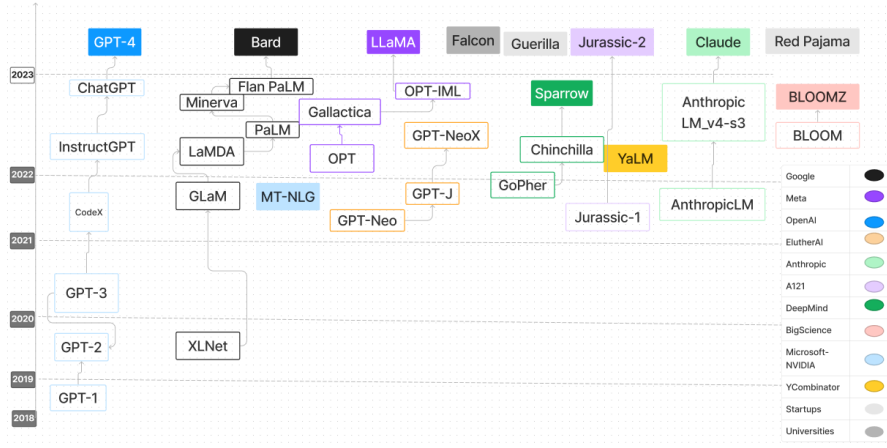


Figure 8.4: LLMs evolution until 2023

ChatGPT is based on the Generative Pre-trained Transformer (GPT) architecture, where a model is trained with high amounts of data and can be fine-tuned for different application. Different kinds of Large Language Models exist, such as Bidirectional Encoder Representations from Transformers (BERT), developed by Google. This approach is suitable for tasks requiring an understanding of context. XLNet is another LLM that improves the Transformer-XL architecture, incorporating a permutation-based training approach [164].

The interaction with a LLM can happen in different ways, from a chatbot-based style to the usage of Application Programming Interfaces (APIs). They can also be used in online platforms or run locally in the user computer. ChatGPT Plus [165] is a subscription-based chatbot that supports OpenAI's GPT-4 model. It offers both a chatbot to talk to and APIs to develop a custom platform. It also allows the user to upload and work on multimedia files instead of simple text. Local implementations such as GPT4All [166], LocalAI [167], and Ollama [168] require no GPU or active internet connection. They can be used both as a chatbot to interact with or an endpoint for API calls. They support a variety of models, including LLaMa 2 and its variations, gpt-3.5-turbo, BERT and more.

8.3.2 Related work

A state-of-the-art analysis revealed that literature presents few reviews related to LLMs. Authors of paper [169] show the potentialities of ChatGPT in reflective writing within university courses. They evaluate the ability of ChatGPT to produce diverse reflective responses using nine prompting strategies. The findings suggest that ChatGPT can generate high-quality reflective responses, outperforming student-written reflections across various assessment criteria. The work presented in [170] explores the reasoning capacity of LLMs like GPT-3.5, GPT-4, and BARD. The paper highlights the limited proficiency of all three models in tasks involving

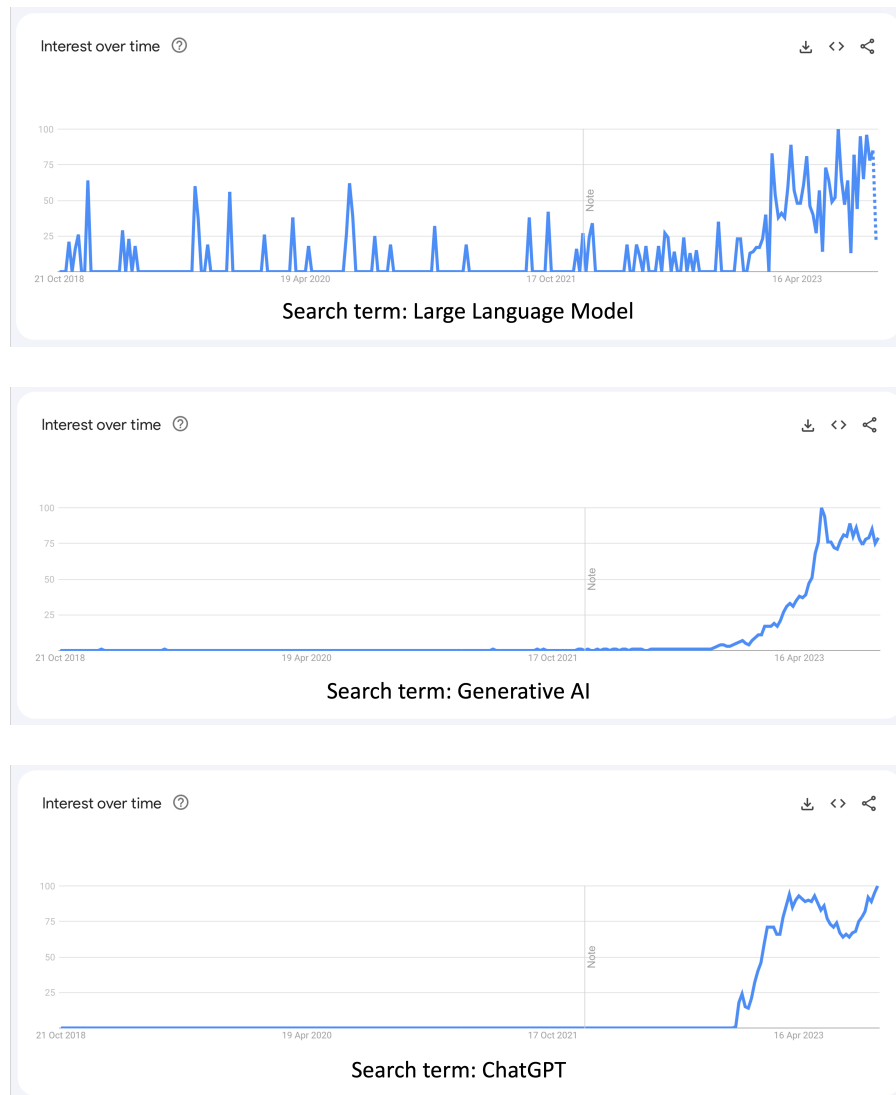


Figure 8.5: Evolution of interest in Generative AI related to the appearance of ChatGPT

Inductive, Mathematical, and Multi-hop Reasoning. To enhance zero-shot performance, the study proposes a set of engineered prompts for all three models, providing a detailed and comprehensive analysis of the results. The opinion paper presented in [171] provides a multi-disciplinary exploration of the applications, opportunities, challenges, and impacts of transformative AI tools like ChatGPT. Drawing insights from 43 contributors across diverse fields, including computer science, marketing, education, and nursing, the article acknowledges the potential for ChatGPT to enhance productivity in various industries. It highlights both positive aspects, such as gains in banking, hospitality, and IT, and concerns, including disruptions, privacy threats, biases, and misuse. The main thematic areas for further research are identified in knowledge, transparency and scholarly research. The study proposed in [172] employs a scalable crowdsourcing data-driven framework to investigate ChatGPT's code generation performance from diverse perspectives across social media platforms. The analysis reveals that ChatGPT is utilized in over 10 programming languages, with Python and JavaScript being the most popular, for tasks ranging from code debugging to interview preparation. The dominant emotion associated with ChatGPT's code generation is fear, overshadowing other emotions.

To our knowledge, there are no reviews investigating how LLMs are effectively used in the code generation domain, together with some insights on the preferred programming languages and the limitations versus benefits analysis.

8.3.3 Research Methodology

We follow the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [173] to perform the proposed review. It is composed of different steps: definition of Research Questions, gathering and filtering process through inclusion and exclusion criteria, and graphical and textual findings and discussion. The steps performed to reach the final number of papers are shown in Fig. 8.6.

This review aims to identify the state-of-the-art on performing code generation tasks using a LLM, as well as to highlight the trend of this research field and research gaps to work on. To accomplish this, we develop the following Research Questions (RQs):

- **RQ1: What is the trend topic of LLM used for code generation, starting from 2021?**

The goal of this question is to understand the evolution during years of the analyzed topic.

- **RQ2: What is the overall performance in accomplishing the code generation task?**

This question aims to understand how LLMs are used in the topic of code

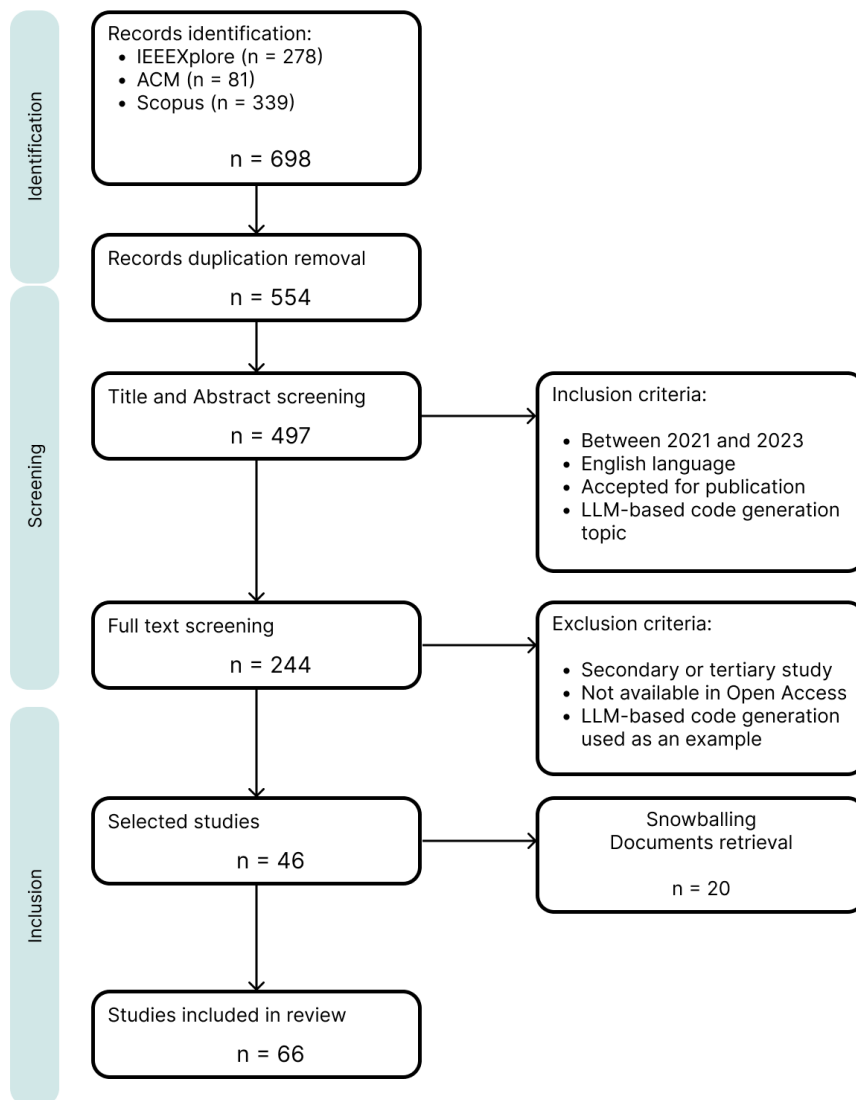


Figure 8.6: PRISMA methodology

generation, if they perform well in different operations (i.e.: identifying bugs, understand programming languages syntax, and more), and what model can perform better between the ones available online.

- **RQ3: What programming languages are used in current research?**
This RQ analyzes the topic from the programming languages point of view. It aims to understand which languages are preferred and why.
- **RQ4: What is the gap between benefits and constraints of using an LLM to perform automatic code generation?**
The purpose of this RQ is to investigate current open problems and identify research gaps and trends.

To ensure reliability and completeness of the review, we screened relevant research databases. A PICO (Population, Intervention, Comparison, Outcomes) technique is pursued to find the research string [174].

((Generative AND ai) OR llm OR (Large AND Language AND (Model OR Models))) AND code generation

The papers gathered from different databases, such as IEEEExplore, ACM, Google Scholar, Scopus, is 698.

The definition of inclusion and exclusion criteria helps in defining which studies will be analyzed to answer the defined RQs. In this work, inclusion criteria include:

- Publication date between 2021 and 2023.
- Publication written in English.
- Publication focused on the code generation topic through LLMs.

Exclusion criteria are presented below:

- Secondary or tertiary study.
- Publication not accepted in a conference, journal or book.
- Publication where the analyzed topic is used only as an example.

The obtained number of papers after the application of the explained criteria is 66. This is considered an acceptable number for our purposes.

8.3.4 Results and discussion

This section highlights the main findings obtained from the papers analysis and divided by the RQs defined above.

RQ1: What is the trend topic of LLM used for code generation, starting from 2021?

Fig. 8.7 shows the papers distribution on a month basis, from 2021 to 2023. A concentration of these papers starts from April 2023: this is an expected result, because of the born of ChatGPT as mass-use tool in November 2022. The highest number of occurrences happens between August and October 2023, then there is a slight reduction of occurrences. The waning focus on research dedicated solely to code generation tasks within the domain of LLMs may be attributed, in part, to the broader versatility and applicability of these models across a spectrum of computational tasks. The advent of LLMs heralded a paradigm shift in Artificial Intelligence research, captivating scholars with their potential to revolutionize numerous domains beyond code generation. Moreover, there are some already optimized tools for code generation tasks, starting from ChatGPT itself. In particular, the version powered by gpt-4 model performs very well in the Python language domain [175]. There exist also other industrial ready tools to generate code, like fine-tuned LLMs such as WizardCoder or CodeLlama ⁶.

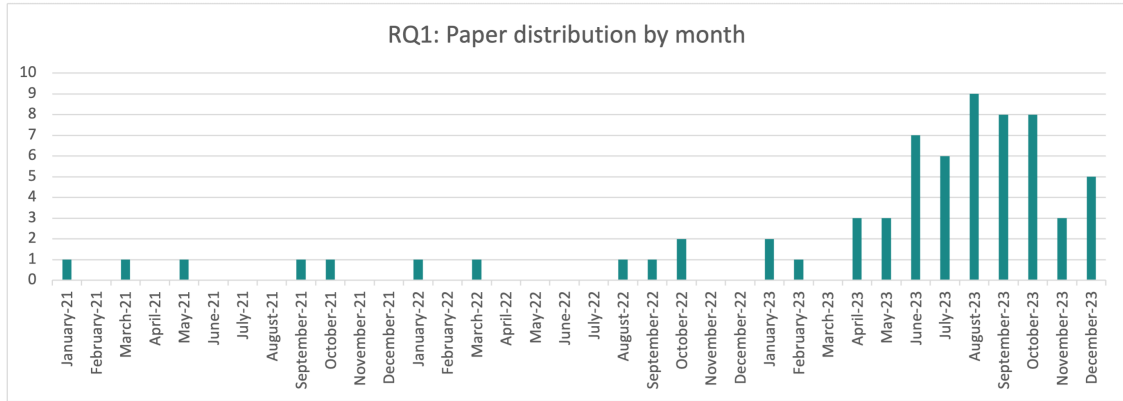


Figure 8.7: Papers distribution by month between 2021 and 2023

The graph proposed in Fig. 8.8 distinguishes between conference papers, journal articles or book sections. Journal articles cover about 85% of the considered papers: this is attributable to the choice not to include papers not available in open access among the exclusion criteria. It is important to underline that among the papers considered in the first collection, most of these were only in preprint format, therefore not yet published. This large number of preprints is a symptom of a research context that is still young and constantly growing.

The journal with the highest number of occurrences is Elsevier Computers and Education: Artificial Intelligence with 6 papers, followed by IEEE Software. Other international journals appear with one paper each.

⁶<https://huggingface.co/spaces/mike-ravkine/can-ai-code-results>

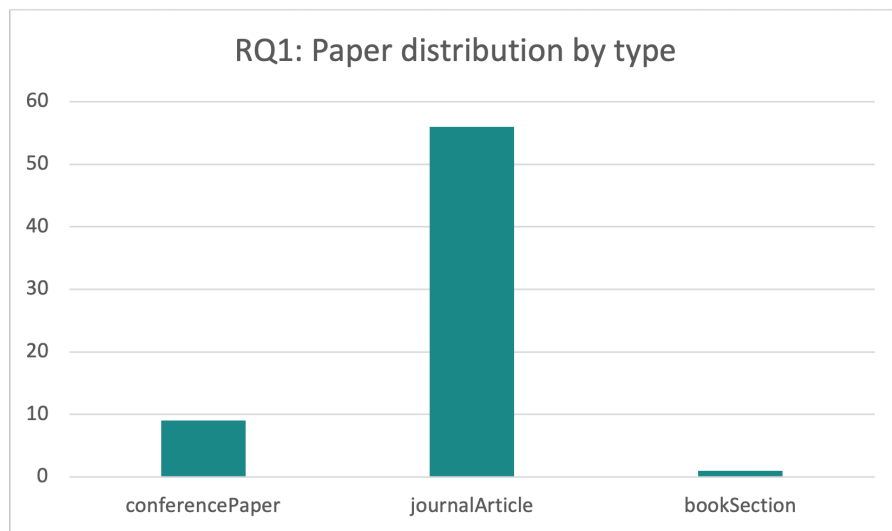


Figure 8.8: Papers distribution by type

RQ2: What is the overall performance in accomplishing the code generation task?

The second RQ is focused on understanding if papers evaluate the code generation task and the performances they achieve. Main findings are summarized in Fig. 8.9. 33% of the analyzed papers experiment with LLMs on different tasks, exploring how the intervention of Generative AI helps humans and their output. Some examples are given below:

- Paper [176] presents a crowdsourcing data-driven framework to investigate ChatGPT's code generation performance by analyzing social media data, revealing insights into its usage across programming languages, tasks, and emotional associations, and releasing a dataset for evaluating the quality of generated code.
- Paper [177] presents an innovative approach using a generative adversarial network (GAN) to enhance both code generation and code search techniques in software engineering. By treating code generation and code search as the generator and discriminator in the GAN framework, the study showcases consistent performance improvements across eight different settings.
- Paper [178] assesses the impact of ChatGPT, specifically GPT-4, on digital forensics through a series of experiments across various use cases such as artefact understanding, evidence searching, code generation, anomaly detection, incident response, and education. It evaluates the strengths, risks, and potential applications of ChatGPT in digital forensics. While acknowledging potential low-risk applications, the paper emphasizes limitations due to the need to upload evidence and the requirement for substantial topic knowledge to identify errors. It suggests that, with appropriate expertise, ChatGPT could serve as a supporting tool in certain circumstances.
- Paper [179] explores the utilization of GPT-4 for generating Governance, Risk, and Compliance (GRC) policies aimed at deterring and mitigating ransomware attacks involving data exfiltration. The research compares the efficacy, efficiency, comprehensiveness, and ethical adherence of GPT-generated policies against those formulated by established security vendors and government cybersecurity agencies. Results showcase instances where GPT-generated policies outperform human-generated ones, particularly when tailored input prompts are provided. Recommendations for corporate adoption of GPT in GRC policy-making are offered based on these findings.

A relevant number of papers talk about ethical implications of using LLMs in generating code or text.

- Paper [180] explores the future relevance of traditional programming languages in end-user programming among the rise of generative AI models, proposing the 'generative shift hypothesis' that anticipates qualitative and quantitative expansions in end-user programming facilitated by generative AI.
- Paper [181] reviews the evolution of software development processes concerning the appropriate targeting of automation to overcome obstacles. It recommends adopting a similar approach in integrating generative AI tools into the software development community.
- Paper [182] explores the transformative potential and risks of large language models (LLMs) in software engineering tasks, pondering the implications of AI-generated content and its impact on professionals in various domains.

A less relevant number of papers focus on implementing new platforms other than experimenting with an existing or a new fine-tuned model, on validating an existing search or on proposing new approaches. We expect this last category to be higher in other fields and not in code generation, because of the focus, by researchers, on better understanding the syntax and best practices for different programming languages and not on proposals on new programming languages or on new approaches on code understanding and documentation. The inclination towards established languages could also be practical in terms of applicability. Enhancing existing languages and their documentation aligns with real-world needs, facilitating better developer tools, code readability, and comprehension.

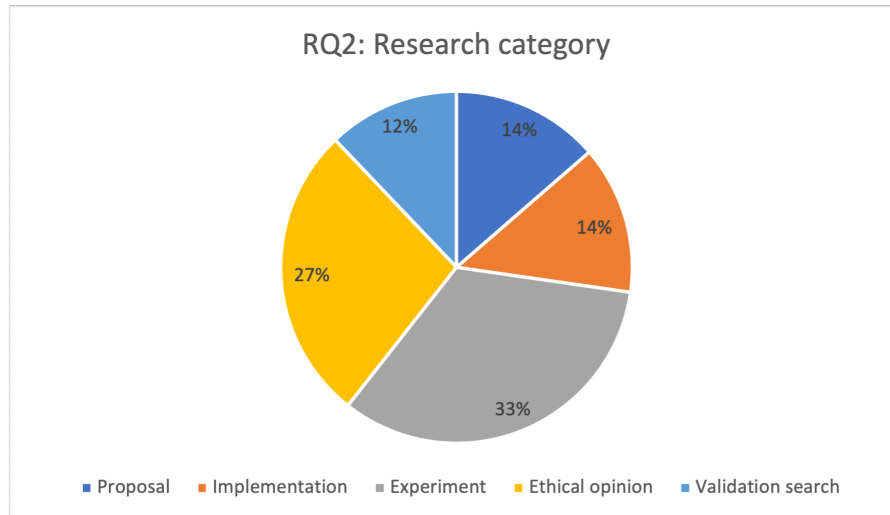


Figure 8.9: Papers divided by research category

Fig. 8.10 shows the value that each paper carries to the community in the analyzed field: software development if the paper develops new tools (3%), bibliometric

if the paper just makes an overview of already available platforms (3%), reliability if the paper considers the reliability of the generated code (7%), technology if the paper focuses on analyzing the topic and how LLMs can help in code generation tasks (50%), quality if the paper is based on the quality of the developed code (27%), performance if the paper focuses on how the LLM performs in accomplishing the required task (2%), business analysis if there are economic considerations (6%), architecture if the paper relies on modeling a new software architecture (2%). The distribution of topics within papers reflects varying priorities and interests within the research community. The focus on technology follows the foundational drive to innovate and refine the technical capabilities of these models. Given the rapid evolution of LLMs, researchers are often driven to explore new techniques, optimization strategies, and model architectures to enhance their efficiency, accuracy, and versatility across different tasks such as code generation. The emphasis on quality in a significant portion of papers aligns with the goal of ensuring robustness and efficacy of code generated by these models. Quality considerations encompass factors such as code correctness, readability, maintainability, and adherence to coding standards. This focus on quality reflects the practical need to ensure that the code produced by these models meets industry standards and is usable in real-world scenarios.

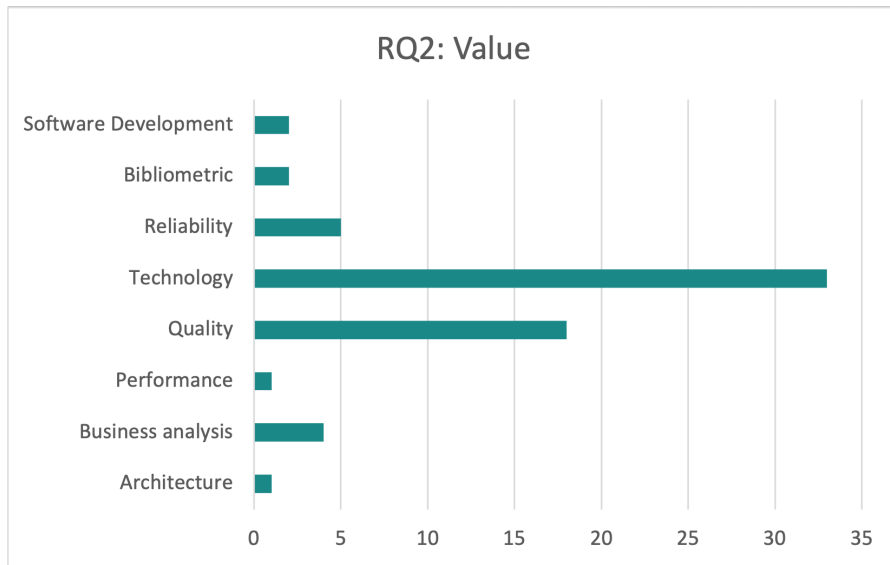


Figure 8.10: Papers divided by value added to the community

Fig. 8.11 shows the application area a paper falls into. 26% of papers belong to the education area, suggesting an interest in using LLMs for code generation tasks in classes for multiple reasons: creation of online learning environments and quizzes [183], analysis of how academy will react to LLMs [184, 185], classification between student-generated and ChatGPT-generated text and comments [186, 187], and analysis on the impact of using ChatGPT in programming

education on students' computational thinking skills, programming self-efficacy, and motivation [188].

Software Engineering comes at second place; this is an expected result, due to the fact that research on LLMs is constrained on code generation tasks, that strictly belong to the Software Engineering field: transforming ChatGPT into a low-code developer [189], generating commit messages through contextual information in repositories [190], analyzing LLMs software modeling capabilities and consistency issues [191], and exploring the potential impact of generative AI technologies like ChatGPT on the Software Development Lifecycle (SDLC) [192]. Healthcare is also popular in this kind of research: LLMs are used for making diagnoses of low- and medium-risk diseases based solely on symptoms [193], for offering reliable suggestions and treatment options to patients [194] and in general for supporting healthcare communication research [195].

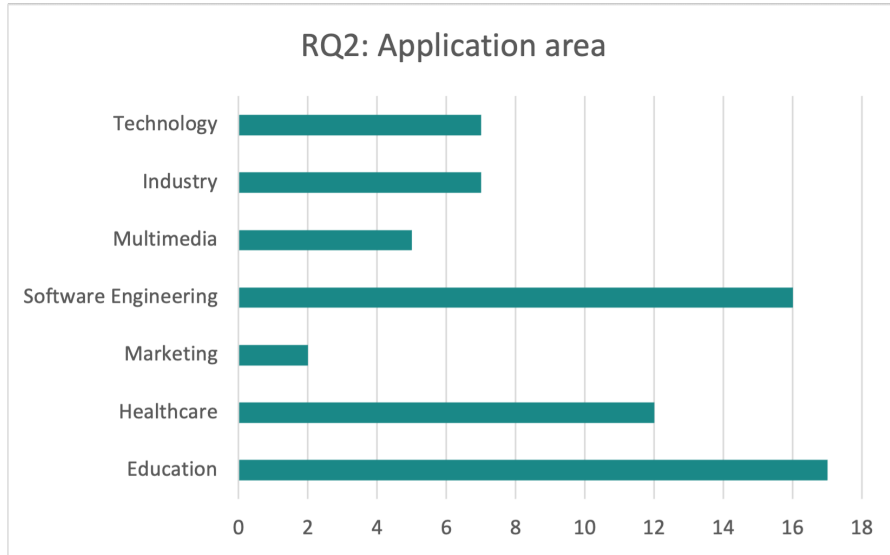


Figure 8.11: Papers divided by main application area

RQ3: What programming languages are used in current research?

An analysis on the preferred programming language used to conduct the research is also conducted. Only a small number of papers explicitly mentions the programming languages used within the research for code generation tasks. Python's prevalence among the discussed languages in these papers might reflect its widespread adoption in the field of machine learning and natural language processing, making it a natural choice for implementing and experimenting with large language models. The absence of explicit mention of programming languages in the majority of the papers might indicate that researchers focus more on the methodologies, or algorithms applied to code generation tasks rather than the specific code generation.

Results are shown in Table 8.1.

Table 8.1: Programming languages analyzed in relevant papers

Programming Language	Paper	Description
Python	[196]	Introduces LEVER, a method enhancing language-to-code generation by training verifiers to assess generated programs based on natural language input, the code, and execution results. It consistently improves code LLMs across table QA, math QA, and basic Python programming datasets, achieving state-of-the-art results.
	[177]	Presents an innovative approach utilizing a generative adversarial network (GAN) to enhance both code generation and code search techniques in software engineering. By treating code generation and code search as the generator and discriminator in the GAN framework, the study showcases consistent performance improvements across eight different settings.
	[197]	Introduces CODEGEN, an open large language model for code synthesis, trained on natural language and programming language data, facilitating program generation from problem specifications. Additionally, it introduces the JAXFORMER training library and demonstrates CODEGEN’s competitiveness in Python code generation through HumanEval and investigates multi-turn prompts for improved program synthesis using the Multi-Turn Programming Benchmark (MTPB).

	[198]	Introduces IntelliCode Compose, a multi-lingual code completion tool leveraging a generative transformer model trained on extensive source code data. It predicts sequences of code tokens for various languages like Python, C#, JavaScript, and TypeScript, achieving high edit similarity and low perplexity for Python programming.
JavaScript	[199]	Explores the application of the GPT-2 model for Automated Program Repair (APR) in JavaScript. It fine-tunes the model with JS code snippets to automatically fix JavaScript bugs, achieving an overall accuracy of up to 17.25% but facing challenges in generating effective bug-fixes in certain cases.
Multiple	[200]	The paper introduces DCServCG, a Data-Centric Service Code Generation model aimed at enhancing web service-based systems by capturing and utilizing service usage information from public repositories that share Open Source Software (OSS). DCServCG improves code generators by focusing on service-based code characteristics and addressing sequence overlap and bias issues through a data-centric concept employing conditional text generation. The evaluation demonstrates improved language modeling metrics, indicating reduced perplexity and better generalization performance compared to traditional models like ServCG.
	[201]	Explores the capabilities of large language models, using OpenAI Codex, in generating programming exercises and code explanations for programming courses, evaluating the quality and novelty of the generated content both qualitatively and quantitatively.

[176]	Presents a crowdsourcing data-driven framework to investigate ChatGPT's code generation performance by analyzing social media data, revealing insights into its usage across programming languages, tasks, and emotional associations, and releasing a dataset for evaluating the quality of generated code.
-------	--

RQ4: What is the gap between benefits and constraints of using an LLM to perform automatic code generation?

The last RQ is focused on understanding the advantages and the problems of using LLM for code generation. In Table 8.2, we discuss it according to the analyzed papers.

Table 8.2: Pros and cons according to the analyzed papers

Paper	Discussion
[200]	It improves the accuracy of code generation for web service-based systems by using service usage data from open-source software repositories. It tackles issues related to sequence overlap and bias by generating data-based text. The resulting model performs better generalization than traditional models like ServCG, as demonstrated by improved perplexity metrics.
[202], [201], [203], [204]	The study emphasizes the role of ChatGPT as an educational tool in design processes, highlighting its benefits in creating interactive learning environments, including automated grading, personalized learning experiences, language lessons, and customized content creation. However, it also emphasizes the limitations of solely relying on ChatGPT and stresses the importance of combining it with manual calculations and established simulation software to validate engineering results. It is crucial to be cautious of potential biases in content generation and to curate educational materials carefully. The challenge is balancing the advantages of ChatGPT with responsible curation to ensure that the educational content is free of bias.

Table 8.2 – continued from previous page

Paper	Discussion
[194], [205], [195], [206], [207], [208], [209]	They acknowledge ChatGPT’s effectiveness in various NLP tasks and its potential applications in healthcare services. These systems can be beneficial in automating healthcare processes, improving patient care, and simplifying report generation. However, they emphasize ethical concerns, data interpretation challenges, accountability issues, and privacy concerns related to sensitive medical information when utilizing ChatGPT in healthcare. The articles also emphasize the importance of ensuring originality, accuracy, and academic integrity before these systems are extensively integrated into clinical practices. Additionally, They underlines the lack of studies exploring LLM applications in nucleic acid research.
[210], [211]	Authors recognize ChatGPT’s ability to generate diverse content and its growing importance in various domains. However, it also points out certain restrictions or limitations of the tool, such as sometimes the generation of incorrect information, may rise with biased content, etc. They emphasize the need for validation and combined methods for accuracy.
[190]	It highlights the significant improvements that CoreGen demonstrates over baseline models. Additionally, it discusses the potential benefits of training contextualized representations on larger code corpora and adapting this framework to other code-to-text generation tasks.
[179]	The study shows that in certain cases, cybersecurity policies generated by GPT (a type of artificial intelligence) are better than policies created by humans, especially when tailored prompts are used. However, the study also recognizes that there are limitations and stresses the importance of having specialized input, human moderation, and expert input to achieve the best results. The study also provides recommendations for companies that are considering integrating GPT into their GRC (governance, risk, and compliance) policy formulation.

Table 8.2 – continued from previous page

Paper	Discussion
[212]	For the authors, ChatGPT’s advantages lie in its versatility for human-machine interface creation, text generation, and knowledge provision, offering potential applications like chatbots, virtual assistants, and automation within Industry 4.0. However, limitations may include biases in generated content and challenges in ensuring accuracy and reliability in automated processes. The gap involves balancing the advantages with mitigating biases and ensuring the reliability of automated operations.
[213], [214]	According to them, AI-generated poetry’s benefits showcase the difficulties people face distinguishing it from human-written poetry. This helps us understand how humans perceive AI-generated content. However, there are limitations as some people negatively respond to algorithm-generated poetry, indicating a preference for human-written work.
[215]	It emphasizes ChatGPT’s potential in overcoming challenges faced by existing deep learning approaches in agricultural text classification, demonstrating promising performance without fine-tuning on agricultural data. However, it acknowledges this as a preliminary study and highlights the need for further exploration to establish ChatGPT’s applicability and performance in diverse agricultural contexts.
[216]	The paper provides valuable empirical insights from a case study, identifying critical AI capabilities and emphasizing the need for business model innovation to scale AI effectively in manufacturing firms. However, it’s essential to further explore the practical implementation and long-term impact of the proposed co-evolutionary framework and its mechanisms for scaling AI through business model innovation.
[217]	The study emphasizes the effectiveness of schema congruence in improving retrieval accuracy and highlights gamified learning’s potential to evoke positive emotions despite an underlying predominance of negative emotions.

Table 8.2 – continued from previous page

Paper	Discussion
[218], [176], [191], [219]	The authors reveal patterns of ChatGPT usage in code generation across various programming languages and tasks, highlighting prevalent emotions like fear associated with its usage, and provide a dataset for evaluating the quality of generated code. They identified ChatGPT’s limited performance in software modelling tasks compared to code generation, offering insights for short-term potential and suggestions for improvement in the modelling community.
[199], [180], [220]	They demonstrate the GPT model’s ability to generate syntactically correct code and highlights its limitations in producing effective bug fixes in specific scenarios. However, the overall accuracy suggests room for improvement in its performance for program repair. They explore the explainability needs of generative AI models in software engineering contexts and proposes XAI features to address these needs, highlighting the importance of human-centred design in driving technical advancements.
[221]	It demonstrates advancements in video generation by addressing temporal aspects and auxiliary tasks, yet may require further refinement for real-world application.

To summarise, LLMs (Language Model Models) are highly effective instruments for generating code. They are simple to train, and the outcomes are both speedy and highly encouraging. However, it is essential to acknowledge that there are some limitations associated with them. One significant challenge is identifying incorrect information or code that may be generated, which could lead to more severe issues when used. Therefore, it is essential to exercise caution when using LLMs and ensure that the generated code passes rigorous quality control checks to avoid any potential issues.

Threats to validity

We highlight some threats to the review’s validity, identified during the writing phase.

- **Fast evolving landscape:** The field of LLMs applied to code generation is characterized by its dynamic and constantly evolving nature. It is challenging

to encompass all the relevant literature, given the novelty of the subject, the limited time frame for the review, and the constant influx of new research. Moreover, the dynamic growth of the field introduces the possibility that some crucial contributions may have emerged after the review period.

- **Pre-prints exclusion:** A significant threat to the completeness of this review comes from the decision to exclude non-published papers, such as pre-prints. The exclusion of pre-prints, which are prevalent in emerging and fast-paced research domains, may lead to an oversight of valuable insights and advancements that have yet to undergo formal peer review.
- **Open Access papers:** The introduction of the inclusion criteria to include only open access papers introduces a potential bias in the selection process. This review may only encompass some of the available literature by excluding papers that are not freely available, thereby missing valuable contributions from subscription-based or proprietary sources. This limitation might result in a partial representation of the diverse research landscape surrounding the analyzed topic.
- **Search string:** The choice of the search string employed in online scientific databases may introduce a level of subjectivity and potential bias. While the chosen string is designed to capture a broad spectrum of relevant literature, alternative search strings may yield different results.
- **Performance in the topic:** The proficiency of LLMs in code generation tasks may result in a lack of research that explicitly addresses challenges or advancements, given that these models may already perform well in this domain [222].

Despite these potential limitations, this review presents a comprehensive overview of the current literature on LLMs applied to code generation tasks. We aim to improve the review further and update it in the future to include new publications and new approaches to the topic.

To conclude, our review provides a general picture of the capability of LLMs in code generation. We analyzed research papers published between 2021 and 2023. Our findings reveal a significant increase in papers published from April 2023 onwards, as highlighted in Fig 8.7. This can be attributed to the widespread adoption of ChatGPT as a tool for mass communication, which was introduced in November 2022. Most papers were published between August and October 2023, after which there was a slight decrease in published papers. This reduction in research focus dedicated solely to code generation tasks within the domain of LLMs could be because of these models' broader versatility and applicability across a spectrum of computational tasks.

We saw that Python is a popular choice for building and testing large language models, likely due to its widespread use in machine learning and natural

language processing. Although most papers do not mention specific programming languages, this could suggest that researchers focus more on the methods, techniques, and algorithms used for generating code rather than the language used for implementation.

Finally, it is widely recognized that LLMs (Language Model Models) are invaluable in generating code. These models are characterized by their ease of training and the rapidity and reliability of their results. Nevertheless, it is crucial to acknowledge that these models have their limitations. One of the most significant challenges is identifying incorrect information or code generated by these models, which can have serious consequences when deployed. Therefore, it is imperative to exercise caution when using LLMs and ensure that the output code passes through rigorous quality control checks to mitigate potential risks.

Chapter 9

Software Engineering Education and Training

Software Engineering Education and Training (SEET) encompasses the development and delivery of instructional methodologies aimed at equipping individuals with essential software engineering skills. The need for continuous employee training and upskilling in the industry links closely to SEET. In this context, the conducted research includes multiple studies. Section 9.1 presents a review of gamification usage in SEET, and Section 9.2 extends this focus to industrial settings. Section 9.3 mixes metaverse and LLMs to deliver innovative platforms for students, and Section 9.4 explores the potential of large language models (LLMs) to enhance SEET, particularly in peer assessment.

9.1 Review on Gamification in SEET

Gamification, the integration of game design elements into non-game contexts, has emerged as a significant approach in various domains, including education and training. It employs elements such as points, badges, quests, and challenges to motivate and engage users, thereby enhancing their experience and performance. Its application ranges from universities to industries.

In the realm of Software Engineering Education and Training (SEET), gamification has the potential to transform traditional learning methods by making them more interactive and engaging [223]. SEET encompasses the instructional methodologies, curricular designs, and practical experiences aimed at equipping students and professionals with the knowledge, skills, and competencies required in the field of software engineering. It includes both formal academic programs, such as university degrees and professional certifications, and informal learning opportunities, such as workshops, online courses, and bootcamps. The objective of SEET is to prepare individuals to effectively design, develop, test, and maintain

software systems, ensuring they meet user needs and adhere to quality standards. SEET traditionally focuses on imparting technical skills and knowledge necessary for developing software systems. However, the conventional teaching methods often struggle to maintain student engagement and motivation [224]. By incorporating gamification, educators can create a more dynamic and stimulating learning environment, which can lead to improved learning outcomes. Gamification not only makes learning more enjoyable but also fosters a deeper understanding of complex concepts through active participation and immediate feedback [225].

In the context of professional training, gamification can play a crucial role in continuous learning and skill development. As the software industry evolves rapidly, professionals need to constantly update their skills and knowledge. Gamified training programs can offer a more compelling and effective way to achieve this, promoting sustained engagement and continuous professional development [226]. Moreover, gamification can increase the awareness of employees in critical scenarios [227] by letting them take action in less time to avoid dangerous situations [228].

Despite the promising potential of gamification, there is a need for a systematic evaluation of its application in SEET topic. This involves examining both the results improvements and the technical challenges associated with implementing gamified systems. To address this gap, we conduct a systematic literature review to evaluate the maturity and impact of gamification in SEET. We propose six Research Questions aimed at exploring the effectiveness of gamification in enhancing learning and training outcomes in Software Engineering. This review is based on an extensive analysis of 68 primary studies, identified and filtered through the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [229]. We assess the evolution of this topic over time, the application areas and the results obtained after the implementation of gamification techniques in university courses. Additionally, we discuss future research directions and practical implications for educators and trainers in the Software Engineering domain.

9.1.1 Background

This section introduces gamification by giving a common definition gathered from the analyzed papers. Moreover, it explores the main components of gamification and its role in SEET.

A brief definition of gamification can be given, based on different analyzed papers [230, 231, 232, 233, 234]: gamification is an approach characterized by the application of game design elements and principles in non-game contexts to enhance user engagement and motivation. Unlike traditional educational methods, which often rely on passive learning, gamification leverages the interactive and stimulating nature of games to create more dynamic learning experiences [235].

In the domain of SEET, gamification has shown significant potential. Traditional Software Engineering education typically involves theoretical learning and

practical exercises designed to build technical skills. However, maintaining student motivation and engagement can be challenging with conventional teaching methods. By incorporating gamification, educators aim to make learning more interactive and enjoyable, thereby increasing student participation [223] and improving learning outcomes [16].

The core components of gamification include the integration of game mechanics, dynamics, and aesthetics [236].

- Game mechanics refer to the rules and feedback systems that drive gameplay, such as scoring, levels, and rewards.
- Game dynamics involve the emotions and behaviors induced by the mechanics, such as competition, collaboration, and achievement.
- Aesthetics pertain to the overall look and feel of the gamified experience, which can enhance its appeal and immersion.

Application of Gamification in Software Engineering Education

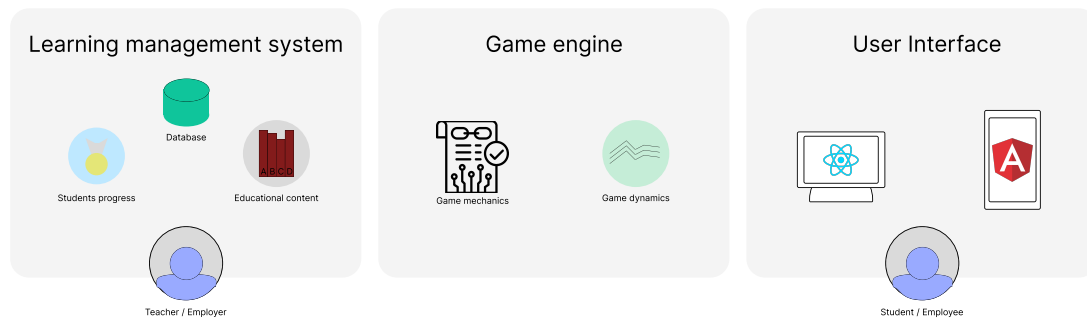


Figure 9.1: A common architecture for gamified educational platforms

Figure 9.1 illustrates a typical architecture for gamified educational platforms. This architecture includes components such as the learning management system, game engine, and user interface [237]. The learning management system handles educational content and tracks student progress, while the game engine manages game mechanics and dynamics. The user interface presents the gamified experience to students, providing them with interactive and engaging learning activities, typically accessible as web apps [238], created using some frameworks (e.g.: Angular, ReactJS).

The unique characteristics of gamification make it well-suited for SEET. Gamification can transform traditional learning environments by promoting active participation, immediate feedback, and a sense of progression. These features help address common challenges in education, such as student disengagement and the difficulty of maintaining sustained interest over time [239].

Gamification fosters an interactive learning environment where students can engage in problem-solving activities that mirror real-world Software Engineering tasks. This practical application of knowledge helps reinforce learning and develops critical thinking skills. For example, gamified platforms might simulate coding challenges or project management tasks, allowing students to apply theoretical concepts in a controlled, game-like setting.

Moreover, gamification can enhance collaborative learning. By incorporating team-based challenges and competitive elements, students are encouraged to work together, share knowledge, and develop essential soft skills such as communication, teamwork, and leadership [240]. This collaborative aspect is crucial in Software Engineering, where teamwork and communication are key to successful project completion.

Despite its benefits, the application of gamification in SEET also presents several challenges. Designing effective gamified systems requires a deep understanding of both game design and educational pedagogy. There is a need to balance game elements with educational content to ensure that learning objectives are met without compromising the fun and engagement aspects [241].

To address the proposed challenges and explore the potential of gamification in SEET, a systematic evaluation of existing studies is necessary. This involves assessing the design, implementation, and outcomes of gamified educational tools and identifying best practices and areas for improvement.

9.1.2 Related work

Different reviews on the topic of gamification applied to SEET have been examined. The main ones are proposed below, together with analyzed databases and main findings.

Dal Sasso et al. [242] propose a critical overview of gamification and its application in supporting Software Engineering tasks, starting from IEEEExplore database. They highlight how to implement gamified approaches and propose a method to evaluate gamification systems. However, the presented work is not a systematic review, but a first approach in evaluating literature.

Pedreira et al. [243] carry out a systematic mapping study to analyze papers between 2011 and mid 2014. They use Scopus, Science Direct, IEEEExplore, ACM Digital Library, and Springer databases to gather papers, and find 29 primary contributions: main results show that research in this field is still preliminary, and most of the considered papers focus on software development and not on proving empirical evidence of pros and cons of gamification.

Barreto et al. [244] carry a mixed-approach literature review, composed by both an ad-hoc review in which they manually select relevant papers and a systematic review following Software Engineering guidelines based on ACM Digital Library, IEEEExplore, and Science Direct databases. They conclude that "researchers in the

field tend towards a strict view of gamification, the practical results of gamification are unclear and polemic, and this research area has still much to improve."

Ngandu et al. [245] analyze 15 papers, conducting a literature review on IEEEXplore and Science Direct to understand the impact of gamification and its key elements to students interest in Software Engineering. Their main findings regard points and leaderboards, considered as the main elements used in this topic.

Chamorro-Atalaya et al. [246] study the impact of COVID-19 pandemics in the education shift and the opportunities carried by gamification in online teaching. Analyzed papers are gathered from Taylor & Francis, IEEEXplore, and Scopus. Software Engineering and Computer Science result to be the main topics in which gamification is applied, and the application of gamification effectively generates motivation, commitment, and permanent participation of students.

Monteiro et al. [247] analyze papers coming from IEEEXplore and ACM Digital Library that report procedures for the evaluation of gamification. However, only three of the 64 found studies actually propose evaluation models for gamification. The main finding is that "the evaluation of gamification requires a mix of subjective and objective inputs, and qualitative and quantitative data analysis approaches".

Related works analysis shows the need of developing an updated literature review, to analyze not only teaching effectiveness, but also the role of gamification in Software Engineering-based jobs. Our review also makes an analysis on how the effectiveness of gamification in SEET is measured. The comparison between the different reviews is summarized in Table 9.1. The columns in the table include the reference for the reviewed work, key terms used in the study to highlight its focus areas, whether the study followed a systematic review or mapping methodology, the primary setting or context where gamification was applied, whether the study involved or considered industrial applications or partnerships or their involvement in the SEET topic, and a summary of the practical findings regarding the effectiveness or impact of gamification as reported by the study.

9.1.3 Research methodology

Our research adheres to the guidelines for a Systematic Literature Review (SLR) as described in [50]. This study aims to explore the application of gamification in SEET, covering literature published from 2015 to 2023, using the PRISMA methodology [229] and useful tools for papers gathering, such as Zotero¹, and for tagging and data extraction, such as Python and Microsoft Excel.

¹<https://www.zotero.org/>

Table 9.1: Comparison between related works and our review

Reference	Keywords	Systematic	Main application field	Industrial	Findings
[242]	Games, Software Engineering, Context, Psychology, Computer bugs, Collaboration, Systematics	No	Universities	No	No findings
[243]	Gamification, Software Engineering, Systematic mapping	Yes	Universities	No	No findings
[244]	Motivation, engagement, gamification, Software Engineering	Mixed	Universities	No	Unclear practical results
[245]	Gamification, Software Engineering, Student interest, Game elements, Engagement, Motivation, Participation	Yes	Students engagement	No	No findings
[246]	gamification, engineering education, design, success factors, motivation	Yes	Universities after COVID-19	No	No findings
[247]	gamification, systematic mapping, evaluation, software engineering, education	Yes	Universities	Yes	Yes
This review	gamification, Software Engineering, education, learning, literature review	Yes	Universities and companies	Yes	Yes

PRISMA Methodology

This section outlines the systematic review methodology employed in this study, following the PRISMA guidelines. This approach ensures a rigorous and transparent review process, allowing for comprehensive identification, selection, and analysis of relevant studies.

The review is guided by some Research Questions (RQs) formulated to focus the scope of the study. These RQs are designed to capture the essence of the investigated topic and to guide the systematic review process.

The Population, Intervention, Comparison, Outcome (PICO) framework is used to refine the RQs and set clear criteria for study selection:

- **Population:** The group or individuals targeted by the intervention.
- **Intervention:** The specific intervention or exposure being investigated.
- **Comparison:** The control or comparison group, if applicable.
- **Outcome:** The outcomes or effects measured in the study.

A search strategy is developed to identify all relevant literature. The search string is constructed using keywords and phrases pertinent to the research question and is applied across multiple databases to ensure thorough coverage. Searches are conducted in major academic databases.

To ensure the selection of relevant and high-quality studies, specific inclusion and exclusion criteria are established. They are needed to ensure that filtered papers are relevant to the scope of the study.

The extracted data, based on defined RQs, are then synthesized to provide a comprehensive overview of the current state of research on the topic, identify trends, and highlight gaps in the literature.

The process for identifying relevant papers, based on the PRISMA guidelines, is illustrated in Figure 9.2. generated using the tool explained in [248].

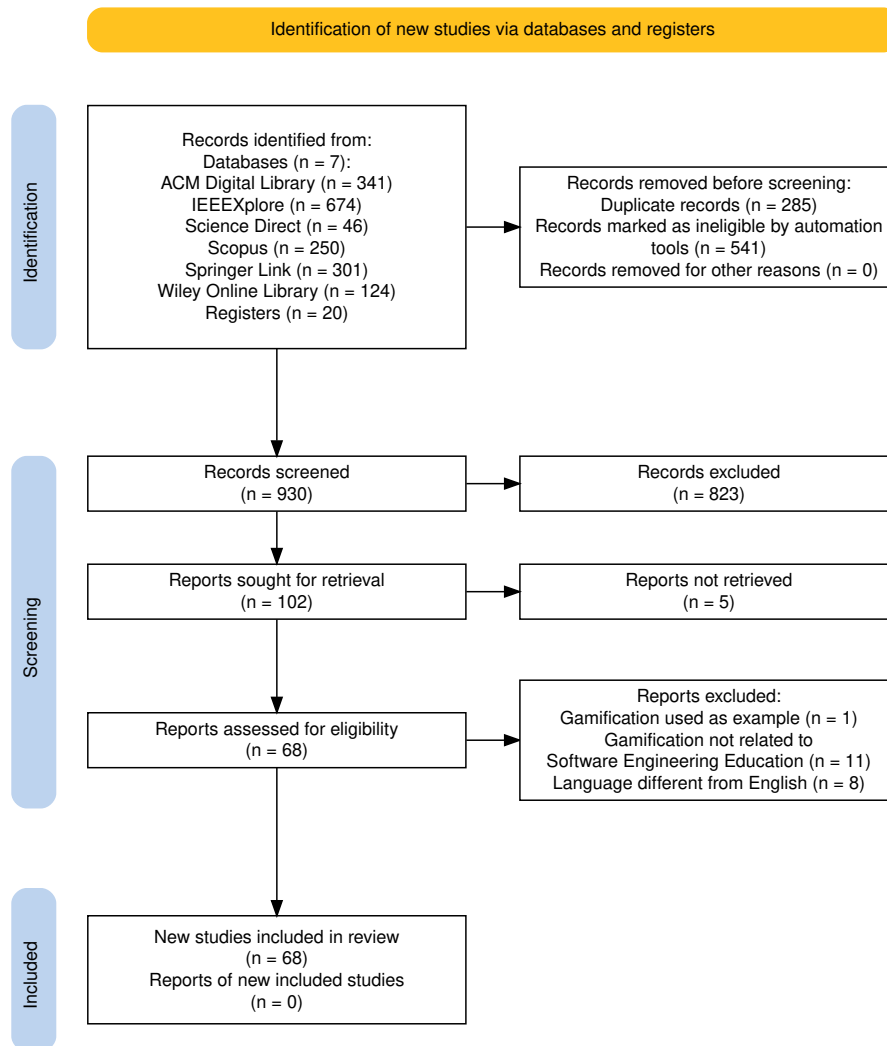


Figure 9.2: PRISMA search methodology

Research Questions definition

The objectives of this study are twofold: (a) to identify the current state of gamification in SEET, and (b) to provide a foundation for highlighting gaps and trends in this field, as well as suggesting future research directions. To achieve these goals, we formulate the following Research Questions (RQs):

- RQ1: What is the publication trend in the area of gamification applied to SEET?
This question investigates the trend in publication quantity and the structure of publication venues, which are useful for understanding the progression of this topic.
- RQ2: In which areas of Software Engineering is Gamification used?
This question aims to identify the key areas of study and their contributions to the scientific community.
- RQ3: What are the analyzed application areas?
This question explores the benefits of using gamification, considering its impact on learner engagement and performance.
- RQ4: What contribution does gamification offer when it is applied to SEET?
This question examines the specific contribution and integration of gamification into educational practices.
- RQ5: In which continents is gamification mostly analyzed?
This question aims to identify the continents that are most interested into gamification applied to SEET.
- RQ6: What are the advantages and disadvantages of gamification, when applied to SEET?
This question seeks to understand the the pros and cons to evaluate the success of gamification in educational settings.

Papers selection

Relevant databases were systematically searched to ensure comprehensive coverage of the literature. A PICO approach was utilized to define the search keywords, grouped into two main categories:

- Population-related search terms: "Software Engineering education," "training"
- Intervention-related search terms: "gamification," "game-based learning"

The search string used was: *"gamification AND (Software Engineering OR programming) AND (education OR training OR teaching OR learning)"*

This search returned a total of 1756 results. The following databases were searched: ACM Digital Library (only Open Access content), IEEE Xplore, ScienceDirect, Scopus, SpringerLink, Wiley Online Library (only Open Access content), and Google Scholar (only Open Access content). This volume of results is considered appropriate for the scope of the review.

Inclusion and Exclusion Criteria

To enhance the reliability and relevance of the studies included in our review, specific inclusion and exclusion criteria were applied.

Inclusion criteria:

- Studies published between 2015 and 2023.
- Studies written in English.
- Studies published in peer-reviewed journals or conference proceedings.
- Studies focused on the application of gamification in Software Engineering education or training.
- Studies that present empirical evidence or substantial theoretical contributions.

Exclusion criteria:

- Studies for which the full text is not available (e.g., article not available online or DOI not found or not readable without subscriptions): 364 studies.
- Secondary or tertiary studies (e.g., reviews or surveys): 175 studies.
- Studies where gamification is not the main focus but is only mentioned: 284 studies.

By adhering to these criteria, we ensured that the selected studies were pertinent and of high quality, thereby providing a solid foundation for our systematic review.

A pool of 68 studies is included in the analysis after the application of the screening procedure.

9.1.4 Results and discussion

The following section analyzes results of the performed review. Each subsection answers one of the six proposed Research Questions.

RQ1: What is the publication trend in the area of gamification applied to SEET?

To analyze the temporal evolution of research on gamification in SEET, we examined the publication trends over the past years. Figure 9.3 illustrates the number of publications per year from 2015 to 2023.

The analysis reveals several notable trends. Starting in 2015, there were a modest number of publications, increasing over the next few years. A significant rise

is observed in 2018, with the number of publications peaking at 11. This increase indicates growing interest and recognition of the potential benefits of gamification in SEET during this period.

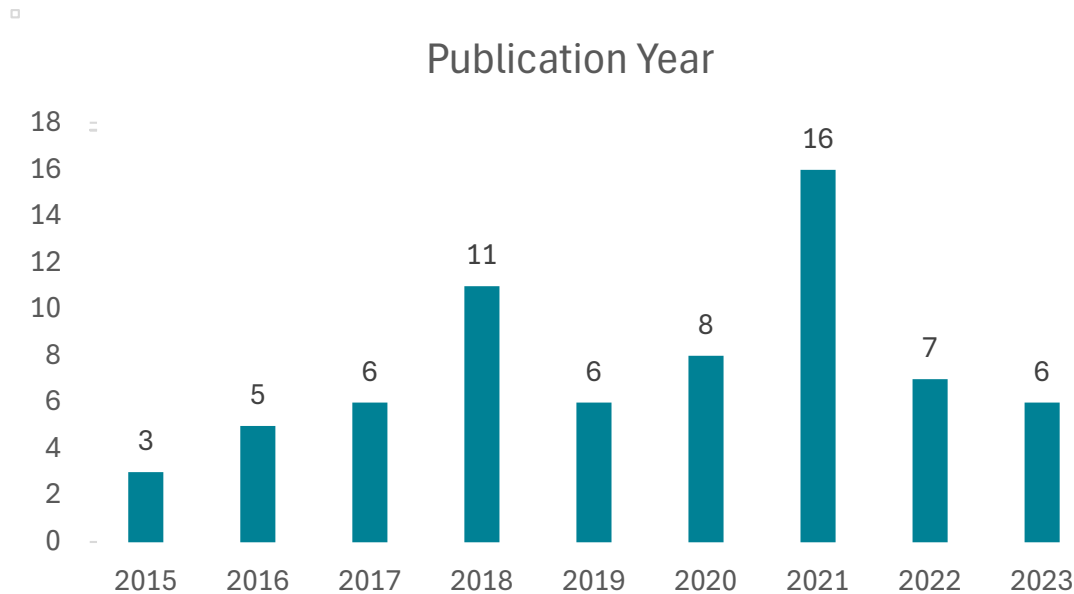


Figure 9.3: Publication trends over time for gamification in SEET

Interestingly, the number of publications remained stable in 2019, again with 6 papers, before experiencing another rise in 2020 with 8 publications. The most substantial growth occurred in 2021, with a peak of 16 publications. This surge can be attributed to the COVID-19 pandemic, which necessitated remote learning solutions and the adoption of innovative teaching methodologies, including gamification, to engage students in virtual environments. The continued interest in gamification indicates that it remains a relevant and important area of research in SEET, together with the higher number of journal publications in the last years.

Figure 9.4 presents the distribution of publication types, differentiating between conference papers and journal articles.

The analysis reveals that the majority of the research output on gamification in SEET has been in the form of conference papers. This is indicative of the dynamic and rapidly evolving nature of the field, where researchers prefer the relatively faster dissemination route offered by conferences to share their latest findings and innovations. Approximately 80% of the total publications were conference papers, reflecting the community's emphasis on quick dissemination and discussion of new ideas.

In contrast, journal articles, which typically undergo a more rigorous and lengthy

peer-review process, constituted around 20% of the publications. This lower percentage suggests that while there is a substantial amount of exploratory and preliminary research being conducted, fewer studies have reached the level of maturity required for journal publication. The presence of journal articles, however, highlights that some research in this domain has achieved significant depth and rigor, contributing to a more formal and comprehensive understanding of gamification in SEET.

□

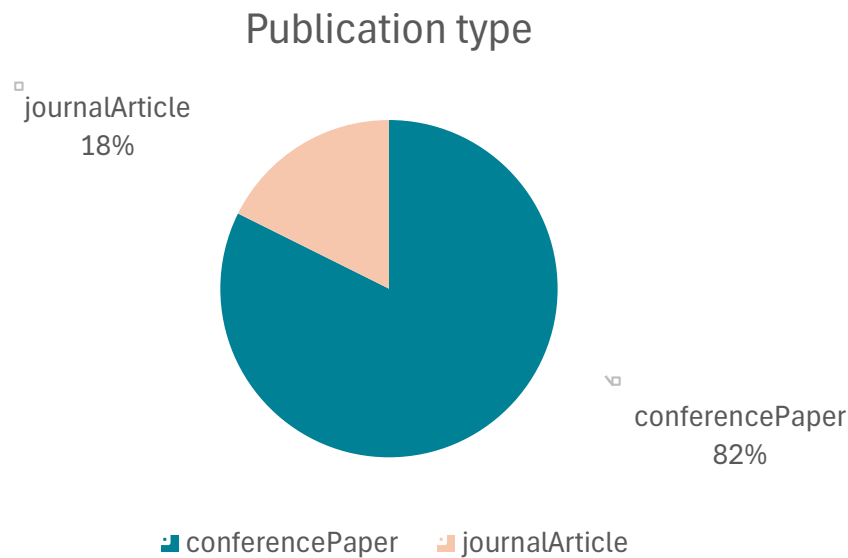


Figure 9.4: Distribution of publication types for gamification in SEET

RQ2: In which areas of Software Engineering is Gamification used?

Figure 9.5 illustrates the sectors where gamification has been applied in SEET.

The analysis indicates that the predominant application area for gamification in SEET is within university-level Software Engineering programs, which accounts for 30 studies, about 44% of the analyzed studies. This reflects a significant focus on integrating gamified approaches to enhance the learning experiences of students in higher education, particularly in courses related to Software Engineering, as shown in papers [232, 230, 249].

Schools and related educational institutions represent the second most common sector, with 23 studies, 34% of the analyzed papers. This includes primary, secondary, and other non-university educational contexts where gamification is used to make learning more engaging and effective.

Companies are also exploring the use of gamification (9% of the papers). In the corporate sector, gamification is employed to improve employee training, professional development, and motivation, as shown in [250]. The lower number of

studies in this sector could be due to the proprietary nature of corporate training programs, which might not be as widely documented in academic literature.

The "Other" category, encompassing 9 studies, includes various applications that do not fit neatly into the previously mentioned sectors. This involves informal learning environments, online courses, or interdisciplinary studies where gamification is applied.

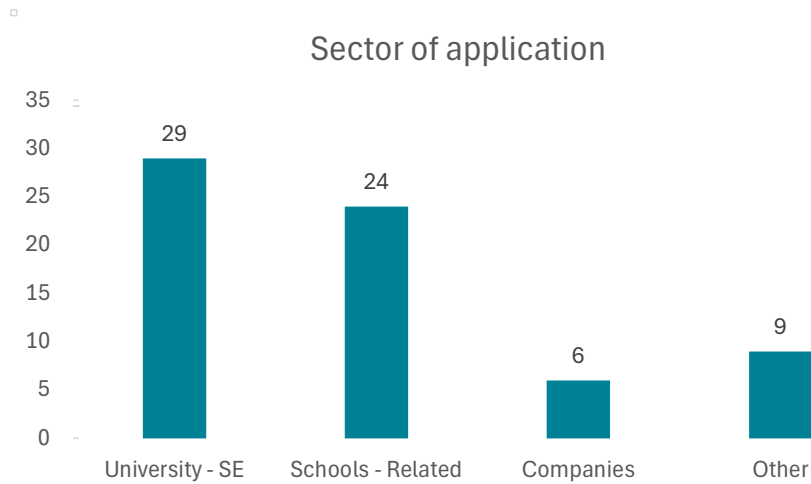


Figure 9.5: Sectors of application for gamification in SEET

RQ3: What are the analyzed application areas?

To explore how gamification is used within SEET, we firstly understand the search type of selected papers, then we analyze the various application areas where gamified approaches are implemented.

To evaluate the depth of analysis on gamification in SEET, we categorized the 68 primary studies into five distinct groups based on their focus: Proposal, Analysis, Implementation/Tool, Validation, and Other. The distribution of studies across these categories provides insight into the current state and focus areas of research in this field. Results are shown in Figure 9.6.

- **Proposal:** This category includes studies that introduce new concepts, frameworks, or methodologies for applying gamification in SEET. We identified 10 papers that primarily focus on theoretical foundations and suggest innovative approaches to integrating gamification into educational contexts.
- **Analysis:** In this category, 10 studies provide detailed examinations of existing gamification techniques and their impacts on learning outcomes.
- **Implementation/Tool:** The largest category, with 24 studies, focuses on the practical aspects of implementing gamification. These papers describe the

development and deployment of specific tools, platforms, or software that incorporate gamification elements into SEET. They often include case studies or reports on pilot projects.

- **Validation:** Comprising 17 studies, this category includes empirical research that evaluates the effectiveness of gamification through experiments, surveys, or longitudinal studies. These papers provide evidence-based insights into how gamification influences student engagement, motivation, and learning outcomes.
- **Other:** The remaining 7 studies cover various other aspects of gamification that do not fit neatly into the above categories. This includes research on the broader impacts of gamification, such as its effects on educational policy, its role in lifelong learning, and interdisciplinary applications.

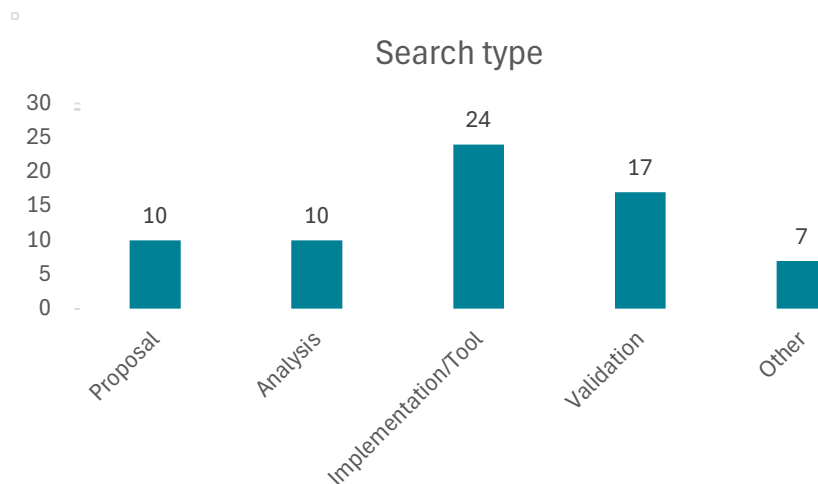


Figure 9.6: Distribution by search type

The categorization reveals a balanced approach to exploring gamification in SEET, with significant emphasis on practical implementation and empirical validation. While a substantial number of studies propose and analyze gamification frameworks, the majority focus on real-world applications and their validation, highlighting a strong interest in understanding the practical benefits and challenges of gamification in education.

Figure 9.7 illustrates the distribution of the application areas.

The analysis reveals that the primary use of gamification in SEET is for teaching support, which constitutes 56% of the studies. This significant proportion indicates that gamification is predominantly applied to enhance educational experiences, making learning more engaging and interactive for students. Examples of this include the incorporation of game elements into lectures, assignments, and

assessments to motivate students and improve their learning outcomes. Work improvement represents 19% of the applications. This area focuses on using gamification to enhance productivity, collaboration, and efficiency in software engineering practices. For instance, gamified tools and platforms are used to improve team dynamics, project management, and individual performance within software development teams. Approach analysis accounts for 18% of the studies. This area involves evaluating and analyzing the effectiveness of different gamified approaches and methodologies in SEET. Research in this domain aims to understand the impact of gamification on learning outcomes, student engagement, and overall educational quality. Serious Games constitute 7% of the applications. These are games designed for purposes beyond mere entertainment, specifically to educate and train individuals in software engineering concepts and practices. Serious games provide immersive and interactive learning environments that simulate real-world software engineering challenges. For instance, a serious game might involve a scenario where players must collaboratively debug a software application or manage a software project with constraints and deadlines [251]. These games are categorized based on their educational objectives and the inclusion of realistic software engineering tasks. An example is "SimSE" [252], a game that simulates software engineering processes, allowing students to experience the impact of their decisions on the project's outcome. Another example is "CodeSpells" [253], where players write code to cast spells, learning programming logic and problem-solving skills in a magical context. Serious games enhance understanding and retention of complex software engineering principles.

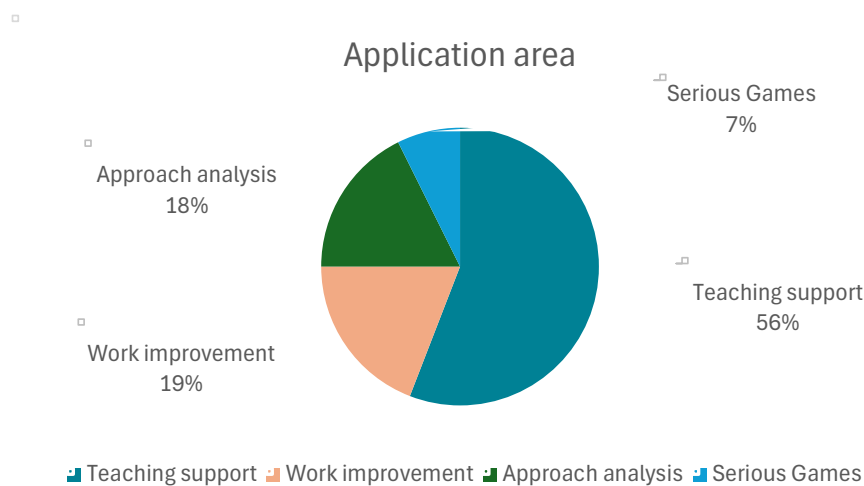


Figure 9.7: Application areas of gamification in SEET

RQ4: What contribution does gamification offer when it is applied to SEET?

To answer this RQ, we summarize the main contribution of each paper in Table 9.2. This table provides an overview of the key findings from each study, highlighting the specific ways in which gamification has been applied to the education topic. By examining these contributions, we can identify common themes, benefits, and challenges associated with gamification in this context, offering insights into its effectiveness and areas for further research.

Table 9.2: Main finding for each analyzed paper

Paper	Contribution
[234]	This paper discusses the use of gamification in MOOCs for a large number of students, using automatic tools to assign rewards (flipped-classroom tickets, quiz benefits, extra learning content) for a course on Spanish history from the 11th to the 16th century.
[254]	This paper covers the use of gamification for web programming in high schools, specifically for learning HTML, CSS, and JavaScript. The gamification involves a web app with rewards such as avatars, lives, and time constraints.
[255]	This paper focuses on using gamification to learn linear algebra, with storytelling as the main gamified element, along with avatars (king or queen), levels representing different topics, and scoring.
[256]	This paper describes creating an application with gamification techniques, emphasizing a reward-based system with customizable items, score saving, and leaderboards.
[257]	This paper presents a mobile application using gamification to understand software engineering, particularly extreme programming (XP), with points and level progression as elements. Positive results were achieved in testing.
[258]	This paper describes a mobile and web application for learning discrete math, physics, and chemistry through gamification, using quizzes, points, customizations, and avatars, with positive feedback from students.

[259]	This paper mentions using a gamified platform to learn software engineering, utilizing missions, experience points (XP), and level progression.
[260]	This paper surveys software engineering professors to determine if GBL and gamification improve learning outcomes, with positive results and gamified elements such as quizzes, points, levels, and badges.
[261]	This paper uses gamification in a penitentiary for digital literacy, with tutorials guiding inmates through basic literacy and computing concepts.
[262]	This paper uses Moodle for gamification in agile and scrum model learning, with points, badges, anonymous leaderboards, quizzes, and storytelling, though the latter was less engaging over time.
[263]	This paper utilizes various existing platforms with gamification for software engineering learning, including Kahoot and "Who Wants to Be a Millionaire?" for theoretical testing, and platforms for project role division and coding.
[264]	This paper describes creating a tool for educators to develop educational content with gamification elements, tested on a software engineering course using Happy Faces for points and Kahoot for web 2.0.
[265]	This paper applies gamification to basic programming learning using playing cards with commands, forming groups to solve assigned algorithms, with different difficulty levels.
[266]	This paper describes a platform (CoverBot) using gamification to teach code debugging, with levels, graphics, and sounds to enhance user experience.
[267]	This paper applies gamification to civil service training with a custom application using missions, points, ranking systems, levels, and badges.

[268]	This paper uses gamification for understanding algorithms and data structures in C++, with Moodle incorporating points and leaderboards to motivate faster assignment completion, and a Q&A forum for extra points.
[269]	This paper analyzes a multi-context, narrative-based platform (GoRace) for educational and workplace use, with storytelling, challenges, rewards, penalties, rankings, and a shop for advantageous items.
[270]	This paper uses a tower defense game for learning formal languages, where users defend a processor from bugs while creating abstract syntax trees for assigned commands.
[271]	This paper discusses gamification in programming and modeling (UML diagrams) using PolyGlot and PapyGame platforms with points, XP, levels, coins, and rewards.
[272]	This paper applies gamification to a Risk Management course with a web app using points, levels, and leaderboards for competition, with positive results.
[273]	This review surveys instructors, identifying gaps in SEE teaching and proposing solutions like SWEBOK guidance, Mentimeter, and Flipped Classroom.
[274]	This paper provides gamification implementation examples like Flipped Classroom, recorded short lessons, and group projects.
[275]	This paper uses gamification for university project development, suggesting characteristics like negative points for wrong code and positive points for solving software quality issues.
[276]	This paper presents "iGaME," a bot for teaching machine learning algorithms in classrooms using gamification.
[277]	This paper uses gamification in "Minecraft" to teach Scrum development methods to electrical engineering students.

[278]	This paper describes applying gamification in Vector to develop software applications, enhancing user engagement and learning.
[279]	This paper describes teachers using gamification principles like realistic stories for students to immerse in software creation tasks.
[280]	This paper presents the serious game "Tree Legend" for studying trees/graphs.
[281]	This paper describes MOOC platforms like Moodle using the "CodeRunner" plugin for coding questions and "Pacman" for pathfinding algorithms.
[282]	This paper describes "Capture the Flag" for understanding AI, machine learning, and microprocessor decoding.
[283]	This paper discusses gamification in software engineering training to expand knowledge of new development technologies, with younger SWE more receptive than seniors. Stackoverflow's gamification with badges and reputation is also mentioned.
[249]	This paper proposes using ChatGPT to find strategies for implementing gamification in Software Engineering Education.
[284]	This paper presents an experiment in a Croatian university during COVID-19, using a mobile app for short lessons and gamified elements like leaderboards, points, and rewards.
[285]	This paper discusses GamiCRS, a web application using PBL (Points-Badges-Levels) for coding skill improvement and student motivation, tested in a Hong Kong university with positive feedback.
[230]	This paper presents MEEGA+, a framework for evaluating educational games in software engineering using the GQIM approach, evaluated by three researchers in five phases.
[232]	This paper discusses gamification's impact on students and teachers in software engineering, education, and psychology, highlighting improvements in individual skills and teamwork.

[233]	This paper discusses e-valUAM, an adaptive gamified system tested in a Madrid university using the MUD model to enhance engagement.
[286]	This paper discusses PBL (problem-based learning) combined with gamification to improve student engagement and motivation, with examples like 'Millionaire' and general brainstorming games.
[231]	This paper compares the PRBL (points-ranking-badges-levels) gamification method with traditional teaching, highlighting its advantages and disadvantages.
[287]	This paper discusses Microlearning, an action-oriented approach with short lessons, combined with interactive gamification elements using the Octalysis Framework.
[288]	This paper discusses a course for medical, aerospace, and IT equipment testers using gamification to address various teaching challenges and enhance realism.
[289]	This paper highlights the advantages and disadvantages of e-learning, showing how gamification can improve teaching and training with role-playing, exercise games, and simulation games.
[290]	This paper characterizes how gamification has been applied in software engineering, identifying benefits and challenges.
[291]	This paper discusses the inclusion of computational thinking in curricula and the need for an educational approach involving various stakeholders.
[292]	This paper examines a course on Professional Software Development and the integration of gamification to enhance learning outcomes.
[293]	This paper highlights the motivational power of games and explores gamification's potential to increase student engagement in programming courses.

[294]	This paper describes the development and impact of Rimigs, a gamification system aimed at improving student engagement and learning outcomes.
[295]	This paper reviews the role of agile methodologies in software development education and how gamification can enhance collaborative learning.
[296]	This paper evaluates the effectiveness of gamification in computer programming education through various case studies and learning outcomes.
[297]	This paper analyzes the impact of social learning and gamification on higher education, focusing on activity levels and learning results.
[250]	This paper explores the importance of communication in software management and how gamification can improve team interactions and project outcomes.
[298]	This paper presents the recurring theme of gamification in software engineering education literature and its influence on student engagement.
[299]	This paper assesses the potential of gamification to enhance student engagement, drive learning, and support sustainable educational practices.
[300]	This paper investigates the effect of educational e-courses with gamification elements on student motivation and learning without actual gameplay.
[301]	This paper introduces the Personalized Adaptive Gamified E-learning (PAGE) model, which extends MOOCs with enhanced learning analytics and visualization to support learner intervention. The results indicate a positive potential for learning adaptation and the necessity of focusing on gamification.
[302]	This paper develops an e-learning system named Code Mania (CoMa) that integrates gamification elements like leaderboards and badges to increase student engagement in a Java Programming course. The system performs well as specified, demonstrating the potential of gamification in enhancing e-learning environments.

[303]	This paper investigates the applicability of gamification across different higher education courses through an experiment involving computer science students. The study shows the comparative results of gamified and non-gamified groups, indicating the impact of gamification on student performance.
[304]	This paper presents an online learning platform with gamification elements designed for software engineering education. It combines formative assessment with gamification to enhance learning experiences, providing detailed examples and system design.
[305]	This paper reports on the outcomes of the 6th International Workshop on Games and Software Engineering, highlighting the growing complexity and need for theoretical frameworks in gamification. The workshop covered perspectives on software projects, testing, and design, with insights from keynotes and panel discussions.
[306]	This paper presents POLYGLOT, a gamified programming environment targeting programming languages education and text-based modelling languages like SysML v2. The approach allows for the creation of heterogeneous gamification scenarios, enhancing the learning experience.
[307]	This paper explores the relevance of publication bias tests in meta-analytical approaches to gamification in higher education. It discusses the challenges in conducting meta-analyses due to heterogeneity and compares methods for correcting publication bias.
[308]	This paper introduces a continuous improvement cycle for teaching scenarios in engineering, combining gamification theory and ABET criteria. The proposed cycle is applied in a computer programming course, showing a positive impact on student engagement and learning outcomes.

[309]	This paper discusses the convergence of game engineering, software engineering, and user experience to create solutions blending game strengths with real-world applications. It highlights the potential benefits of gamification and serious games in various domains such as education and health-care.
[310]	This paper presents a gamification approach in a hardware-based course on Microprocessors and Microcontrollers for computer science students. The approach improved course grades and motivated students to enroll in other hardware courses, demonstrating the positive impact of gamification on student interest and performance.
[311]	This paper presents empirical research on the use of gamification in online programming courses. A gamified e-course was designed, and its impact on student engagement and use of learning materials was examined, showing potential benefits of gamification in e-learning.
[312]	This paper reports on a gamification approach using Minecraft to train students in Scrum, an agile project management method. The study compares two teaching periods, highlighting findings and lessons learned from using game-based learning to teach Scrum principles.
[313]	This paper analyzes gamification software for promoting minority languages. It provides an overview of current educational software and assesses the need for new gamification solutions to support regional and minority languages.
[314]	This paper presents jLegends, an online multiplayer platform game designed to teach programming with JavaScript. The game employs a role-playing approach to enhance learning through game mechanics, demonstrating the effectiveness of game-based learning in programming education.

RQ5: In which continents is gamification mostly analyzed?

An analysis on the geographical distribution of relevant papers reveals that Europe is the leading region, with 41% of the studies, as shown in Figure 9.8. This significant proportion indicates a robust interest and investment in gamification strategies within European educational institutions and research communities.

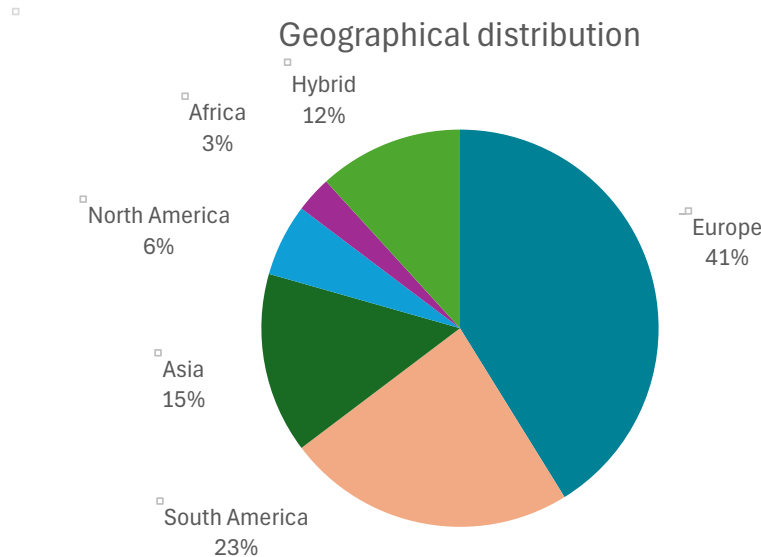


Figure 9.8: Geographical distribution of studies on gamification in SEET

The prominence of European research in this field suggests that many universities and educational bodies in Europe are actively exploring and implementing gamification to enhance learning outcomes. This focus could be driven by several factors, including the strong support for educational innovation in European countries, the availability of funding for educational research, and the collaborative networks among European researchers. The "hybrid" field includes papers where authors have affiliations from two or more continents, to avoid inconsistencies in the data extraction.

RQ6: What are the advantages and disadvantages of gamification, when applied to SEET?

The application of Gamification as an educational tool has been the subject of extensive analysis, revealing both its advantages and disadvantages. We examine the potential benefits and drawbacks of this technique below.

Among the advantages, Gamification has been shown to significantly enhance student participation [315] and interest [293] compared to traditional teaching methods. For instance, in the study conducted at the University of Applied Sciences Würzburg-Schweinfurt [262], 40 students were surveyed, with 27 respondents.

Initially, 35% of students reported moderate motivation levels before engaging with the gamified course. Post-intervention, 40% of students indicated increased motivation due to the Gamification content, although nearly 20% did not find it motivating at all. This finding aligns with the broader research on Gamification, highlighting that motivation varies among individuals and is influenced by different types of gamified elements [259].

Furthermore, the economic growth associated with Gamification is notable. As reported in [269], the gamification market is projected to expand from \$9.1 billion in 2020 to \$30.7 billion by 2025, with a growth rate of 27.4% per year. This underscores the increasing interest and investment in Gamification as a promising educational approach. Gamification also provides intrinsic benefits for student motivation. By offering rewards and real-time feedback, students can visualize their progress and achievements, thereby enhancing their learning experience.

However, the application of Gamification is not without its challenges. Some limitations of gamification in SEET are summarized below [260]:

- Difficulty in measuring performance improvements
- Increased workload for educators [301]
- Lack of digital platforms to implement gamified techniques [260]
- Challenges in engaging all students
- Difficulty for some students to understand the gamification method
- Lack of appreciation for the method by some students
- Difficulty for students in gaining human feedback, for platforms in which gamification is used alongside Artificial Intelligence [249]
- Insufficient knowledge of gamification approaches
- Limited time and interest: students can sometimes become annoyed or disengaged by gamification elements if they find them distracting [316]
- Scarcity of materials and resources [301]
- Ensuring proper use of gamification by students

The analysis indicates that Gamification, like any pedagogical method, presents both strengths and weaknesses. The primary challenge lies in the nascent stage of this technique, which precludes definitive conclusions about its long-term efficacy [275]. Nevertheless, short- to medium-term studies and experiences in educational settings provide valuable insights into its potential benefits and limitations [317]. Furthermore, the novelty of gamification means that large-scale, comprehensive studies are currently lacking, making it difficult to obtain a fully reliable

overview of all its advantages and disadvantages. Continued research and practical implementation are essential to fully understand the impact of Gamification on education.

The use of gamification in SEET is a contentious and highly debated topic among experts in teaching. While disagreements exist regarding the integration of gaming aspects into educational systems, numerous proposed projects and studies have demonstrated positive outcomes that support the efficacy of gamification.

The advantages of using game environments for teaching are numerous. Gamification allows students to actively construct their understanding of topics, learn at their own pace individually or collectively in spontaneous groups, and proceed on different paths at varying speeds according to their interests and abilities. It also promotes collaboration and encourages just-in-time learning, as opposed to general training.

However, this teaching method also has some psychological drawbacks, particularly concerning its potential negative effects on students. Students, with gamification, are free to fail and free to experiment. While these freedoms aim to provide students with the ideal tools to build their own experiences, they can also lead to an overlock of responsibility. This can result in a stressful and unmanageable situation for some students.

Our review, based on the analysis of 68 papers, reveals a significant interest in using gamification in universities and secondary schools. Despite its recent development and the promising studies showcasing its effectiveness, there remains a tendency to rely on traditional learning methods, often overlooking the potential of gamification. Nonetheless, the growing need to integrate digital content to enhance learning has spurred increased interest in this alternative method. It is crucial to recognize that not all students or users are motivated by gamification. While the majority may find it effective, there will always be a percentage of students who prefer traditional teaching methods due to differing attitudes and learning times. Therefore, it is unrealistic to expect a single tool to be universally effective.

In conclusion, gamification in education should be viewed as a valuable support tool rather than a total replacement for traditional teaching methods. As highlighted in many of the analyzed papers, gamification is often used alongside classic, proven teaching methods and sometimes as an alternative support. Its potential to enhance learning experiences is significant, but it must be integrated thoughtfully to complement and not completely replace traditional educational approaches.

9.2 Gamification in Industries

This short review analyzes the role of gamification in industries. Industries are adopting gamification approaches to let employees know how to use machinery and infrastructure. The use of a virtual environment grants safety during the training phase and more engagement for workers. Gamification also comes in hand after the COVID-19 pandemic created new needs in the online training topic [1].

We use the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) guidelines to conduct the review [229]. We firstly define Research Questions (RQs), then we perform a complete search with a papers screening phase. Finally we extract relevant information. The PRISMA flow diagram is shown in Fig. 9.9.

We define five Research Questions to accomplish our goal.

- RQ1: When was gamification for industry born?
- RQ2: What are the trend topics on gamification for machinery and infrastructure?
- RQ3: What are the application fields?
- RQ4: What are the main problems in the application of gamification for industries and what prevents stakeholders to use this approach?
- RQ5: Can gamification track the level of acquired skills during training?

The data gathering phase is conducted using a search string:

gamification AND (learning OR training) AND (infrastructure OR machinery)
AND industry

The obtained papers are filtered using some inclusion (language, topic) and exclusion criteria (importance of the topic, open access availability, published after 2020). The PRISMA process results in 94 main papers. The number could be increased considering a wider range for the publication date or including some works not published in open access.

Below are presented the main results of the literature review. One of the key benefits of gamification-based training software is its ability to provide real-time and actionable data. Companies can track the progress of their employees at any point in their training program, identifying the causes of malfunctioning and making ad-hoc adjustments. There are some downsides to analyze. Most of the gamification applications apply together with holograms and Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) techniques. The initial capital commitment necessary to get digital and holographic instruments is quite expensive. This technique is generally costly, with high prices mainly attributed to hardware parts

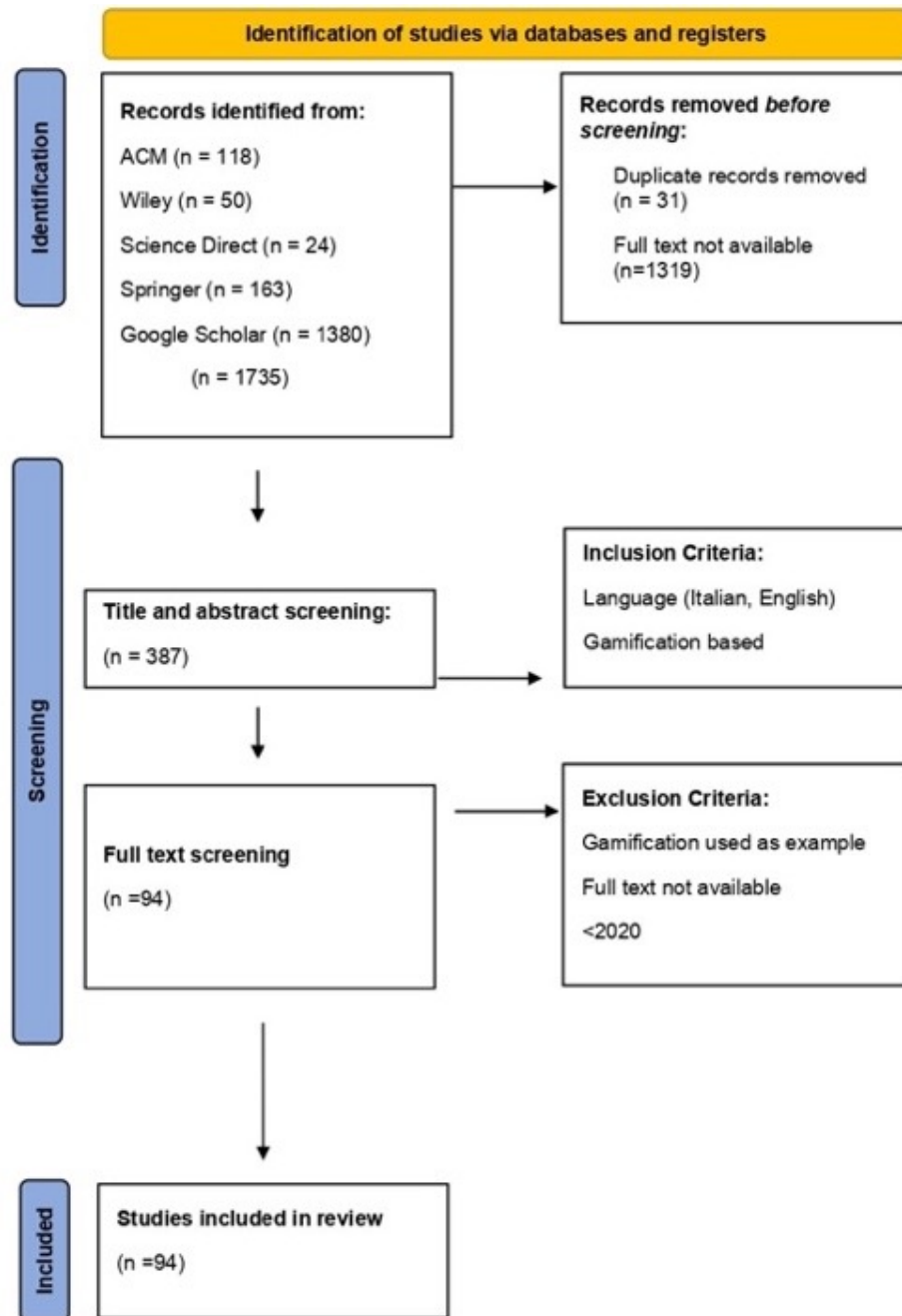


Figure 9.9: PRISMA flow diagram

and the need for specific equipment. Over time, safety training has improved together with playful solutions and augmented reality and virtual reality simulations aimed at improving teaching effectiveness. Applying the principles of gamification and using serious games to train workers in their workplace offers important benefits in terms of teaching effectiveness [4]: a) it increases worker engagement by

promoting friendly competition and reward for completing tasks; b) it spreads a culture of safety that is strongly linked to risk awareness; c) it allows to create a safe environment where workers can test their knowledge of safety procedures (e.g., company evacuation plans, firefighting activities, etc.) in realistic scenarios; d) it makes workers more alert to their behaviors and aware of the risks; e) it allows workers to practice repeatedly until they have mastered notions and procedures; f) it makes training more enjoyable and facilitates memorization and retention of information learned.

9.3 Intersection between Metaverse and LLMs

Generative AI is a broad field of artificial intelligence that includes a variety of strategies and models for generating data or content [157]. These models may generate new content from scratch, typically without direct human input or in response to precise requests. Large Language Models (LLMs) are a subset of Generative AI: they are Neural Networks trained on massive volumes of textual data collected from many sources, including online blogs, code repositories, open data, and media content. Their training is designed to teach them how to understand and generate human language. These models have shown amazing abilities in a variety of natural language processing tasks, including text production, translation, summarization, and others.

Between the different application of LLMs, we focus on Education and Training tasks, in particular in the Software Engineering topic. The main goal is to develop a digital twin of a professor, able to answer simple questions made by the course students, in an environment built in the metaverse. In this way, students can obtain a first feedback to solve their doubts regarding the course material. On the other hand, professors can better manage their time and workflow, receiving and answering only the more difficult questions.

As far as we know, this is a completely new approach in the Software Engineering Education topic. Various attempts have been conducted to generate the digital twin of a teacher: authors of paper [318] propose the digital twin of an educational institution to overcome the constraints made by COVID-19 pandemic. A similar analysis is conducted in [319]: a virtual classroom is implemented to monitor and improve public school courses. The most similar approach to the one proposed in this paper is contained in iSTAR framework [320]: this framework aims to extend the human-machine collaboration and synergy in education and collaborative teaching, exploring the advantages of integrating machines into a teaching course.

Our paper is different from the ones explained above because it takes into account the possibility to adopt LLMs to generate a more complete Digital Twin of a university teacher. Students can also interact with this teacher using immersive technologies such as Virtual Reality (VR). The final goal is to let students explore

their university in the Metaverse and chat or talk with a teacher to solve their doubts about the course material.

9.3.1 Our approach

We divide our research in three parts: identification and training of a Large Language Model, development of a Metaverse platform, and connection of the Metaverse-based avatar to the LLM through APIs. Fig. 9.10 shows the details of each step.

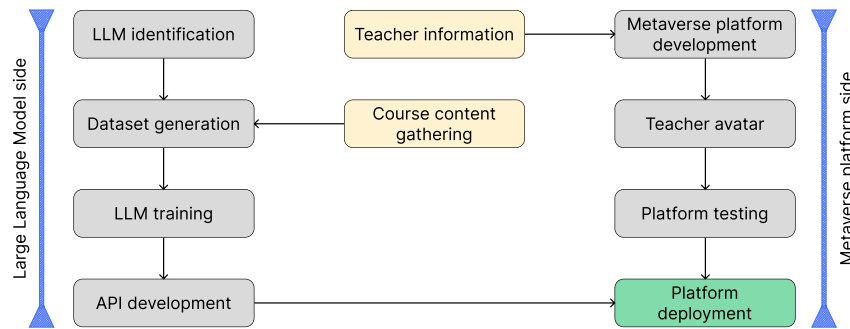


Figure 9.10: Overview of the research steps

LLM identification and training

The first step to follow to generate an AI-powered Digital Twin of a teacher is to find the most suitable LLM between the ones available online. There are various LLMs, each with its own architecture and parameters. Some notable ones include Generative Pre-trained Transformer (GPT), Bidirectional Encoder Representations from Transformers (BERT) and Llama. GPT is a model capable of generating human-like text without the need of a specific context. The last iteration of the model, GPT-4, can generate highly coherent and contextually relevant text, together with multimedia analysis [321]. BERT, on the other side, considers both preceding and following words to improve the output [322]. It is lightweight and easy to use for classification tasks [323]. Llama is defined as a collection of pretrained and fine-tuned LLMs, with a scale from 7 billion to 70 billion parameters [324]. It has been developed by Meta in 2023. Table 9.3 shows some models that fit our task, together with considerations on their parameters, the price required to use the model, the possibility to connect through APIs and the possibility to install the model in a local environment.

We choose Mistral 7b as reference LLM because it is lightweight and it becomes easier to train it based on our needs. Anyway, we plan to test our approach with different LLMs.

Table 9.3: Comparison of LLMs available online

Model name	Parameters	Price	API	Offline
GPT-3	Not known	Free as chatbot	Yes, \$	No
GPT-4	Not known	\$20/month	Yes, \$	No
LLaMa 2	7b - 13b - 70b	Free	Yes	Yes
BERT	110M - 340M	Free	Yes	Yes
Falcon	Up to 180b	Free	Yes	Yes
Mistral	7b	Free	Yes	Yes

The training phase is made by different tasks: the dataset is generated from the course material written for a Software Engineering course in the bachelor degree of Computer Science. The material is given as a single PDF file, then it is split into chunks of a defined number of tokens, where a token is equal to 0.75 words. These chunks are useful for the information retrieval part; a single chunk should be relevant to different user queries. Each chunk is then translated into an embedding, then all the embeddings are inserted into a vector database. This database can be queried using students prompts, then these prompts are embedded and checked for the most similar embedding present into the vector database. The database output can be given to the LLM as context for formulating the response. Fig. 9.11 shows the steps explained above.

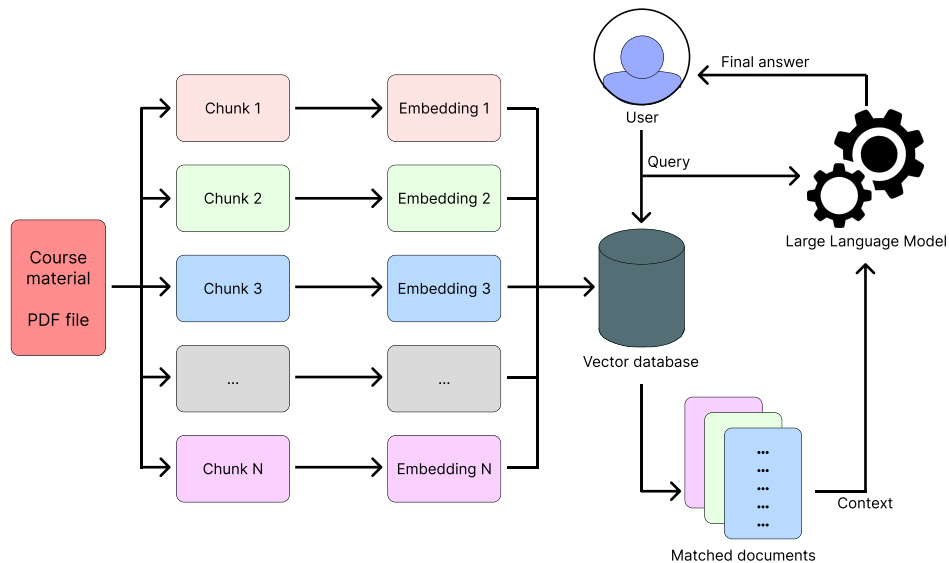


Figure 9.11: Details of the LLM training phase

The chosen LLM is used locally thanks to a GUI available on GitHub², that also makes it possible to create a local server and send prompts to the LLM using some predefined APIs.

²<https://github.com/oobabooga/text-generation-webui>

Metaverse implementation

Metaverse is particularly useful in immersive and interactive contexts, such as tourism [325] or education [326]. In the metaverse, the student will be able to formulate a question to the avatar of the teacher and receive an answer, generated by the LLM system. During the session, only the student is connected from his/her device. The question can be either written through a keyboard or expressed verbally. In fact, the metaverse platform could be exploited not only by a Head Mounted Display (HMD), but also by a desktop or mobile app because, currently, most of the students do not own an HMD. The metaverse platform will also give the possibility to have more than one student interacting with the teacher in the same room, stimulating a collaborative approach to the learning. Furthermore, it will be possible to interact also with the avatar of a fictitious student who suggests some frequently asked questions. The metaverse platform will be developed on Spatial and the integration with the LLM system will be managed in Unity through the Spatial Creator Toolkit.

The input to the LLM is sent through API calls in the form:

User input: {*USER_INPUT*}

Context: {*CHUNK_RETRIEVED_FROM_VECTOR_DB*}

The proposed approach aims to build the Digital Twin of a teacher, capable of giving an initial feedback to students doubts thanks to its underlying layer made by a LLM, in an immersive way thanks to the use of the Metaverse. Education can be improved with these technologies, both for teachers and students. Teachers can filter requests and improve their time management; students do not need to wait for an answer by the teacher, and obtain a first feedback from the Digital Twin and solve their doubts in a faster way.

9.4 Role of ChatGPT in Education

Generative AI and Large Language Models (LLMs) are increasing their popularity after the release of ChatGPT on November 2022. These models use natural language processing (NLP) techniques to take an input provided by the user and give an answer generated from scratch in human-readable form. LLMs can accomplish different tasks, from code generation [327] to text classification [328] to clinics and healthcare applications [329].

Education is a critical sector in which the usage of LLMs can result in a transformation of actual teaching techniques [330]. The field of software engineering education constantly seeks innovative approaches to enhance learning outcomes and prepare students for real-world challenges. Traditional methods of assessment often

rely on subjective judgments, which are influenced by individual biases and interpretations, and as a result, these methods may lack consistency in grading standards and depth in evaluating nuanced aspects of student performance [331, 332, 333]. However, with the advent of LLMs like ChatGPT, there lies an opportunity to revolutionize the way students engage with course content and interact with each other. By incorporating LLMs into software engineering education, educators can present students with modeling exercises solved by AI models like ChatGPT. These exercises serve as learning artifacts that students can critically evaluate and provide feedback on. Engaging in a dialogue with the AI model not only encourages students to articulate their considerations and insights but also exposes them to diverse problem-solving approaches and perspectives.

This paper aims to explore the potentialities of using ChatGPT as an assistant for the conduction of an assessment exam of a Software Engineering course. In particular, instead of using ChatGPT as an external tool, we include it in a role-playing game style test asking our students to work with it as if it was the colleague of an hypothetical company. The ultimate goal of the work is to teach students how to use a powerful tool such as Generative AI and make them aware of the potentialities and the limitations of those approaches. By leveraging LLMs in this manner, educators aim to address the shortcomings of traditional assessment methods by providing more consistent, detailed, and objective feedback to students, thereby enhancing the educational experience and preparing them for contemporary challenges in software engineering.

9.4.1 Software Engineering Education techniques

Over the 20th century, new and more performing teaching techniques and approaches have born. This has given the opportunity in the last decade to test the formulated approaches on an increasing number of students. The use of advanced computational methods in Software Engineering is not new. Various methodologies have been proposed and implemented to enhance learning and assessment processes. Although the number of innovative training approaches is high and constantly increasing, the attention of scholars has however focused more on some of them: Mastery Learning, Peer grading, Self grading and Flipped classroom. Recent studies such as the one published in 2021 in [334] have highlighted some important aspects of these teaching approaches:

- The grades assigned by the students themselves through the Self Grading approach tend to be between 8-10% higher than those assigned using the Peer Grading.
- About 25% of student groups self-evaluate with a lower rating than their peers.

- There rarely is an evaluation match between self and Peer Grading.
- Peer Grading turns out to be a good approximation of the real evaluation. In cases where the difference between Self and Peer evaluations is significant, the real evaluation lies somewhere between the two results.
- Gender and nationality do not in any way influence the results obtained by applying the didactic approaches.

Between these approaches, we focus on Peer Assessment. It is defined as a structured learning process to enable students to criticize and provide mutual feedback on their work and performance. Peer assessment helps students cultivate the ability to assess and provide feedback to others, skills that are extremely useful - if not indispensable - in the work environment. Peer evaluation has been practiced in a wide range of domains, from natural science to medicine, from engineering to business[335]. The results of a peer review typically take the form of a numerical assessment, a written commentary, or a combination of both. In addition to reducing instructor workloads, peer assessment is also believed to bring many potential benefits to student learning, including a sense of belonging and autonomy[336]. The adoption of peer assessment carries improvements in the education field. Peer assessment can:

- Enable students to take more responsibility and manage their own learning.
- Enable students to learn to assess and give constructive feedback to others to develop lifelong assessment skills.
- Enhance student learning by disseminating knowledge and exchanging ideas.
- Motivate students to engage with course material in more depth.

In order to correctly apply the teaching approach, it is important to explain and make students aware of the reason why peer evaluation is performed, illustrating the expectations and advantages of engaging in a process of this type. This aims to empower students and increase their sense of inclusion. It is also important to initially provide students with some examples of feedback of varying quality, discussing with them what type of feedback is useful and why, engaging students in a discussion of the criteria used, listening to discussions on group feedback, and providing guidance and input when needed. A possible approach to this technique is to provide the possibility for students to evaluate anonymous tasks in order to guarantee a more objective feedback, as proposed and tested in [337]. These methodologies highlight how such reflective and adaptive capabilities can be crucial in maintaining the effectiveness and reliability of systems as they adapt to different educational contexts and user interactions, underscoring the significance of implementing these principles in gamified educational platforms. This is particularly relevant to our

approach of using LLMs for peer assessment, as it emphasizes the need for systems that can dynamically adapt to provide personalized and effective feedback.

9.4.2 Related work

Current literature is growing with different proposals on mixing LLMs with Software Engineering Education techniques. Ozkaya [338] analyzes the role of LLMs in performing different Software Engineering tasks. The main identified applications range from giving real time feedbacks to developers to improved unit testing, from language translation to documentation. Software Engineering Education is considered to be one of the new development environments for LLMs. Frankford et al. [339] emphasize the transformative potential of artificial intelligence (AI) in education, particularly in programming. They highlight the significant gaps in scientific evaluation concerning the integration of Large Language Models (LLMs) into Automated Programming Assessment Systems (APASs) as AI-Tutors. Their study focuses on understanding student interactions with such AI-Tutors, using the GPT-3.5-Turbo model within the APAS Artemis. Their findings from empirical data and an exploratory survey identify distinct user types based on interaction patterns, and discuss both the advantages—such as timely feedback and scalability—and challenges, including generic responses and concerns about inhibiting learning progress. Rasnayaka et al. [340] underscore the transformative potential of LLMs in Software Engineering Education, emphasizing their capabilities in code generation despite their primary design for general language tasks. Their study involved 214 students working in teams within an academic setting where LLM integration into the development tool-chain was encouraged—a departure from traditional prohibitions. This approach allowed for an in-depth analysis of AI-generated code quality, the effectiveness of prompts used for generation, and the levels of human intervention required for code integration. Additionally, they conducted a perception study to gauge students' views on the usefulness and future applications of LLMs in software development. Their findings indicate that LLMs can significantly aid in early-stage software development by generating foundational code structures and assisting with syntax and error debugging. Kirova et al. [341] underscore the growing significance of LLMs in the era of AI, highlighting their expanding applications from content creation to advanced code completion tasks. They emphasize the unmatched opportunities presented by LLMs while acknowledging the unique challenges they pose to the software engineering domain. Their paper argues for the urgent need to adapt software engineering education to prepare future engineers for the evolving LLM environment. While existing literature and social media have explored AI's integration into education broadly, there remains a noticeable gap specifically regarding the implications of LLMs for software engineering education. Meissner et al. [342] highlight the challenges associated with manual creation of self-assessment quizzes in Software Engineering Education. They underscore the

time-consuming and cognitively demanding nature of this process, where experts must meticulously review lecture material for quiz validity. In response to these challenges, the paper proposes an innovative approach consisting in using a LLM to automate the generation of self-assessment quizzes based on lecture content. The study evaluates a prototype developed for this purpose, which was assessed by domain experts. Their findings demonstrate that automatic quiz generation significantly reduces the workload of educators while effectively covering the delivered lecture material. However, concerns are raised regarding the originality and versatility of the generated quizzes, suggesting the need for further refinement in prompt engineering to enhance the sophistication of quiz outputs. Kozov et al. [343] emphasize the rapid pace of technological change, necessitating continuous updates to university curriculums to incorporate cutting-edge technologies like LLM-powered AI. Their approach focuses on using LLM-powered tools such as Stable diffusion for AI-generated images and ChatGPT for code generation in workshops dedicated to Analysis of Software Requirements and Specifications, and Artificial Intelligence. The study includes a comparative analysis of various LLMs capable of generating images, outlining the criteria for selecting the most suitable tool. Additionally, they present student feedback indicating a positive and motivational impact during and after the workshops, underscoring the effectiveness of their educational approach. Arora et al. [344] focus on the utilization patterns of undergraduate and graduate students engaging with LLMs in advanced computing courses. They address a notable gap in the literature by conducting a detailed quantitative and qualitative analysis of direct interactions between students and LLMs within a Distributed Systems course at an Indian University. This study stands out for its inclusion of over 4,000 prompts from 411 students and interviews with 10 students, providing insights into how LLMs are employed to generate code, debug, and assist with conceptual understanding and test case generation. The findings highlight LLMs' strengths in generating boilerplate code and aiding in debugging. This paper is different from the ones found in literature because it puts LLMs at the same level of students. The proposed approach aims at teaching students how LLMs answer Software Engineering questions and how these answers can be improved, following the peer assessment technique. The final goal is to let students be aware of the opportunities and limitations of LLMs when applied to Software Engineering, also stimulating critical thinking and improving the learning experience.

9.4.3 Methodology

We aim to simulate the life inside a company by making ChatGPT a colleague of each student. In this way, students can get mutual feedbacks from the LLM and share doubts and insights on the platform they are going to model. In particular, for the assessment exam proposed in this paper, we give students the solution to a modeling problem given by ChatGPT and ask them to make improvements to that

solution, taking into account new actors and requirements, and modifying the class and sequence diagrams.

Prompt generation

We use ChatGPT 3.5 to accomplish our task. This tool offers a text2text generation, meaning that we can not send multimedia files or get images as answer, so we ask the LLM to produce the UML diagrams in PlantUML, so we can get a code that we can easily convert to a diagram³. We keep the exercise simple to avoid issues in generating the UML diagrams, as shown in [345].

We tested different prompts to obtain the best solution to the proposed exercise. Throughout our experimentation, we observed that using the same prompt could yield different outcomes across different sessions, underscoring the inherent variability in LLM responses influenced by factors such as model initialization and context. Moreover, our findings indicated that employing more detailed prompts often resulted in solutions that closely adhered to the specific instructions provided but tended to limit the creativity and flexibility of the generated answers. This observation stems from the nature of LLMs, which, while capable of generating precise and contextually relevant responses with detailed prompts, may prioritize conformity to explicit instructions over innovative problem-solving approaches. Thus, while detailed prompts can enhance accuracy in certain contexts, they may inadvertently restrict the breadth of potential solutions. This trade-off between specificity and creativity underscores the need for a balanced approach in prompt design when utilizing LLMs for educational exercises. The prompt used for the generation of the solution is the following: *From now on, you are an expert in the field of Software Engineering and platform modeling through UML. I send you an exercise and you have to solve it giving me: a list of functional and non functional requirements following the FURPS+ paradigm; a list of actors and use cases; a class diagram; a sequence diagram of one of the use cases. Give me the diagrams in PlantUML. The exercise is as following: you want to model a platform for booking appointments with a professor or one of his or her assistants in your university. The professor should be able to insert his or her preferred time, date, and mode (in presence or online). Each assistant should be able to modify those information to accomodate his or her needs. Students should be able to see all available appointments, book a time slot and choose the preferred mode between the available ones. Model the platform starting from the functional and non functional requirements, a list of actors and use cases, a class diagram and the sequence diagram of the use cases "Booking an appointment".* We slightly modified the prompt to obtain the best result: after the first generation, we asked ChatGPT to give detailed results for each diagram.

³<https://www.gituml.com/plantuml>

The choice of prompt complexity plays a crucial role in the quality and specificity of the generated outputs when utilizing generative AI for educational purposes. As observed in our study, prompts with fewer details tend to produce more general use cases, as shown by the absence of certain scenarios such as the login use case in Figure 9.13, compared to Figure 9.12. However, this simplicity comes at the cost of generating more basic descriptions, such as the lack of methods implementation in the class diagram in Figure 9.12. In navigating this trade-off, we have opted to provide students with the answers generated by prompts detailed in Section 9.4.3. Despite not being flawless, we have found this approach to be the most suitable for our educational objectives. By presenting students with these generated solutions, we afford them the opportunity to comprehend proposed use cases and diagrams while critically evaluating the output of the generative AI model. This not only facilitates an understanding of fundamental concepts but also encourages students to explore more efficient approaches to accomplish various tasks within the software engineering domain.

Outputs given by the LLM

The chosen solution to submit to the course students are shown as follows: ChatGPT gives a list of four main functional requirements divided in a total of 26 atomic requirements. Then, it gives a list of non functional requirements, written following the FURPS+ paradigm.

1. Booking System

(a) Professor Actions

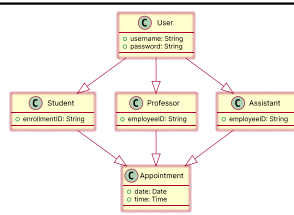
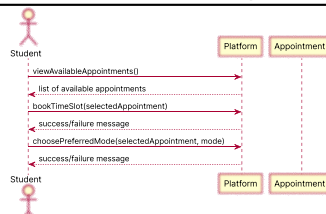
Prompt	Functional requirements	UML class diagram
From now on, you are an expert in the field of Software Engineering and platform modeling through UML. I send you an exercise and you have to solve it giving me: a list of functional and non functional requirements following the FURPS+ paradigm; a list of actors and use cases; a class diagram; a sequence diagram of one of the use cases. Give me the diagrams in PlantUML. The exercise is as following: you want to model a platform for booking appointments with a professor or one of his or her assistants in your university.	1. Appointment Booking: • Users should be able to schedule appointments with professors or their assistants. • The system should allow users to specify the date and time for the appointment. 2. User Authentication: • Users must log in to the platform using university credentials to book appointments. 3. Professor/Assistant Availability: • The system should display the availability of professors and assistants for booking. 4. Appointment Notification: • Users should receive notifications about their upcoming appointments.	
		UML sequence diagram 

Figure 9.12: Solution generation: first prompt with less details

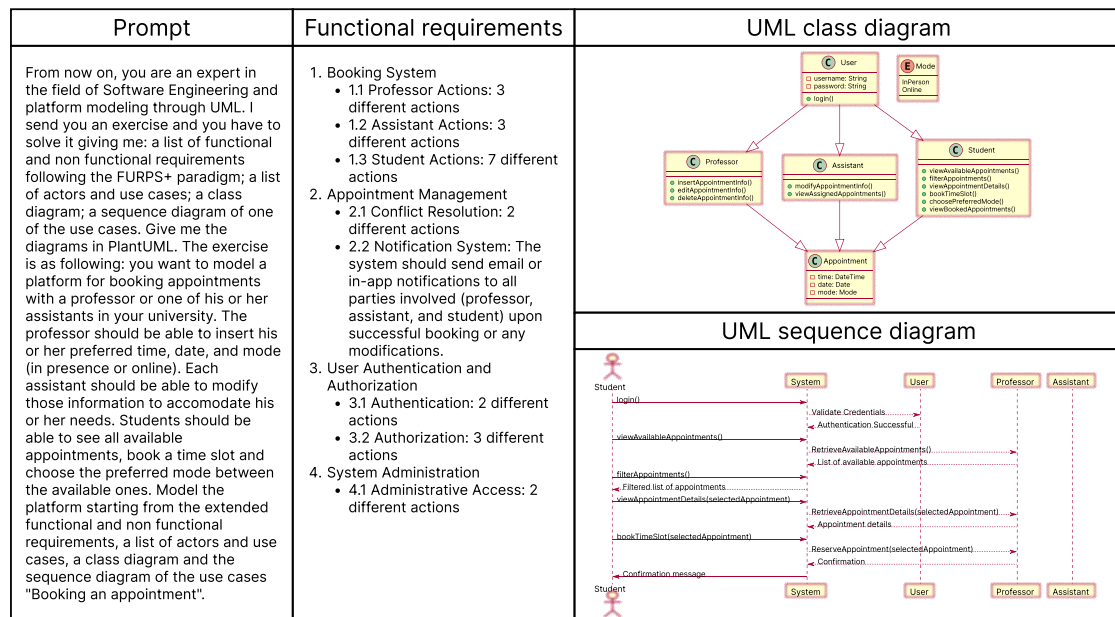


Figure 9.13: Solution generation: second prompt with extended details

- Professors can log in to the system using their credentials.
- Professors can insert their preferred appointment details, including date, time and mode (in person or online).
- Professors can edit or delete their existing appointments.

(b) Assistant Actions

- Assistants can log in to the system using their credentials.
- Assistants can modify the appointment information provided by the professor to accommodate their own schedules.
- Assistants can view the appointments they are assigned to.

(c) Student Actions

- Students can log in to the system using their credentials.
- Students can view a list of available appointments.
- Students can filter available appointments based on date, time, and mode.
- Students can select a specific appointment to view more details.
- Students can book a time slot for an available appointment.
- Students can choose the preferred mode (In Person or Online) for the booked appointment.
- Students can view their booked appointments and their details.

2. Appointment management

(a) Conflict resolution

- i. The system should check for conflicts when a new appointment is added.
- ii. If a conflict is detected, the system should notify the relevant parties (professor, assistant, and student) and suggest alternative slots.

(b) Notification system

- i. The system should send email or in-app notifications to all parties involved (professor, assistant, and student) upon successful booking or any modifications.

3. User Authentication and Authorization

(a) Authentication

- i. Users (professors, assistants, and students) must authenticate themselves with valid credentials to access the system.
- ii. Passwords must be securely stored using encryption.

(b) Authorization

- i. Professors can only modify their own appointments.
- ii. Assistants can only modify appointments assigned to them.
- iii. Students can only book and modify their own appointments.

4. System Administration

(a) Administrative Access

- i. The system should provide administrative access for system administrators to manage user accounts, resolve conflicts, and monitor system health.
- ii. Administrators can view logs and reports on system activities.

The class diagram proposed by ChatGPT represents 5 classes: user, assistant, professor, student, and appointment. The User class represents common attributes and actions shared by professors, assistants, and students. Each user type (Professor, Assistant, Student) inherits from the User class. Each class has its own methods (i.e.: the Professor can insert appointment info, while the Student can filter available appointments). The class diagram is shown in Fig. 9.14.

The sequence diagram shows an actor and four participants. It includes the login process for the student before accessing appointment-related functionalities. It also includes additional actions like filtering appointments, viewing appointment details, and viewing booked appointments. These actions provide a more detailed

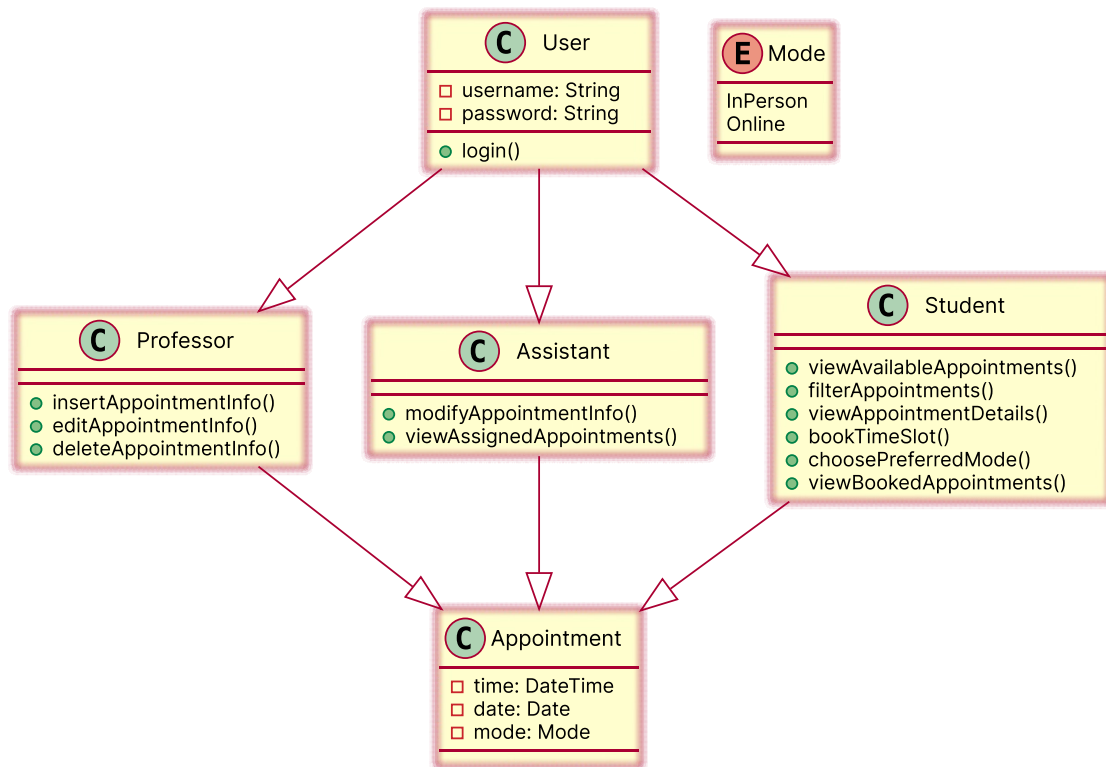


Figure 9.14: Class diagram generated by ChatGPT

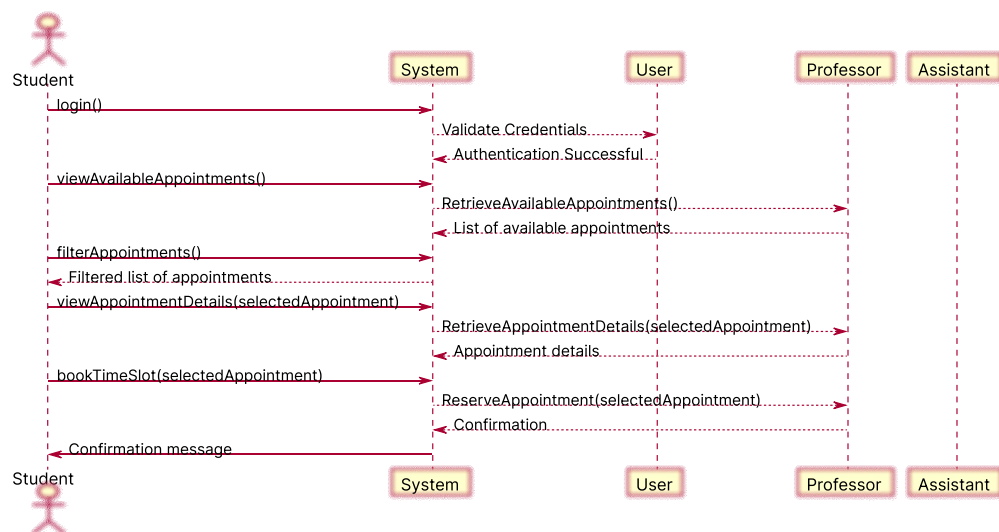


Figure 9.15: Sequence diagram generated by ChatGPT

flow of interactions during the *Booking an Appointment* use case. The diagram is shown in Fig. 9.15. The modeling phase provided by ChatGPT presents some

inconsistencies: for example, the sequence diagram does not use the Assistant lifeline, meaning that the Student cannot book a time slot with a professor assistant without seeing it between the professor available timeslots. Moreover, the class diagram does not specify attributes for Professor, Assistant and Student classes, excluding the possibility to use university credentials or data to characterize those actors. We do not ask ChatGPT to make improvements on these aspects because one of the goals of peer assessments is to discuss a provided solution, that could not be the most efficient for the platform needs. For this reason, we let students analyze this modeling and try to understand the possible improvements to make on the requirements and diagrams.

9.4.4 Results

The main question we want to answer is: how does providing an AI-generated solution compare to one generated by a human in which errors or inconsistencies in the model have been carefully crafted to make students realise about potential mistakes?

To give a comprehensive answer, we selected an experimental group that had to comment an AI-generated exercise solution. The test has been carried out by a total of 141 students in a given time of 90 minutes. The time given to students is the same time given for a traditional exam test.

In order to evaluate the outcomes of the experiment, a dual approach combining qualitative and quantitative analyses was employed. Qualitative insights were gathered to capture the nuanced experiences and attitudes of the students towards the AI-integrated educational approach. Feedbacks were obtained regarding the students' perceptions, challenges encountered, and potential benefits of interacting with ChatGPT through a survey. These qualitative findings provide rich contextual information, offering insights into the effectiveness of the AI-integrated approach from a student perspective. Additionally, a quantitative analysis was conducted to measure the improvement in learning effectiveness resulting from the intervention. By comparing pre- and post-intervention performance metrics, such as test scores, completion rates, and engagement levels, quantitative data was used to assess the extent to which the AI-integrated approach contributed to enhanced learning outcomes.

Qualitative analysis

The main observations on the control group are summarized below:

- Students proved to be able to find incongruities in ChatGPT resolution of the exercise. For instance, there were no login options in the platform, or there were some theoretical mistakes in the sequence diagram definition.

- All students completed the test in the given amount of time. The average completion time is 87.36 minutes, with a standard deviation of 4.94 minutes.
- Students were motivated to understand the reasons behind ChatGPT resolution, going over the simple exam.
- Students tried to think about each answer after the exam, creating some focus groups in which they explained some modeling choices and some constraints on the exam.

Table 9.4: Feedback form questions and answers

Question	Description	Answer
How easy was it to understand the UML solution generated by ChatGPT?	1 - Very difficult 10 - Very easy	Median value: 7.46
Were the elements of the diagrams clear and well structured?	1 - Very unclear 10 - Very clear	Median value: 7.62
If there were errors or ambiguities, do you think they were due more to limitations of the algorithm or to a misinterpretation of the exercise?	1 - Algorithm limitation 10 - Exercise misunderstanding	Median value: 5.57
Do you think this exercise contributed to your understanding of natural language generation tools, particularly ChatGPT, in software engineering contexts?	Yes: 127, No: 14	
Have you ever participated in similar exercises involving human-generated solutions or other tools?	Yes: 16, No: 125	
Have you thought about using ChatGPT (or similar) BEFORE reading the exercise?	1: Absolutely not 10: Absolutely yes	Median value: 4.58
Have you thought about using ChatGPT (or similar) AFTER reading the exercise?	1: Absolutely not 10: Absolutely yes	Median value: 3.96
What types of material did you find most useful in solving the exam?	Personal skills: 78; Course slides: 36;	Online searching: 14; Generative AI tools: 13

A survey has been conducted to understand how students reacted to this innovative approach to the course. The form collects answers regarding the quality,

validity, and clarity of the peer assessment technique applied through ChatGPT. It also identifies ambiguities or limitations, together with suggestions for improvement ⁴. Table 9.4 shows the main results of the form, answered by all 141 students, while Fig. 9.17 and Fig. 9.16 describe some key parameters of the survey. The exercise solution provided by ChatGPT is quite easy to understand and diagrams are aligned with the course theory. Students claim to be more aware of Generative AI after the assessment exam, even if this is the first time they approached with such methodology. Some significant comments left by students after the assessment exam are listed below. To ensure relevance and depth, we filtered out comments that merely expressed generic approval such as "I liked it" without providing substantive insights. The selected comments were chosen based on their ability to offer constructive feedback, identify specific aspects of the exam experience that impacted learning, or suggest improvements for future assessments.

- I believe the method used today is more effective, as I believe that AI is the future and we will find ourselves increasingly forced to use these technologies. Therefore, understanding that this technology must always be supervised by us makes me understand that our knowledge must always have a solid basis because even an AI can make mistakes.
- I think it was very effective to evaluate a test carried out by an artificial intelligence. In fact, AI compiles the structure of the platform and leaves room for creativity for further implementations.
- I believe that involving solutions generated by LLM is very effective, as it trains critical thinking and above all the grasp of inconsistent information (for example information that could appear in the class diagram but not in the requirements and vice versa). This is a skill that I think is crucial if we want to use ChatGPT or similar algorithms in industries.
- ChatGPT can give a big hand in the initial drafting of the resolution of a problem, but in my opinion it cannot yet replace the human mind for a complete and elaborate resolution
- The activity is very engaging and interesting because it is very different from classic exams and "forces" you to test yourself and, in this case, analyze the chosen model from your personal point of view.

⁴Results of the feedback form are available at https://politecnicobari-my.sharepoint.com/:x:/g/personal/marco_fiore_poliba_it/EfHYiLFKn25ChG_Mk8xLVkUBz600a1_PTaQTCLpGuVHMaQ?e=ynZWSe

- I have not found many positive aspects in using ChatGPT, the solution provided by the latter is absolutely appreciable, but it does not meet all the functional and non-functional requirements that an exercise of this type should have.
- It has been a really interesting activity! It is strange to think that up until a year ago it wouldn't have been possible to make such exam.

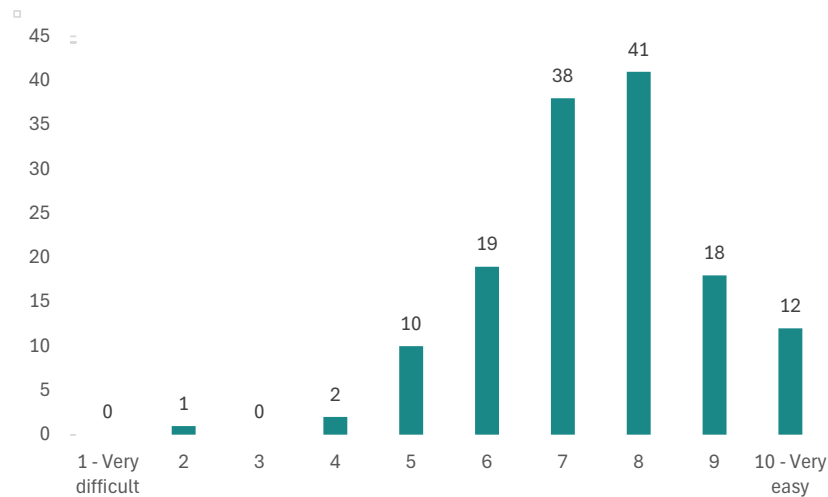


Figure 9.16: Answers for form question: How easy was it to understand the UML solution generated by ChatGPT?

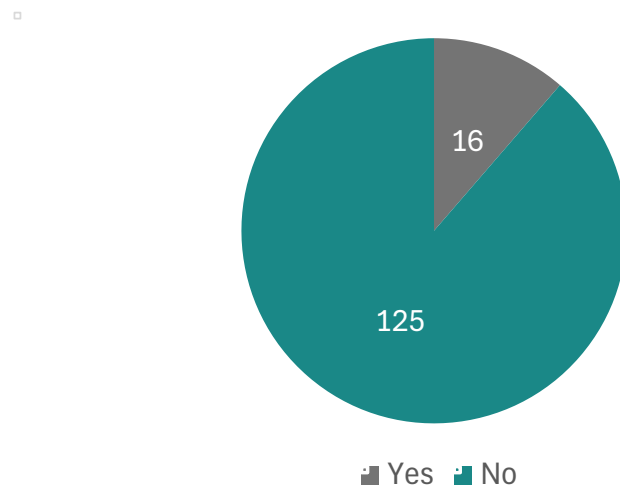


Figure 9.17: Answers for form question: Have you ever participated in similar exercises involving human-generated solutions or other tools?

In the analysis of the survey responses, a prevailing sense of positivity emerged, characterized by expressions of joy, satisfaction, and enthusiasm. Many students

show their excitement and appreciation for the discussed topics. However, alongside these positive sentiments, fear or apprehension has been detected, particularly concerning the potential outcomes or implications of the applied methodology. Some students express concerns or uncertainties about the future based on the results of the analysis. Such findings offer a deeper understanding of how the application of Generative Artificial Intelligence in Education courses is perceived and received by students.

Out of the 141 students participating in the exercise, only a small fraction, specifically 13, chose to delve deeper into their interaction with ChatGPT after the initial stage. These students exhibited a distinct eagerness to not only understand the solution presented by ChatGPT but also to explore additional insights and novel approaches to tackle the challenges and constraints posed by the exercise. Their decision to continue the conversation with ChatGPT reflects a proactive attitude towards learning. By actively seeking out further guidance and feedback from ChatGPT, these students showcase a readiness to embrace innovative learning tools and harness the potential of AI-driven educational platforms.

Quantitative analysis

The quantitative analysis of the experiment gives interesting insights on the impact of the LLM-based educational approach. Pre- and post-intervention assessments were conducted to measure changes in key performance indicators among the participating students. Statistical analysis revealed a significant improvement in learning outcomes following the implementation of the AI-integrated methodology. Specifically, the medium score of the pre-intervention test is 27.06 out of a total of 30 points, while the medium score of the post-intervention test is 28.51 out of 30 points, demonstrating an average increase of 1.5 points (+4.83%) and indicating a substantial enhancement in students' mastery of the subject matter. This trend is shown in Fig. 9.18.

Moreover, completion rates of assignments and exercises witnessed a notable increase for post-intervention in the number of tasks completed compared to the pre-intervention period, from a medium value of 83.97% completion to a medium value of 94.75% completion (+10.78%). This uptick in completion rates suggests a heightened level of engagement and commitment among students towards the AI-integrated learning activities. A summary of this result is shown in Fig. 9.19.

These quantitative findings provide empirical evidence of the efficacy of the AI-integrated approach in fostering enhanced learning outcomes and promoting active student participation within the educational setting.

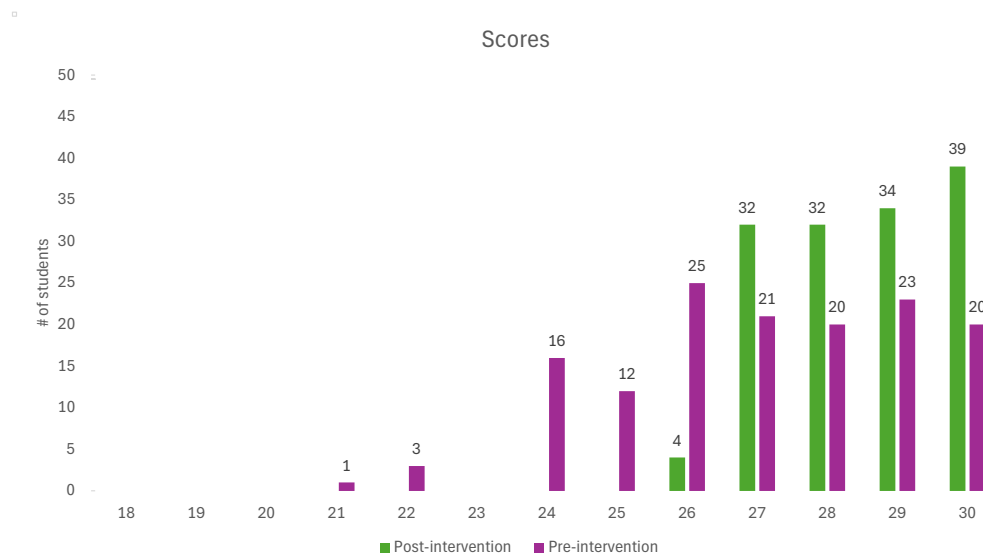


Figure 9.18: Scores obtained by students in pre- and post-intervention assessment

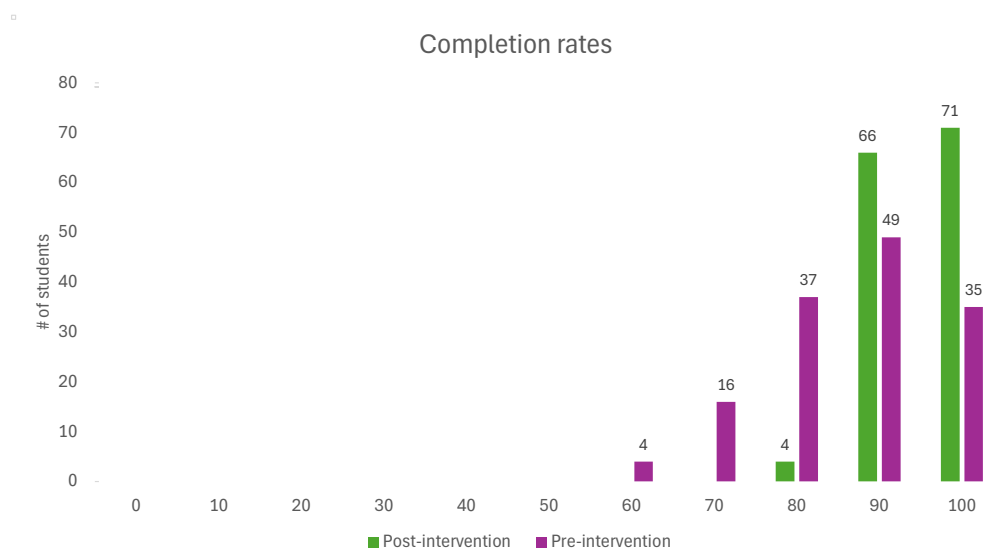


Figure 9.19: Completion rate in pre- and post-intervention assessment

9.4.5 Threats to validity

In this study, we identified some potential threats to validity and implemented measures to mitigate them. These threats are analyzed as follows:

- **Selection Bias:** Participation in continued interaction with ChatGPT could raise the possibility that more motivated or higher-performing students opted in, potentially skewing results. To counteract this, we selected students from the same bachelor's degree course, to ensure a balanced starting performance level.
- **Generalizability:** The study was conducted in a specific educational context and may not be generalizable to other settings or disciplines. Future research will replicate the study across different universities and subjects to validate the findings.
- **Sample Size:** The relatively small number of students who continued engaging with ChatGPT might limit the generalizability of the results. Increasing the sample size in future studies will help enhance external validity.
- **Usage of metrics and qualitative measures:** Engagement and learning effectiveness were measured using specific indicators like test scores and completion rates. While these metrics are common, they might not capture all dimensions of these constructs. The inclusion of qualitative measures such as student interviews and surveys provide additional insights into student engagement and learning experiences.
- **Intervention Fidelity:** Ensuring consistent implementation of the AI-integrated approach across all participants is crucial. Regular checks and standard guidelines were put in place to ensure uniform application of the intervention.

By identifying and addressing these threats, we aim to enhance the robustness and reliability of our findings. Continuous evaluation and refinement of our methods will further strengthen the validity of future studies.

Peer assessment serves as a valuable educational tool, encouraging students to think critically about their modeling choices within the realm of Software Engineering. By moving beyond the confines of traditional exams, peer assessment fosters active engagement and prompts students to consider diverse perspectives and approaches. The integration of ChatGPT as a peer reviewer introduces an innovative and interactive dimension to this process, offering students a novel opportunity to evaluate their peers' work and receive feedback from an AI "colleague"[346]. However, while ChatGPT presents exciting possibilities for enhancing peer assessment, it is essential to recognize the unique role of human creativity in UML modeling. Generative AI, while powerful, cannot replicate the depth and nuance of human thought and creativity in this domain. Human intervention remains indispensable for crafting engaging and diverse learning experiences that stimulate students' imagination and problem-solving skills.

As we look toward future research directions, there is a need to explore additional scenarios where ChatGPT's features can be effectively applied in educational settings. For example, investigating the feasibility of enabling students to engage in dialogue with ChatGPT about its exercise solutions, while maintaining the conversational context established by the instructor, presents an intriguing avenue for exploration. Addressing the challenge of contextual awareness in AI-generated interactions represents a key research frontier in this topic [347]. Even innovative technologies such as Metaverse can take advantage of LLMs and, if used in the education sector, can contribute to the creation of engaging and immersive experiences for learners [325]. While acknowledging the imperfections inherent in AI-generated outputs, we believe that the benefits of leveraging generative AI for educational purposes outweigh the limitations. By harnessing the power of AI technologies in conjunction with traditional pedagogical methods, educators can cultivate a dynamic and interactive learning environment that empowers students to actively participate in their learning journey and develop essential skills for success in the field of software engineering.

Chapter 10

Conclusion and future research directions

This dissertation has delved into the potential of Blockchain technology, with an emphasis on its application to agri-food traceability and contributions to Software Engineering Education and Training (SEET). The research presented here covers a broad spectrum of the current state and potential advancements in Blockchain, identifying key challenges and providing solutions in terms of security, privacy, architecture, and complementary technologies.

10.1 Blockchain and agri-food traceability

The research has been carried out following a systematic research and the design and development of agri-food traceability platforms. The findings from these studies underscore Blockchain's capability to foster trust and transparency across sectors, specifically in the agri-food industry. By enabling secure and immutable traceability, Blockchain enhances consumer confidence in product authenticity while streamlining supply chain management for producers. The research's theoretical and practical components have been instrumental in modeling Blockchain-based traceability platforms, catering to the needs of both producers and consumers and facilitating transparent information sharing.

In addressing the challenges presented by Blockchain adoption, this dissertation has investigated quantum-safe encryption algorithms and alternative architectures. Then, architectural improvements have been proposed, from the coexistence of private and public Blockchains in a single workflow to the integration of Blockchain and NoSQL databases in a hybrid framework, together with Blockchain implementations on IoT devices.

Additionally, the exploration of emerging technologies, such as Augmented Reality (AR) and Large Language Models (LLMs), highlights Blockchain's expanding

potential to adapt to diverse domains, including digital tourism and SEET. The study has further demonstrated that integrating Blockchain with these technologies can significantly enhance platform usability, accessibility, and efficiency.

The baseline of Blockchain-based traceability application is shown in Fig. 10.1. These architectures include the producer and the final customer, with the possibility of expanding the producer in some sub-actors. In the distributed system, each actor serves as a node. All immutable traceability information is accessible to the end user through their device, usually via an RFID tag or QR code. New data is then entered by the producer and controlled by pre-established smart contracts. The accuracy of the data being added to the Blockchain is guaranteed by these smart contracts.

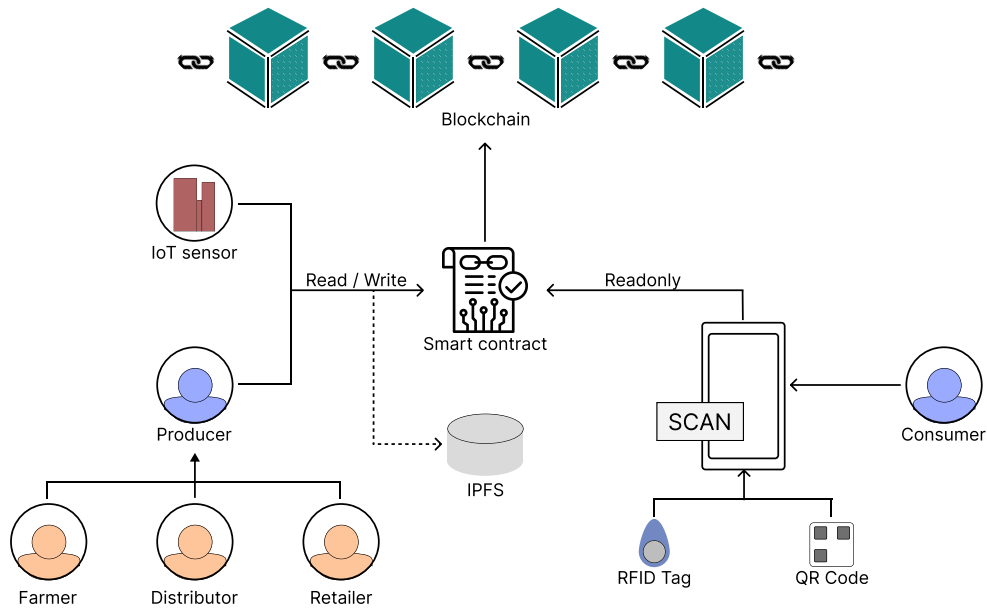


Figure 10.1: Blockchain-based platforms common architecture

The work conducted during the PhD program allowed the design of a more complex architecture, that is still a work in progress, shown in Fig. 10.2. The proposed architecture integrates several key components to enhance traceability in agri-food systems, emphasizing both consumer interaction and secure data management.

- Public Blockchain and Private Blockchains:** This architecture utilizes a hybrid Blockchain model, combining public and private Blockchains to balance transparency and data privacy. The public Blockchain, accessible to consumers, ensures immutability and transparency, while private Blockchains handle sensitive or enterprise-specific data, shared among producers, distributors, and retailers. Each actor in the supply chain (e.g., farmer, distributor, retailer) interacts with this hybrid system, governed by smart contracts that

regulate data exchange across both Blockchain types, optimizing workflow control.

- **Smart Contracts:** Smart contracts automate data validation and ensure that information being added to the Blockchain aligns with pre-defined rules. These contracts facilitate secure, tamper-resistant interactions across supply chain stages, making data entries reliable and traceable from production to consumer access.
- **Consumer and Producer Interfaces:** The architecture includes separate front-end interfaces for producers and consumers, enhancing usability and engagement for each user group. Producers use the interface to manage data entries, while consumers access product information by scanning a QR code or RFID tag, which connects them to the Blockchain and reveals traceability data.
- **Digital Twin System:** A digital twin replicates each product's journey in virtual space, connecting to sensors in the physical supply chain. It allows real-time tracking of product conditions and events. The AR System complements the digital twin by enhancing the user's physical-world interaction with traceability data, facilitating an interactive and informative experience.
- **Edge Computing and Sensors:** Distributed sensors and edge nodes capture real-time data from each stage of the supply chain (e.g., temperature, humidity, location). This data is processed at the edge, minimizing latency and network load, and then selectively transferred to the Blockchain via smart contracts. Edge computing enables efficient data handling while ensuring data integrity and traceability.
- **Large Language Models and InterPlanetary File System:** The architecture also employs LLMs and IPFS to enhance accessibility and storage efficiency. LLMs provide advanced interaction capabilities, assisting consumers by interpreting and explaining Blockchain data, potentially in a conversational format. IPFS supports decentralized storage of large files, like 3D models or high-resolution images linked to the digital twin, ensuring scalability and reducing storage demands on the Blockchain.

This architecture balances transparency, security, and scalability, addressing agri-food traceability's unique demands. It reflects a comprehensive approach, supporting producers and consumers alike in fostering a more informed, reliable, and interactive traceability experience.

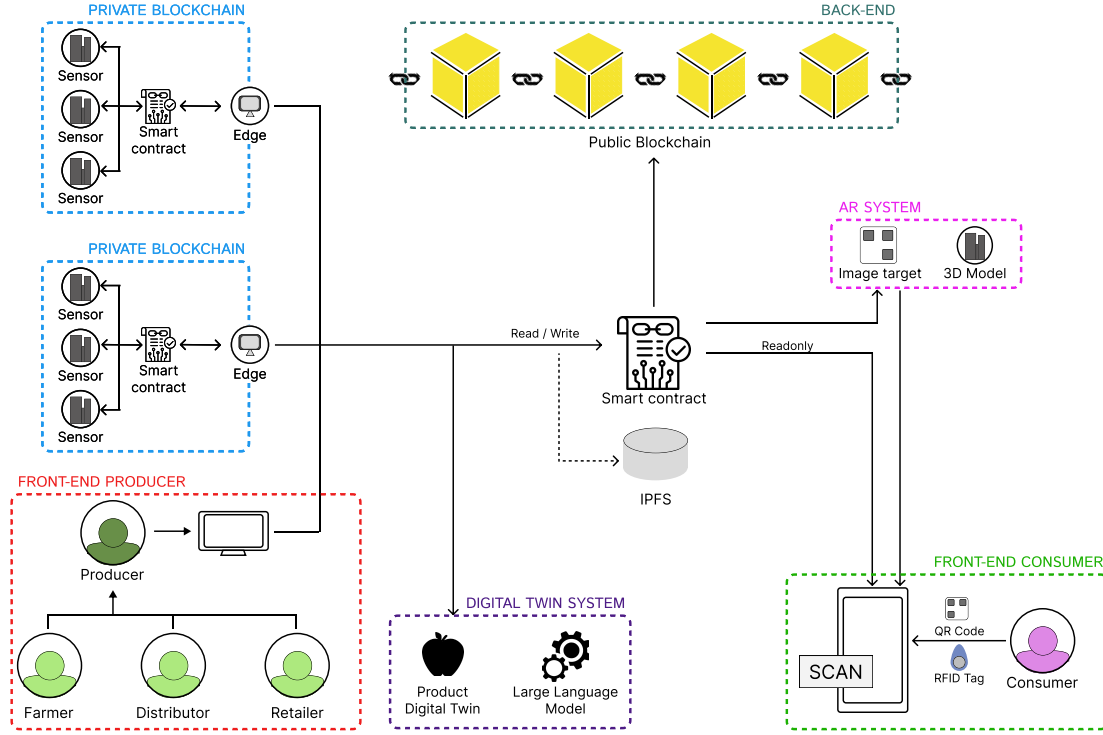


Figure 10.2: Work in progress novel architecture

10.2 Software Engineering Education and Training

The secondary focus on SEET has brought valuable insights into innovative teaching strategies that can enhance engagement, comprehension, and skill acquisition in Software Engineering courses. One prominent approach explored during the PhD program is gamification, where game-based elements such as points, levels, and rewards are integrated into educational environments. This method motivates learners by creating a competitive yet collaborative atmosphere, which has been shown to improve students engagement and deepen understanding of complex technical concepts.

Peer assessment facilitated by LLMs represents another significant advancement. In this approach, LLMs assist in providing feedback on assignments and projects, enabling students to engage in critical reflection while benefiting from structured, AI-enhanced insights. LLM-powered assessments can streamline grading, promote fairness, and facilitate scalable assessment, especially in large classes. This encourages students to learn from one another, develop a sense of accountability, and enhance their evaluative skills, essential for both teamwork and independent work in professional settings.

10.3 Open challenges

The research conducted during these three years opens lots of possibilities; some of them are proposed below.

- **Support decision tool for new Blockchain developers:** As Blockchain technology continues to evolve, developers, particularly those new to the field, face challenges in choosing suitable Blockchain architectures, consensus mechanisms, and security protocols. A support decision tool tailored for novice Blockchain developers could streamline the selection process by recommending architectures based on the project requirements and environmental constraints. Such a tool could integrate a knowledge base with practical examples and best practices, helping developers make informed decisions, reduce development time, and avoid common implementation pitfalls.
- **Automatic generation of smart contracts through Large Language Models (LLMs):** The manual creation of smart contracts requires technical expertise and can be error-prone. Leveraging LLMs for the automatic generation of smart contracts offers a promising solution to simplify this process. Future research could focus on training LLMs with extensive smart contract data and industry-specific requirements to automatically produce secure and efficient contract code. Such advancements could make smart contract creation more accessible to non-experts, enhance development efficiency, and reduce risks associated with coding errors.
- **Integration of Blockchain in Internet of Drones (IoD):** With the increasing deployment of drones in applications ranging from logistics to environmental monitoring, secure and transparent data management is essential. Integrating Blockchain technology within the Internet of Drones (IoD) could provide a decentralized, tamper-proof infrastructure for tracking drone operations, data exchanges, and compliance with regulatory requirements.

In conclusion, this dissertation lays a foundation for future research in Blockchain interoperability. The findings and frameworks proposed here will hopefully contribute to a more robust, transparent, and adaptable Blockchain ecosystem, offering significant advancements to the agri-food sector and beyond.

Bibliography

- [1] M. Fiore and M. Mongiello, “History of Blockchain Technology and its Impact in Social Good,” in *2023 8th IEEE History of Electrotechnology Conference (HISTELCON)*, pp. 36–38, Sept. 2023.
- [2] M. Fiore and M. Mongiello, “Blockchain Technology to Support Agri-Food Supply Chains: A Comprehensive Review,” *IEEE Access*, vol. 11, pp. 75311–75324, 2023.
- [3] M. Fiore, M. Frem, M. Mongiello, F. Bozzo, C. Montemurro, G. Tricarico, and A. Petrontino, “Blockchain-based food traceability in Apulian marketplace: Improving sustainable agri-food consumers perception and trust,” *Internet Technology Letters*, p. e503, 2024.
- [4] M. Fiore, M. Mongiello, G. Tricarico, F. Bozzo, C. Montemurro, A. Petrontino, C. Giambattista, and G. Mercuri, “Blockchain-based Food Traceability System for Apulian Marketplace: Enhancing Transparency and Accountability in the Food Supply Chain (S).,” in *2023 35th International Conference on Software Engineering and Knowledge Engineering (SEKE)*, pp. 114–117, 2023.
- [5] M. Fiore, F. Carrozzino, M. Mongiello, G. Volpe, and A. M. Mangini, “A Blockchain-Based Modular Architecture for Managing Multiple and Quantum-Safe Encryption Algorithms,” in *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, pp. 598–601, July 2023.
- [6] M. Fiore, F. Carrozzino, M. Mongiello, and F. Nocera, “Key-pair Generation using Fingerprint-based Seed in Blockchain Systems,” in *Blockchain & Cryptocurrency Conference (B2C’ 2022)*, p. 112, 2022.
- [7] F. Nocera, S. Abascià, M. Fiore, A. A. Shah, M. Mongiello, E. Di Sciascio, and G. Acciani, “Cyber-Attack Mitigation in Cloud-Fog Environment Using an Ensemble Machine Learning Model,” in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, July 2022.
- [8] M. Fiore, M. Mongiello, and G. Acciani, “A context-aware multiple Blockchain architecture for managing low memory devices,” in *2023 8th International*

- Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, June 2023.
- [9] A. Longo, A. Di Palma, L. Casamassima, M. Fiore, and M. Mongiello, “Blockchain and NoSQL: Enhancing throughput via a deep learning-based hybrid architecture,” *Internet Technology Letters*, 2024.
 - [10] M. Fiore, F. Nocera, and M. Mongiello, “A Reward-based Blockchain Platform for Exchanging Goods and Services,” in *Blockchain & Cryptocurrency Conference (B2C’ 2022)*, p. 45, 2022.
 - [11] M. Fiore and M. Mongiello, “Blockchain for Smart Cities Improvement: An Architecture Proposal,” in *2023 7th International Conference on Computer, Software and Modeling (ICCSM)*, pp. 1–5, July 2023.
 - [12] G. Spadavecchia, M. Fiore, M. Mongiello, and D. De Venuto, “A Novel Approach for Fast and Secure Data Transmission using Blockchain and IoT,” in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–4, June 2024.
 - [13] S. Bistarelli, M. Fiore, A. I. Lazzizzera, I. Mercanti, and M. Mongiello, “Analysis of Blockchain Sustainability through the Comparison of Different Smart Contracts Programming Languages,” in *6th Distributed Ledger Technology Workshop (DLT 2024)*, vol. 3791, (Turin, Italy), pp. 1–11, 2024.
 - [14] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, “Edge Computing and Cloud Computing for Internet of Things: A Review,” *Informatics*, vol. 11, p. 71, Dec. 2024.
 - [15] E. C. Ciliberti, M. Fiore, and M. Mongiello, “Development of a Metaverse Platform for Tourism Promotion in Apulia,” in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pp. 680–681, June 2023.
 - [16] M. Fiore, M. Gattullo, and M. Mongiello, “First Steps in Constructing an AI-Powered Digital Twin Teacher: Harnessing Large Language Models in a Metaverse Classroom,” in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 939–940, Mar. 2024.
 - [17] M. Fiore, M. Gattullo, M. Mongiello, and A. Uva, “Merging Blockchain and Augmented Reality for an Immersive Traceability Platform,” in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 933–934, Mar. 2024.
 - [18] V. Di Nardo, R. Fino, M. Fiore, G. Mignogna, M. Mongiello, and G. Simeone, “Usage of Gamification Techniques in Software Engineering Education and Training: A Systematic Review,” *Computers*, vol. 13, p. 196, Aug. 2024.
 - [19] M. Fiore and M. Mongiello, “Gamification for Machinery and Infrastructure Learning in Industries: A Review,” in *Automation, Robotics & Communications for Industry 4.0/5.0*, p. 157, 2023.
 - [20] M. Fiore and M. Mongiello, “Using Peer Assessment Leveraging Large Language Models in Software Engineering Education,” *International Journal of*

- Software Engineering and Knowledge Engineering*, July 2024.
- [21] D. L. Chaum, *Computer Systems established, maintained and trusted by mutually suspicious groups*. Electronics Research Laboratory, University of California, 1979.
 - [22] S. Haber and W. S. Stornetta, *How to time-stamp a digital document*. Springer, 1991.
 - [23] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized business review*, 2008.
 - [24] V. Buterin *et al.*, “Ethereum white paper,” *GitHub repository*, vol. 1, pp. 22–23, 2013.
 - [25] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the thirteenth EuroSys conference*, pp. 1–15, 2018.
 - [26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, 2017.
 - [27] X. Xu, I. Weber, and M. Staples, *Architecture for blockchain applications*. Springer, 2019.
 - [28] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, “Survey on blockchain for internet of things,” *Computer Communications*, vol. 136, pp. 10–29, 2019.
 - [29] K. Wüst and A. Gervais, “Do you need a blockchain?,” in *2018 crypto valley conference on blockchain technology (CVCBT)*, pp. 45–54, IEEE, 2018.
 - [30] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, “A taxonomy of blockchain-based systems for architecture design,” in *2017 IEEE international conference on software architecture (ICSA)*, pp. 243–252, IEEE, 2017.
 - [31] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.
 - [32] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and informatics*, vol. 36, pp. 55–81, 2019.
 - [33] R. Martino and A. Cilardo, “Designing a sha-256 processor for blockchain-based iot applications,” *Internet of Things*, vol. 11, p. 100254, 2020.
 - [34] K. Devika and R. Bhakthavatchalu, “Parameterizable fpga implementation of sha-256 using blockchain concept,” in *2019 International conference on communication and signal processing (ICCSP)*, pp. 0370–0374, IEEE, 2019.
 - [35] C. E. Santos Jr, L. M. d. Silva, M. F. Torquato, S. N. Silva, and M. A. Fernandes, “Sha-256 hardware proposal for iot devices in the blockchain context,” *Sensors*, vol. 24, no. 12, p. 3908, 2024.

- [36] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*, pp. 369–378, Springer, 1987.
- [37] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO)*, pp. 1545–1550, Ieee, 2018.
- [38] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, no. 1, 2012.
- [39] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–35, 2023.
- [40] E. S. Negara, A. N. Hidayanto, R. Andryani, and R. Syaputra, "Survey of smart contract framework and its application," *Information*, vol. 12, no. 7, p. 257, 2021.
- [41] P. Jacquet and B. Mans, "Green mining: Toward a less energetic impact of cryptocurrencies," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 210–215, IEEE, 2019.
- [42] X. R. Zheng and Y. Lu, "Blockchain technology—recent research and future trend," *Enterprise Information Systems*, vol. 16, no. 12, p. 1939895, 2022.
- [43] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.
- [44] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–43, 2020.
- [45] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.
- [46] S. Casale-Brunet, P. Ribeca, P. Doyle, and M. Mattavelli, "Networks of ethereum non-fungible tokens: A graph-based analysis of the erc-721 ecosystem," in *2021 IEEE International Conference on Blockchain (Blockchain)*, pp. 188–195, IEEE, 2021.
- [47] G. Hong and H. Chang, "A study on corporate information assets management system using nft," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 608–610, IEEE, 2022.
- [48] W. Rehman, H. e Zainab, J. Imran, and N. Z. Bawany, "Nfts: Applications and challenges," in *2021 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1–7, IEEE, 2021.

- [49] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate internet-of-things data," *Future generation computer systems*, vol. 112, pp. 307–319, 2020.
- [50] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *12th international conference on evaluation and assessment in software engineering (EASE)*, BCS Learning & Development, 2008.
- [51] S. Keele *et al.*, "Guidelines for performing systematic literature reviews in software engineering," 2007.
- [52] M. Garaus and H. Treiblmaier, "The influence of blockchain-based food traceability on retailer choice: The mediating role of trust," *Food Control*, vol. 129, p. 108082, 2021.
- [53] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Computers in Industry*, vol. 109, pp. 83–99, 2019.
- [54] N. Niknejad, W. Ismail, M. Bahari, R. Hendradi, and A. Z. Salleh, "Mapping the research trends on blockchain technology in food and agriculture industry: A bibliometric analysis," *Environmental Technology & Innovation*, vol. 21, p. 101272, 2021.
- [55] S. A. Bhat, N.-F. Huang, I. B. Sofi, and M. Sultan, "Agriculture-food supply chain management based on blockchain and iot: A narrative on enterprise blockchain interoperability," *Agriculture*, vol. 12, no. 1, p. 40, 2021.
- [56] T. K. Dasaklis, T. G. Voutsinas, G. T. Tsoulfas, and F. Casino, "A systematic literature review of blockchain-enabled supply chain traceability implementations," *Sustainability*, vol. 14, no. 4, p. 2439, 2022.
- [57] A. sharma, T. Bhatia, and A. Sharma, "Digitalization of agri-food supply chain with blockchain technology: A review, taxonomy and open research issues," *SSRN Electronic Journal*, 01 2022.
- [58] G. Agnusdei and B. Coluccia, "Sustainable agrifood supply chains: Bibliometric, network and content analyses," *Science of The Total Environment*, p. 153704, 2022.
- [59] M. Alobid, S. Abujudeh, and I. Szűcs, "The role of blockchain in revolutionizing the agricultural sector," *Sustainability*, vol. 14, no. 7, p. 4313, 2022.
- [60] S. Tanwar, A. Parmar, A. Kumari, N. K. Jadav, W.-C. Hong, and R. Sharma, "Blockchain adoption to secure the food industry: Opportunities and challenges," *Sustainability*, vol. 14, no. 12, p. 7036, 2022.
- [61] U. Marfuah and I. Yuliasih, "Blockchain traceability for agroindustry-a literature review and future agenda," in *IOP Conference Series: Earth and Environmental Science*, vol. 1063, p. 012056, IOP Publishing, 2022.
- [62] J. Sultana, S. Y. Teoh, S. Karanasios, *et al.*, "The impact of blockchain on supply chains: A systematic review," *Australasian Journal of Information*

- Systems*, vol. 26, 2022.
- [63] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," *IEEE Access*, 2022.
 - [64] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.
 - [65] R. Ben Ayed, M. Hanana, S. Ercisli, R. Karunakaran, A. Rebai, and F. Moreau, "Integration of innovative technologies in the agri-food sector: The fundamentals and practical case of dna-based traceability of olives from fruit to oil," *Plants*, vol. 11, no. 9, p. 1230, 2022.
 - [66] Y. Kayikci, N. Subramanian, M. Dora, and M. S. Bhatia, "Food supply chain in the era of industry 4.0: Blockchain technology implementation opportunities and impediments from the perspective of people, process, performance, and technology," *Production Planning & Control*, pp. 1–21, 2020.
 - [67] M. P. Kramer, L. Bitsch, and J. H. Hanf, "The impact of instrumental stakeholder management on blockchain technology adoption behavior in agri-food supply chains," *Journal of Risk and Financial Management*, vol. 14, no. 12, p. 598, 2021.
 - [68] H. Treiblmaier, A. Rejeb, R. van Hoek, and M. Lacity, "Intra-and interorganizational barriers to blockchain adoption: A general assessment and coping strategies in the agrifood industry," *Logistics*, vol. 5, no. 4, p. 87, 2021.
 - [69] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food control*, vol. 39, pp. 172–184, 2014.
 - [70] T. Bosona and G. Gebresenbet, "Food traceability as an integral part of logistics management in food and agricultural supply chain," *Food control*, vol. 33, no. 1, pp. 32–48, 2013.
 - [71] B. M. Yakubu, R. Latif, A. Yakubu, M. I. Khan, and A. I. Magashi, "Ricechain: secure and traceable rice supply chain framework using blockchain technology," *PeerJ Computer Science*, vol. 8, p. e801, 2022.
 - [72] G. Varavallo, G. Caragnano, F. Bertone, L. Verneti-Prot, and O. Terzo, "Traceability platform based on green blockchain: An application case study in dairy supply chain," *Sustainability*, vol. 14, no. 6, p. 3321, 2022.
 - [73] A. Tan, D. Gligor, and A. Ngah, "Applying blockchain for halal food traceability," *International Journal of Logistics Research and Applications*, vol. 25, no. 6, pp. 947–964, 2022.
 - [74] K. Kampan, T. W. Tsusaka, and A. K. Anal, "Adoption of blockchain technology for enhanced traceability of livestock-based products," *Sustainability*, vol. 14, no. 20, p. 13148, 2022.
 - [75] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam,

- “Blockchain-based agri-food supply chain: A complete solution,” *IEEE Access*, vol. 8, pp. 69230–69243, 2020.
- [76] C. Contini, F. Boncinelli, G. Piracci, G. Scozzafava, and L. Casini, “Can blockchain technology strengthen consumer preferences for credence attributes?,” *Agricultural and Food Economics*, vol. 11, no. 1, p. 27, 2023.
- [77] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.
- [78] N. Dey, M. Ghosh, and A. Chakrabarti, “Quantum solutions to possible challenges of blockchain technology,” *arXiv preprint arXiv:2110.05321*, 2021.
- [79] Y. Gao, X. Chen, Y. Chen, Y. Sun, X. Niu, and Y. Yang, “A secure cryptocurrency scheme based on post-quantum blockchain,” *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
- [80] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, “Quantum-secured blockchain,” *CoRR*, vol. abs/1705.09258, 2017.
- [81] T. M. Fernández-Caramés and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” *IEEE Access*, vol. 8, pp. 21091–21116, 2020.
- [82] V. Fernandez, A. B. O. López, and D. Arroyo, “Securing blockchain with quantum safe cryptography: When and how?,” in *13th International Conference on Computational Intelligence in Security for Information Systems, CISIS 2020, Burgos, Spain, September 2020* (Á. Herrero, C. Cambra, D. Urda, J. Sedano, H. Quintián, and E. Corchado, eds.), vol. 1267 of *Advances in Intelligent Systems and Computing*, pp. 371–379, Springer, 2020.
- [83] M. Allende, D. L. León, S. Cerón, A. Leal, A. Pareja, M. da Silva, A. Pardo, D. Jones, D. Worrall, B. Merriman, J. Gilmore, N. Kitchenner, and S. E. Venegas-Andraca, “Quantum-resistance in blockchain networks,” *CoRR*, vol. abs/2106.06640, 2021.
- [84] M. Buser, R. Dowsley, M. F. Esgin, C. Gritti, S. K. Kermanshahi, V. Kuchta, J. T. LeGrow, J. K. Liu, R. C. Phan, A. Sakzad, R. Steinfeld, and J. Yu, “A survey on exotic signatures for post-quantum blockchain: Challenges & research directions,” *IACR Cryptol. ePrint Arch.*, p. 1151, 2022.
- [85] R. Longo, C. Mascia, A. Meneghetti, G. Santilli, and G. Tognolini, “Adaptable cryptographic primitives in blockchains via smart contracts,” *Cryptogr.*, vol. 6, no. 3, p. 32, 2022.
- [86] M. Mosca and M. Piani, “Quantum threat timeline report 2020,” *Website: <https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020>*, 2021.
- [87] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, *et al.*, “Status report on the second round of the nist post-quantum cryptography standardization process,” *US*

Department of Commerce, NIST, 2020.

- [88] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
- [89] K. T. Akhter Md Hasib, I. Chowdhury, S. Sakib, M. Monirujjaman Khan, N. Alsufyani, A. Alsufyani, and S. Bourouis, “Electronic health record monitoring system and data security using blockchain technology,” *Security and Communication Networks*, vol. 2022, 2022.
- [90] A. M. Shew, H. A. Snell, R. M. Nayga Jr, and M. C. Lacity, “Consumer valuation of blockchain traceability for beef in the u nited s tates,” *Applied Economic Perspectives and Policy*, vol. 44, no. 1, pp. 299–323, 2022.
- [91] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, “Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges,” *Journal of cleaner production*, vol. 260, p. 121031, 2020.
- [92] F. Tian, “An agri-food supply chain traceability system for china based on rfid & blockchain technology,” in *2016 13th international conference on service systems and service management (ICSSSM)*, pp. 1–6, IEEE, 2016.
- [93] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, “Blockchain-based traceability in agri-food supply chain management: A practical implementation,” in *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, pp. 1–4, IEEE, 2018.
- [94] I. A. Omar, M. Debe, R. Jayaraman, K. Salah, M. Omar, and J. Arshad, “Blockchain-based supply chain traceability for covid-19 personal protective equipment,” *Computers & Industrial Engineering*, vol. 167, p. 107995, 2022.
- [95] V. Kamath, Y. Lahari, K. Mohanchandra, *et al.*, “Blockchain based framework for secure data sharing of medicine supply chain in health care system,” *International Journal of Artificial Intelligence*, vol. 9, no. 1, pp. 32–28, 2022.
- [96] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, “Blockchain for healthcare data management: opportunities, challenges, and future recommendations,” *Neural Computing and Applications*, vol. 34, no. 14, pp. 11475–11490, 2022.
- [97] S. Balamurugan, A. Ayyasamy, and K. S. Joseph, “Iot-blockchain driven traceability techniques for improved safety measures in food supply chain,” *International Journal of Information Technology*, vol. 14, no. 2, pp. 1087–1098, 2022.
- [98] M. S. Ali, K. Dolui, and F. Antonelli, “Iot data privacy via blockchains and ipfs,” in *Proceedings of the seventh international conference on the internet of things*, pp. 1–7, 2017.
- [99] L. Cocco, R. Tonelli, and M. Marchesi, “Blockchain and self sovereign identity to support quality in the food supply chain,” *Future Internet*, vol. 13, no. 12, p. 301, 2021.

- [100] M. Uddin, "Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry," *International Journal of Pharmaceutics*, vol. 597, p. 120235, 2021.
- [101] K. Gao, Y. Liu, H. Xu, and T. Han, "Design and implementation of food supply chain traceability system based on hyperledger fabric," *International Journal of Computational Science and Engineering*, vol. 23, no. 2, pp. 185–193, 2020.
- [102] H. Huang, X. Zhou, and J. Liu, "Food supply chain traceability scheme based on blockchain and epc technology," in *International Conference on Smart Blockchain*, pp. 32–42, Springer, 2019.
- [103] Z. Ge, D. Loghin, B. C. Ooi, P. Ruan, and T. Wang, "Hybrid blockchain database systems: design and performance," *Proceedings of the VLDB Endowment*, vol. 15, no. 5, pp. 1092–1104, 2022.
- [104] M. Nasreen and S. K. Singh, "Implementation of blockchain based electronic health record system using java eclipse and mongodb," in *2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pp. 1–6, IEEE, 2022.
- [105] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, and I. Yaqoob, "appxchain: Application-level interoperability for blockchain networks," *IEEE Access*, vol. 9, pp. 87777–87791, 2021.
- [106] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A cross-chain solution to integrating multiple blockchains for iot data management," *Sensors*, vol. 19, no. 9, p. 2042, 2019.
- [107] Y. E. Oktian, S.-G. Lee, and H. J. Lee, "Hierarchical multi-blockchain architecture for scalable internet of things environment," *Electronics*, vol. 9, no. 6, p. 1050, 2020.
- [108] L. Ngwira, M. M. Merlec, Y. K. Lee, and H. P. In, "Towards context-aware smart contracts for blockchain iot systems," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 82–87, 2021.
- [109] C. Profentzas, M. Almgren, and O. Landsiedel, "Tinyevm: Off-chain smart contracts on low-power iot devices," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pp. 507–518, 2020.
- [110] S. Benedict, P. Rumaise, and J. Kaur, "Iot blockchain solution for air quality monitoring in smartcities," in *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, IEEE, 2019.
- [111] D. Sofia, N. Lotrecchiano, P. Trucillo, A. Giuliano, and L. Terrone, "Novel air pollution measurement system based on ethereum blockchain," *Journal of Sensor and Actuator Networks*, vol. 9, no. 4, p. 49, 2020.
- [112] C. T. de Tazoult, R. Chiky, and V. Foltescu, "A distributed pollution monitoring system: The application of blockchain to air quality monitoring,"

- in *Computational Collective Intelligence: 11th International Conference, ICCI 2019, Hendaye, France, September 4–6, 2019, Proceedings, Part II 11*, pp. 688–697, Springer, 2019.
- [113] A. K. Hassan, M. S. Saraya, A. M. Ali-Eldin, and M. M. Abdelsalam, “Low-cost iot air quality monitoring station using cloud platform and blockchain technology,” *Applied Sciences*, vol. 14, no. 13, p. 5774, 2024.
- [114] E. C. Thom, “The discomfort index,” *Weatherwise*, vol. 12, no. 2, pp. 57–61, 1959.
- [115] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jararweh, “Blockchain-based database in an iot environment: challenges, opportunities, and analysis,” *Cluster Computing*, vol. 23, pp. 2151–2165, 2020.
- [116] A. I. Sanka and R. C. Cheung, “Efficient high performance fpga based nosql caching system for blockchain scalability and throughput improvement,” in *2018 26th International Conference on Systems Engineering (ICSEng)*, pp. 1–8, IEEE, 2018.
- [117] A. I. Sanka, M. H. Chowdhury, and R. C. Cheung, “Efficient high-performance fpga-redis hybrid nosql caching system for blockchain scalability,” *Computer Communications*, vol. 169, pp. 81–91, 2021.
- [118] S. Nathan, C. Govindarajan, A. Saraf, M. Sethi, and P. Jayachandran, “Blockchain meets database: Design and implementation of a blockchain relational database,” *arXiv preprint arXiv:1903.01919*, 2019.
- [119] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, “Bigchaindb: a scalable blockchain database,” *white paper, BigChainDB*, 2016.
- [120] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, “Blockbench: A framework for analyzing private blockchains,” in *Proceedings of the 2017 ACM International Conference on Management of Data, SIGMOD ’17*, (New York, NY, USA), p. 1085–1100, Association for Computing Machinery, 2017.
- [121] A. Aldweesh, M. Alharby, E. Solaiman, and A. van Moorsel, “Performance benchmarking of smart contracts to assess miner incentives in ethereum,” in *14th European Dependable Computing Conference, EDCC 2018, Iași, Romania, September 10-14, 2018*, pp. 144–149, IEEE Computer Society, 2018.
- [122] S. Benahmed, I. Pidikseev, R. Hussain, J. Lee, S. M. A. Kazmi, A. Oracevic, and F. Hussain, “A comparative analysis of distributed ledger technologies for smart contract development,” in *30th IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2019, Istanbul, Turkey, September 8-11, 2019*, pp. 1–6, IEEE, 2019.
- [123] N. M. Alshahrani, M. M. Kiah, and B. B. Zaidan, “Smart contract evaluation by multi-criteria analysis: Selection challenges and open issues, a review,” in *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, pp. 1–8, 2023.

- [124] B. Alkhazi and A. Alipour, “Multi-objective test selection of smart contract and blockchain applications,” *PeerJ Comput. Sci.*, vol. 9, p. e1587, 2023.
- [125] K. Ikeda and M.-N. Hamid, “Applications of blockchain in the financial sector and a peer-to-peer global barter web,” in *Advances in Computers*, vol. 111, pp. 99–120, Elsevier, 2018.
- [126] L. Argento, F. Buccafurri, A. Furfaro, S. Graziano, A. Guzzo, G. Lax, F. Pasqua, and D. Saccà, “Id-service: A blockchain-based platform to support digital-identity-aware service accountability,” *Applied Sciences*, vol. 11, no. 1, p. 165, 2020.
- [127] N. Khalili, *Design and Implementation of a Blockchain-based Global Authentication System Using Biometrics and Subscriber Identification Module*. PhD thesis, Université d’Ottawa/University of Ottawa, 2022.
- [128] M. Mita, K. Ito, S. Ohsawa, and H. Tanaka, “What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems,” in *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, pp. 60–66, IEEE, 2019.
- [129] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.
- [130] A. Rejeb, K. Rejeb, S. J. Simske, and J. G. Keogh, “Blockchain technology in the smart city: A bibliometric review,” *Quality & Quantity*, vol. 56, no. 5, pp. 2875–2906, 2022.
- [131] F. Ullah and F. Al-Turjman, “A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities,” *Neural Computing and Applications*, pp. 1–22, 2021.
- [132] N. F. M. Shari and A. Malip, “State-of-the-art solutions of blockchain technology for data dissemination in smart cities: A comprehensive review,” *Computer Communications*, 2022.
- [133] A. Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, “Sustainable smart cities: convergence of artificial intelligence and blockchain,” *Sustainability*, vol. 13, no. 23, p. 13076, 2021.
- [134] R. Godahewa, C. Deng, A. Prouzeau, and C. Bergmeir, “A generative deep learning framework across time series to optimize the energy consumption of air conditioning systems,” *IEEE Access*, vol. 10, pp. 6842–6855, 2022.
- [135] R. Olu-Ajayi, H. Alaka, I. Sulaimon, F. Sunmola, and S. Ajayi, “Building energy consumption prediction for residential buildings using deep learning and other machine learning techniques,” *Journal of Building Engineering*, vol. 45, p. 103406, 2022.
- [136] M. Saleem, S. Abbas, T. M. Ghazal, M. A. Khan, N. Sahawneh, and M. Ahmad, “Smart cities: Fusion-based intelligent traffic congestion control system

- for vehicular networks using machine learning techniques,” *Egyptian Informatics Journal*, 2022.
- [137] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, “Blockchain for waste management in smart cities: A survey,” *IEEE Access*, vol. 9, pp. 131520–131541, 2021.
- [138] S. Kumar, R. S. Rathore, M. Mahmud, O. Kaiwartya, and J. Lloret, “Best—blockchain-enabled secure and trusted public emergency services for smart cities environment,” *Sensors*, vol. 22, no. 15, p. 5733, 2022.
- [139] T. M. Ghazal, M. K. Hasan, H. M. Alzoubi, M. Al Hmadi, N. A. Al-Dmour, S. Islam, R. Kamran, and B. Mago, “Securing smart cities using blockchain technology,” in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, pp. 1–4, IEEE, 2022.
- [140] D. Shi, C. Cao, and J. Ye, “Secure government data sharing based on blockchain and attribute-based encryption,” in *International Symposium on Security and Privacy in Social Networks and Big Data*, pp. 324–338, Springer, 2022.
- [141] C. Lin, G. Han, J. Du, T. Xu, L. Shu, and Z. Lv, “Spatiotemporal congestion-aware path planning toward intelligent transportation systems in software-defined smart city iot,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8012–8024, 2020.
- [142] Z. Qadir, F. Ullah, H. S. Munawar, and F. Al-Turjman, “Addressing disasters in smart cities through uavs path planning and 5g communications: A systematic review,” *Computer Communications*, vol. 168, pp. 114–135, 2021.
- [143] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, “Applications, deployments, and integration of internet of drones (iod): a review,” *IEEE Sensors Journal*, 2021.
- [144] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, “Utm-chain: blockchain-based secure unmanned traffic management for internet of drones,” *Sensors*, vol. 21, no. 9, p. 3049, 2021.
- [145] M. P. Singh, A. Singh, G. S. Aujla, R. S. Bali, and A. Jindal, “Referenced blockchain approach for road traffic monitoring in a smart city using internet of drones,” in *ICC 2022-IEEE International Conference on Communications*, pp. 1–6, IEEE, 2022.
- [146] S. Liao, J. Wu, J. Li, A. K. Bashir, and W. Yang, “Securing collaborative environment monitoring in smart cities using blockchain enabled software-defined internet of drones,” *IEEE Internet of Things Magazine*, vol. 4, no. 1, pp. 12–18, 2021.
- [147] S. Huh, S. Muralidharan, H. Ko, and B. Yoo, “Xr collaboration architecture based on decentralized web,” in *The 24th International Conference on 3D Web Technology*, pp. 1–9, 2019.
- [148] J. Mathew, K. Kanjirappally, and J. Joseph, “Virtual environment using

- metaverse,” in *Proceedings of the National Conference on Emerging Computer Applications (NCECA)*, vol. 4, p. 373, 2022.
- [149] A. Cannavo and F. Lamberti, “How blockchain, virtual reality, and augmented reality are converging, and why,” *IEEE Consumer Electronics Magazine*, vol. 10, no. 5, pp. 6–13, 2020.
- [150] P. Suanpang, C. Niamsorn, P. Pothipassa, T. Chunhapataragul, T. Netwong, and K. Jernsittiparsert, “Extensible metaverse implication for a smart tourism city,” *Sustainability*, vol. 14, no. 21, p. 14027, 2022.
- [151] D. Gursoy, S. Malodia, and A. Dhir, “The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions,” *Journal of Hospitality Marketing & Management*, vol. 31, no. 5, pp. 527–534, 2022.
- [152] C. Koo, J. Kwon, N. Chung, and J. Kim, “Metaverse tourism: conceptual framework and research propositions,” *Current Issues in Tourism*, pp. 1–7, 2022.
- [153] D. Buhalis and N. Karatay, “Mixed reality (mr) for generation z in cultural heritage tourism towards metaverse,” in *Information and Communication Technologies in Tourism 2022: Proceedings of the ENTER 2022 eTourism Conference, January 11–14, 2022*, pp. 16–27, Springer, 2022.
- [154] F. Xu, D. Buhalis, and J. Weber, “Serious games and the gamification of tourism,” *Tourism management*, vol. 60, pp. 244–256, 2017.
- [155] M. G. Pasca, M. F. Renzi, L. Di Pietro, and R. Guglielmetti Mugion, “Gamification in tourism and hospitality research in the era of digital platforms: a systematic literature review,” *Journal of Service Theory and Practice*, vol. 31, no. 5, pp. 691–737, 2021.
- [156] E. Pietroni, “Experience design, virtual reality and media hybridization for the digital communication inside museums,” *Applied System Innovation*, vol. 2, no. 4, p. 35, 2019.
- [157] A. Jo, “The promise and peril of generative ai,” *Nature*, vol. 614, no. 1, pp. 214–216, 2023.
- [158] H. Abburi, M. Suesserman, N. Pudota, B. Veeramani, E. Bowen, and S. Bhattacharya, “Generative ai text classification using ensemble llm approaches,” *arXiv preprint arXiv:2309.07755*, 2023.
- [159] N. M. Guerreiro, D. M. Alves, J. Waldendorf, B. Haddow, A. Birch, P. Colombo, and A. F. Martins, “Hallucinations in large multilingual translation models,” *Transactions of the Association for Computational Linguistics*, vol. 11, pp. 1500–1517, 2023.
- [160] P. Laban, W. Kryściński, D. Agarwal, A. R. Fabbri, C. Xiong, S. Joty, and C.-S. Wu, “Summedits: Measuring llm ability at factual reasoning through the lens of summarization,” in *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, pp. 9662–9676, 2023.
- [161] E. Adamopoulou and L. Moussiades, “An overview of chatbot technology,”

- in *IFIP international conference on artificial intelligence applications and innovations*, pp. 373–383, Springer, 2020.
- [162] J. Weizenbaum, “Eliza—a computer program for the study of natural language communication between man and machine,” *Communications of the ACM*, vol. 9, no. 1, pp. 36–45, 1966.
- [163] M. U. Hadi, R. Qureshi, A. Shah, M. Irfan, A. Zafar, M. B. Shaikh, N. Akhtar, J. Wu, S. Mirjalili, *et al.*, “A survey on large language models: Applications, challenges, limitations, and practical usage,” *Authorea Preprints*, 2023.
- [164] M. O. Topal, A. Bas, and I. van Heerden, “Exploring transformers in natural language generation: Gpt, bert, and xlnet,” *arXiv preprint arXiv:2102.08036*, 2021.
- [165] D. M. Katz, M. J. Bommarito, S. Gao, and P. Arredondo, “Gpt-4 passes the bar exam,” *Available at SSRN 4389233*, 2023.
- [166] Y. Anand, Z. Nussbaum, B. Duderstadt, B. Schmidt, and A. Mulyar, “Gpt4all: Training an assistant-style chatbot with large scale data distillation from gpt-3.5-turbo.” <https://github.com/nomic-ai/gpt4all>, 2023.
- [167] EDiGiacinto, “Localai repository.” <https://github.com/go-skynet/LocalAI>, 2023.
- [168] jmorganca, “Ollama repository.” <https://github.com/jmorganca/ollama>, 2023.
- [169] Y. Li, L. Sha, L. Yan, J. Lin, M. Raković, K. Galbraith, K. Lyons, D. Gašević, and G. Chen, “Can large language models write reflectively,” *Computers and Education: Artificial Intelligence*, vol. 4, p. 100140, 2023.
- [170] J. L. Espejel, E. H. Ettifouri, M. S. Y. Alassan, E. M. Chouham, and W. Dahhane, “Gpt-3.5, gpt-4, or bard? evaluating llms reasoning ability in zero-shot setting and performance boosting through prompts,” *Natural Language Processing Journal*, vol. 5, p. 100032, 2023.
- [171] Y. K. Dwivedi, N. Kshetri, L. Hughes, E. L. Slade, A. Jeyaraj, A. K. Kar, A. M. Baabdullah, A. Koohang, V. Raghavan, M. Ahuja, *et al.*, ““so what if chatgpt wrote it?” multidisciplinary perspectives on opportunities, challenges and implications of generative conversational ai for research, practice and policy,” *International Journal of Information Management*, vol. 71, p. 102642, 2023.
- [172] Y. Feng, S. Vanam, M. Cherukupally, W. Zheng, M. Qiu, and H. Chen, “Investigating code generation performance of chat-gpt with crowdsourcing social data,” in *Proceedings of the 47th IEEE Computer Software and Applications Conference*, pp. 1–10, 2023.
- [173] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, “How to properly use the prisma statement,” *Systematic Reviews*, vol. 10, no. 1, pp. 1–3, 2021.
- [174] M. B. Eriksen and T. F. Frandsen, “The impact of patient, intervention, comparison, outcome (pico) as a search strategy tool on literature search

- quality: a systematic review,” *Journal of the Medical Library Association: JMLA*, vol. 106, no. 4, p. 420, 2018.
- [175] J. Doughty, Z. Wan, A. Bompelli, J. Qayum, T. Wang, J. Zhang, Y. Zheng, A. Doyle, P. Sridhar, A. Agarwal, *et al.*, “A comparative study of ai-generated (gpt-4) and human-crafted mcqs in programming education,” *arXiv preprint arXiv:2312.03173*, 2023.
- [176] Y. Feng, S. Vanam, M. Cherukupally, W. Zheng, M. Qiu, and H. Chen, “Investigating Code Generation Performance of ChatGPT with Crowdsourcing Social Data,” in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, (Torino, Italy), pp. 876–885, IEEE, June 2023.
- [177] S. Wang, B. Lin, Z. Sun, M. Wen, Y. Liu, Y. Lei, and X. Mao, “Two Birds with One Stone: Boosting Code Generation and Code Search via a Generative Adversarial Network,” *Proceedings of the ACM on Programming Languages*, vol. 7, pp. 239:486–239:515, Oct. 2023.
- [178] M. Scanlon, F. Breitingner, C. Hargreaves, J.-N. Hilgert, and J. Sheppard, “ChatGPT for digital forensic investigation: The good, the bad, and the unknown,” *Forensic Science International: Digital Investigation*, vol. 46, p. 301609, Oct. 2023.
- [179] T. McIntosh, T. Liu, T. Susnjak, H. Alavizadeh, A. Ng, R. Nowrozy, and P. Watters, “Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation,” *Computers & Security*, vol. 134, p. 103424, Nov. 2023.
- [180] A. Sarkar, “Will Code Remain a Relevant User Interface for End-User Programming with Generative AI Models?,” in *Proceedings of the 2023 ACM SIGPLAN International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software*, Onward! 2023, (New York, NY, USA), pp. 153–167, Association for Computing Machinery, Oct. 2023.
- [181] I. Ozkaya, “The Next Frontier in Software Development: AI-Augmented Software Development Processes,” *IEEE Software*, vol. 40, pp. 4–9, July 2023.
- [182] I. Ozkaya, “Application of Large Language Models to Software Engineering Tasks: Opportunities, Risks, and Implications,” *IEEE Software*, vol. 40, pp. 4–8, May 2023.
- [183] C. Diwan, S. Srinivasa, G. Suri, S. Agarwal, and P. Ram, “AI-based learning content generation and learning pathway augmentation to increase learner engagement,” *Computers and Education: Artificial Intelligence*, vol. 4, p. 100110, Jan. 2023.
- [184] D. O. Eke, “ChatGPT and the rise of generative AI: Threat to academic integrity?,” *Journal of Responsible Technology*, vol. 13, p. 100060, Apr. 2023.
- [185] J. L. Steele, “To GPT or not GPT? Empowering our students to learn with AI,” *Computers and Education: Artificial Intelligence*, vol. 5, p. 100160, Jan. 2023.

- [186] Y. Li, L. Sha, L. Yan, J. Lin, M. Raković, K. Galbraith, K. Lyons, D. Gašević, and G. Chen, “Can large language models write reflectively,” *Computers and Education: Artificial Intelligence*, vol. 4, p. 100140, Jan. 2023.
- [187] Y. J. Park, D. Kaplan, Z. Ren, C.-W. Hsu, C. Li, H. Xu, S. Li, and J. Li, “Can ChatGPT be used to generate scientific hypotheses?,” *Journal of Materiomics*, Sept. 2023.
- [188] R. Yilmaz and F. G. Karaoglan Yilmaz, “The effect of generative artificial intelligence (AI)-based tool use on students’ computational thinking skills, programming self-efficacy and motivation,” *Computers and Education: Artificial Intelligence*, vol. 4, p. 100147, Jan. 2023.
- [189] J. Martins, F. Branco, and H. Mamede, “Combining Low-Code Development with ChatGPT to Novel No-Code Approaches: A Focus-group Study,” *Intelligent Systems with Applications*, p. 200289, Oct. 2023.
- [190] L. Y. Nie, C. Gao, Z. Zhong, W. Lam, Y. Liu, and Z. Xu, “CoreGen: Contextualized Code Representation Learning for Commit Message Generation,” *Neurocomputing*, vol. 459, pp. 97–107, Oct. 2021.
- [191] J. Cámara, J. Troya, L. Burgueño, and A. Vallecillo, “On the assessment of generative AI in modeling tasks: An experience report with ChatGPT and UML,” *Software and Systems Modeling*, vol. 22, pp. 781–793, June 2023.
- [192] A. S. Pothukuchi, L. V. Kota, and V. Mallikarjunaradhya, “Impact of Generative AI on the Software Development Lifecycle (SDLC),” Aug. 2023.
- [193] L. Caruccio, S. Cirillo, G. Polese, G. Solimando, S. Sundaramurthy, and G. Tortora, “Can ChatGPT provide intelligent diagnoses? A comparative study between predictive models and ChatGPT to define a new medical diagnostic bot,” *Expert Systems with Applications*, vol. 235, p. 121186, Jan. 2024.
- [194] M. Javaid, A. Haleem, and R. P. Singh, “ChatGPT for healthcare services: An emerging stage for an innovative perspective,” *Benchmark Transactions on Benchmarks, Standards and Evaluations*, vol. 3, p. 100105, Feb. 2023.
- [195] J. Menichetti, M. A. Hillen, A. Papageorgiou, and A. H. Pieterse, “How can ChatGPT be used to support healthcare communication research?,” *Patient Education and Counseling*, vol. 115, p. 107947, Oct. 2023.
- [196] A. Ni, S. Iyer, D. Radev, V. Stoyanov, W.-T. Yih, S. Wang, and X. V. Lin, “LEVER: Learning to Verify Language-to-Code Generation with Execution,” in *Proceedings of the 40th International Conference on Machine Learning*, pp. 26106–26128, PMLR, July 2023.
- [197] E. Nijkamp, B. Pang, H. Hayashi, L. Tu, H. Wang, Y. Zhou, S. Savarese, and C. Xiong, “CodeGen: An Open Large Language Model for Code with Multi-Turn Program Synthesis,” in *The Eleventh International Conference on Learning Representations*, Sept. 2022.
- [198] A. Svyatkovskiy, S. K. Deng, S. Fu, and N. Sundaresan, “IntelliCode compose: Code generation using transformer,” in *Proceedings of the 28th ACM Joint*

- Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2020, (New York, NY, USA), pp. 1433–1443, Association for Computing Machinery, Nov. 2020.
- [199] M. Lajkó, V. Csuvi, and L. Vidács, “Towards JavaScript program repair with generative pre-trained transformer (GPT-2),” in *Proceedings of the Third International Workshop on Automated Program Repair*, APR ’22, (New York, NY, USA), pp. 61–68, Association for Computing Machinery, Oct. 2022.
- [200] Z. Alizadehsani, H. Ghaemi, A. Shahraki, A. Gonzalez-Briones, and J. M. Corchado, “DCServCG: A data-centric service code generation using deep learning,” *Engineering Applications of Artificial Intelligence*, vol. 123, p. 106304, Aug. 2023.
- [201] S. Sarsa, P. Denny, A. Hellas, and J. Leinonen, “Automatic Generation of Programming Exercises and Code Explanations Using Large Language Models,” in *Proceedings of the 2022 ACM Conference on International Computing Education Research - Volume 1*, vol. 1 of *ICER ’22*, (New York, NY, USA), pp. 27–43, Association for Computing Machinery, Aug. 2022.
- [202] Z. Y. Kong, V. S. K. Adi, J. G. Segovia-Hernández, and J. Sunarso, “Complementary role of large language models in educating undergraduate design of distillation column: Methodology development,” *Digital Chemical Engineering*, vol. 9, p. 100126, Dec. 2023.
- [203] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and I. H. Khan, “Unlocking the opportunities through ChatGPT Tool towards ameliorating the education system,” *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 3, p. 100115, June 2023.
- [204] C. Bull and A. Kharrufa, “Generative AI Assistants in Software Development Education: A vision for integrating Generative AI into educational practice, not instinctively defending against it,” *IEEE Software*, pp. 1–9, 2023.
- [205] H. Ali, P. Patel, I. Obaitan, B. P. Mohan, A. H. Sohail, L. Smith-Martinez, K. Lambert, M. K. Gangwani, J. J. Easler, and D. G. Adler, “Evaluating ChatGPT’s Performance in Responding to Questions About Endoscopic Procedures for Patients,” *iGIE*, Oct. 2023.
- [206] S. Chatterjee, M. Bhattacharya, S.-S. Lee, and C. Chakraborty, “Can artificial intelligence-strengthened ChatGPT or other large language models transform nucleic acid research?,” *Molecular Therapy - Nucleic Acids*, vol. 33, pp. 205–207, Sept. 2023.
- [207] T.-H. Kim, J. W. Kang, and M. S. Lee, “AI Chat bot - ChatGPT-4: A new opportunity and challenges in complementary and alternative medicine,” *Integrative Medicine Research*, vol. 12, p. 100977, Sept. 2023.
- [208] S. W. Li, M. W. Kemp, S. J. S. Logan, P. S. Dimri, N. Singh, C. N. Z. Mattar, P. Dashraath, H. Ramlal, A. P. Mahyuddin, S. Kanayan, S. W. D. Carter, S. P. T. Thain, E. L. Fee, S. E. Illanes, M. A. Choolani, M. Rauff, A. Biswas, J. J. H. Low, J. S. Ng, A. T. Gosavi, Z. Huang, P. Rajendran, K. W. R.

- Ng, J. J. L. Wong, G. M. F. Chan, K. Z. X. Lee, J. J. Y. Yap, N. Ahmad, S. Shanmugam, R. Kathirvel, M. Mathur, W. W. Lim, and M. Y. Lim, "ChatGPT outscored human candidates in a virtual objective structured clinical examination in obstetrics and gynecology," *American Journal of Obstetrics and Gynecology*, vol. 229, pp. 172.e1–172.e12, Aug. 2023.
- [209] J. Kocoń, I. Cichecki, O. Kaszyca, M. Kochanek, D. Szydło, J. Baran, J. Bielaniewicz, M. Gruza, A. Janz, K. Kancierz, A. Kocoń, B. Kopytyra, W. Mieleszczenko-Kowszewicz, P. Miłkowski, M. Oleksy, M. Piasecki, Ł. Radliński, K. Wojtasik, S. Woźniak, and P. Kazienko, "ChatGPT: Jack of all trades, master of none," *Information Fusion*, vol. 99, p. 101861, Nov. 2023.
- [210] A. Haleem, M. Javaid, and R. P. Singh, "An era of ChatGPT as a significant futuristic support tool: A study on features, abilities, and challenges," *Benchmark Council Transactions on Benchmarks, Standards and Evaluations*, vol. 2, p. 100089, Oct. 2022.
- [211] F. M. Megahed, Y.-J. Chen, J. A. Ferris, S. Knoth, and L. A. Jones-Farmer, "How generative AI models such as ChatGPT can be (mis)used in SPC practice, education, and research? An exploratory study," *Quality Engineering*, pp. 1–29, June 2023.
- [212] M. Javaid, A. Haleem, and R. P. Singh, "A study on ChatGPT for Industry 4.0: Background, Potentials, Challenges, and Eventualities," *Journal of Economy and Technology*, Aug. 2023.
- [213] N. Köbis and L. D. Mossink, "Artificial intelligence versus Maya Angelou: Experimental evidence that people cannot differentiate AI-generated from human-written poetry," *Computers in Human Behavior*, vol. 114, p. 106553, Jan. 2021.
- [214] U. Bezirhan and M. von Davier, "Automated reading passage generation with OpenAI's large language model," *Computers and Education: Artificial Intelligence*, vol. 5, p. 100161, Jan. 2023.
- [215] B. Zhao, W. Jin, J. Del Ser, and G. Yang, "ChatAgri: Exploring potentials of ChatGPT on cross-linguistic agricultural text classification," *Neurocomputing*, vol. 557, p. 126708, Nov. 2023.
- [216] D. Sjödin, V. Parida, M. Palmié, and J. Wincent, "How AI capabilities enable business model innovation: Scaling AI through co-evolutionary processes and feedback loops," *Journal of Business Research*, vol. 134, pp. 574–587, Sept. 2021.
- [217] A. J. Vidanaralage, A. T. Dharmaratne, and S. Haque, "AI-based multidisciplinary framework to assess the impact of gamified video-based learning through schema and emotion analysis," *Computers and Education: Artificial Intelligence*, vol. 3, p. 100109, Jan. 2022.
- [218] T. Taulli, "Auto Code Generation," in *Generative AI: How ChatGPT and Other AI Tools Will Revolutionize Business* (T. Taulli, ed.), pp. 127–143,

- Berkeley, CA: Apress, 2023.
- [219] C. Ebert and P. Louridas, “Generative AI for Software Practitioners,” *IEEE Software*, vol. 40, pp. 30–38, July 2023.
- [220] J. Sun, Q. V. Liao, M. Muller, M. Agarwal, S. Houde, K. Talamadupula, and J. D. Weisz, “Investigating Explainability of Generative AI for Code through Scenario-based Design,” in *27th International Conference on Intelligent User Interfaces, IUI ’22*, (New York, NY, USA), pp. 212–228, Association for Computing Machinery, Mar. 2022.
- [221] K. Hong, Y. Uh, and H. Byun, “ArrowGAN : Learning to generate videos by learning Arrow of Time,” *Neurocomputing*, vol. 438, pp. 223–234, May 2021.
- [222] T. Y. Zhuo, “Large language models are state-of-the-art evaluators of code generation,” *arXiv preprint arXiv:2304.14317*, 2023.
- [223] R. Malhotra, M. Massoudi, and R. Jindal, “An Innovative Approach: Coupling Project-Based Learning and Game-Based Learning Approach in Teaching Software Engineering Course,” in *2020 IEEE International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET)*, pp. 1–5, 2020.
- [224] M. K. Kim and S. M. Kim, “Dynamic learner engagement in a wiki-enhanced writing course,” *Journal of Computing in Higher Education*, vol. 32, no. 3, pp. 582–606, 2020.
- [225] D. T. K. Ng, C. Xinyu, J. K. L. Leung, and S. K. W. Chu, “Fostering students’ ai literacy development through educational games: Ai knowledge, affective and cognitive engagement,” *Journal of Computer Assisted Learning*, 2024.
- [226] M. Magioli Sereno and H. B. Ang, “The impact of gamification on training, work engagement, and job satisfaction in banking,” *International Journal of Training and Development*, 2024.
- [227] M. Mongiello, F. Nocera, A. Parchitelli, L. Patrono, P. Rametta, L. Riccardi, and I. Sergi, “A smart iot-aware system for crisis scenario management,” *Journal of Communications software and Systems*, vol. 14, no. 1, pp. 91–98, 2018.
- [228] G. Cavallera, R. C. Rosito, V. Lacasa, M. Mongiello, F. Nocera, L. Patrono, and I. Sergi, “An innovative smart system based on iot technologies for fire and danger situations,” in *2019 4th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, IEEE, 2019.
- [229] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: The prisma statement,” *International Journal of Surgery*, vol. 8, no. 5, pp. 336–341, 2010.
- [230] R. H. B. Monteiro, S. R. B. Oliveira, and M. R. De Almeida Souza, “A standard framework for gamification evaluation in education and training of software engineering: An evaluation from a proof of concept,” in *2021 IEEE Frontiers in Education Conference (FIE)*, pp. 1–7, 2021.
- [231] M. Tsunoda and H. Yumoto, “Applying Gamification and Posing to Software

- Development,” in *2018 25th Asia-Pacific Software Engineering Conference (APSEC)*, pp. 638–642, 2018.
- [232] Y. Takbiri, A. Amini, and A. Bastanfard, “A Structured Gamification Approach for Improving Children’s Performance in Online Learning Platforms,” in *2019 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS)*, pp. 1–6, 2019.
- [233] P. Molins-Ruano, F. Jurado, P. Rodríguez, S. Atrio, and G. M. Sacha, “An approach to gamify an adaptive questionnaire environment,” in *2016 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1129–1133, 2016.
- [234] A. Ortega-Arranz, M. Kalz, and A. Martínez-Monés, “Creating engaging experiences in MOOCs through in-course redeemable rewards,” in *2018 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1875–1882, 2018.
- [235] G. C. Nistor and A. Iacob, “The advantages of gamification and game-based learning and their benefits in the development of education,” in *The international scientific conference eLearning and software for education*, vol. 1, pp. 308–312, " Carol I" National Defence University, 2018.
- [236] N. Limantara, F. L. Gaol, H. Prabowo, *et al.*, “Mechanics, dynamics, and aesthetics framework on gamification at university,” in *2020 international conference on informatics, multimedia, cyber and information system (ICIMCIS)*, pp. 34–39, IEEE, 2020.
- [237] D. Strmecki, A. Bernik, and D. Radosevic, “Gamification in e-learning: Introducing gamified design elements into e-learning systems,” *J. Comput. Sci.*, vol. 11, no. 12, pp. 1108–1117, 2015.
- [238] G. Zichermann and C. Cunningham, *Gamification by design: Implementing game mechanics in web and mobile apps*. " O'Reilly Media, Inc.", 2011.
- [239] R. S. Alsawaier, “The effect of gamification on motivation and engagement,” *The International Journal of Information and Learning Technology*, vol. 35, no. 1, pp. 56–79, 2018.
- [240] A. M. Apandi, “Gamification meets mobile learning: soft-skills enhancement,” in *Research Anthology on Developments in Gamification and Game-Based Learning*, pp. 1280–1299, IGI Global, 2022.
- [241] M. K. Kabilan, N. Annamalai, and K.-M. Chuah, “Practices, purposes and challenges in integrating gamification using technology: A mixed-methods study on university academics,” *Education and Information Technologies*, vol. 28, no. 11, pp. 14249–14281, 2023.
- [242] T. Dal Sasso, A. Mocci, M. Lanza, and E. Mastrodicasa, “How to gamify software engineering,” in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 261–271, 2017.
- [243] O. Pedreira, F. García, N. Brisaboa, and M. Piattini, “Gamification in software engineering—a systematic mapping,” *Information and software technology*, vol. 57, pp. 157–168, 2015.

- [244] C. F. Barreto and C. França, “Gamification in software engineering: A literature review,” in *2021 IEEE/ACM 13th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE)*, pp. 105–108, IEEE, 2021.
- [245] M. R. Ngandu, D. Risinamhodzi, G. P. Dzvapatsva, and C. Matobobo, “Capturing student interest in software engineering through gamification: a systematic literature review,” *Discover Education*, vol. 2, no. 1, p. 47, 2023.
- [246] O. Chamorro-Atalaya, G. Morales-Romero, N. Trinidad-Loli, B. Caycho-Salas, T. Guía-Altamirano, E. Auqui-Ramos, Y. Rocca-Carvajal, M. Arones, J. A. Arévalo-Tuesta, and R. Gonzales-Huaytahuilca, “Gamification in engineering education during covid-19: a systematic review on design considerations and success factors in its implementation,” *International Journal of Learning, Teaching and Educational Research*, vol. 22, no. 6, pp. 301–327, 2023.
- [247] R. H. Barbosa Monteiro, M. R. de Almeida Souza, S. R. Bezerra Oliveira, C. dos Santos Portela, and C. E. de Cristo Lobato, “The diversity of gamification evaluation in the software engineering education and industry: Trends, comparisons and gaps,” in *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, pp. 154–164, 2021.
- [248] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, “Prisma2020: An r package and shiny app for producing prisma 2020-compliant flow diagrams, with interactivity for optimised digital transparency and open synthesis,” *Campbell systematic reviews*, vol. 18, no. 2, p. e1230, 2022.
- [249] T. Fulcini and M. Torchiano, “Is ChatGPT Capable of Crafting Gamification Strategies for Software Engineering Tasks?,” in *Proceedings of the 2nd International Workshop on Gamification in Software Development, Verification, and Validation*, Gamify 2023, (New York, NY, USA), pp. 22–28, Association for Computing Machinery, 2023.
- [250] W. Ren and S. Barrett, “An empirical investigation on the benefits of gamification in communication within university development teams,” *Computer Applications in Engineering Education*, vol. 31, no. 6, pp. 1808–1822, 2023.
- [251] M. A. Miljanovic and J. S. Bradbury, “Robobug: a serious game for learning debugging techniques,” in *Proceedings of the 2017 acm conference on international computing education research*, pp. 93–100, 2017.
- [252] E. O. Navarro and A. van der Hoek, “Simse: An interactive simulation game for software engineering education,” in *CATE*, vol. 1, pp. 12–17, 2004.
- [253] S. Esper, S. R. Foster, and W. G. Griswold, “Codespells: embodying the metaphor of wizardry for programming,” in *Proceedings of the 18th ACM conference on Innovation and technology in computer science education*, pp. 249–254, 2013.

- [254] R. F. Arif, H. A. Rosyid, and U. Pujianto, "Design and Implementation of Interactive Coding with Gamification for Web Programming Subject for Vocational High School Students," in *2019 International Conference on Electrical, Electronics and Information Engineering (ICEEIE)*, vol. 6, pp. 177–182, 2019.
- [255] R. H. A. Rahim, S. H. Tanalol, R. Ismail, A. Baharum, E. A. Rahim, and N. A. M. Noor, "Development of Gamification Linear Algebra Application Using Storytelling," in *2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 133–137, 2019.
- [256] M. Hajarian and P. Diaz, "Effective Gamification: A Guideline for Gamification Workshop of WEEF-GEDC 2021 Madrid Conference," in *2021 World Engineering Education Forum/Global Engineering Deans Council (WEEF/GEDC)*, pp. 506–510, 2021.
- [257] D. Iquiria, M. Galarza, and O. Sharhorodska, "Enhancing software engineering courses with a mobile gamified platform: Results of a mixed approach," in *2021 XVI Latin American Conference on Learning Technologies (LACLO)*, pp. 534–537, 2021.
- [258] V. Robledo-Rella, Ma. de Lourdes Quezada Batalla, J. M. Ramírez-de-Arellano, and R. D. S. Acosta, "Gam-mate: Gamification Applied to an Undergrad Discrete Math Course," in *2022 10th International Conference on Information and Education Technology (ICIET)*, pp. 135–139, 2022.
- [259] P. Gomes Fernandes Matsubara and C. Lima Corrêa Da Silva, "Game Elements in a Software Engineering Study Group: A Case Study," in *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET)*, pp. 160–169, 2017.
- [260] P. Rodrigues, M. Souza, and E. Figueiredo, "Games and Gamification in Software Engineering Education: A Survey with Educators," in *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1–9, 2018.
- [261] C. P. Quinde, R. I. Paredes, S. A. Maldonado, J. S. Guerrero, and M. F. V. Toro, "Gamification as a didactic strategy in a digital literacy: Case study for incarcerated individuals," in *2018 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1314–1319, 2018.
- [262] I. John and T. Fertig, "Gamification for Software Engineering Students - an Experience Report," in *2022 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1942–1947, 2022.
- [263] G. Ivanova, V. Kozov, and P. Zlatarov, "Gamification in Software Engineering Education," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1445–1450, 2019.
- [264] G. P. Gasca-Hurtado, M. C. Gómez-Álvarez, J. A. Hincapié, and V. V.

- Zepeda, "Gamification of an Educational Environment in Software Engineering: Case Study for Digital Accessibility of People With Disabilities," *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, vol. 16, no. 4, pp. 382–392, 2021.
- [265] M. Carreño-León, A. Sandoval-Bringas, F. Álvarez-Rodríguez, and Y. Camacho-González, "Gamification technique for teaching programming," in *2018 IEEE Global Engineering Education Conference (EDUCON)*, pp. 2009–2014, 2018.
- [266] E. Sherif, A. Liu, B. Nguyen, S. Lerner, and W. G. Griswold, "Gamification to Aid the Learning of Test Coverage Concepts," in *2020 IEEE 32nd Conference on Software Engineering Education and Training (CSEE&T)*, pp. 1–5, 2020.
- [267] D. Norsanto and Y. Rosmansyah, "Gamified mobile micro-learning framework: A case study of civil service management learning," in *2018 International Conference on Information and Communications Technology (ICOIACT)*, pp. 146–151, 2018.
- [268] M. W. Call, E. Fox, and G. Sprint, "Gamifying Software Engineering Tools to Motivate Computer Science Students to Start and Finish Programming Assignments Earlier," *IEEE Transactions on Education*, vol. 64, no. 4, pp. 423–431, 2021.
- [269] M. Trinidad, A. Calderón, and M. Ruiz, "GoRace: A Multi-Context and Narrative-Based Gamification Suite to Overcome Gamification Technological Challenges," *IEEE Access*, vol. 9, pp. 65882–65905, 2021.
- [270] W. Prasetya, C. Leek, O. Melkonian, J. ten Tusscher, J. van Bergen, J. Everink, T. van der Klis, R. Meijerink, R. Oosenbrug, J. Oostveen, T. van den Pol, and W. van Zon, "Having Fun in Learning Formal Specifications," in *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, pp. 192–196, 2019.
- [271] A. Bucchiarone, A. Cicchetti, S. Bassanelli, and A. Marconi, "How to merge gamification efforts for programming and modelling: A tool implementation perspective," in *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, pp. 721–726, 2021.
- [272] L. Lema Moreta, A. C. Gamboa, and M. G. Palacios, "Implementing a Gamified application for a Risk Management course," in *2016 IEEE Ecuador Technical Chapters Meeting (ETCM)*, pp. 1–6, 2016.
- [273] S. Ouhbi and N. Pombo, "Software Engineering Education: Challenges and Perspectives," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, pp. 202–209, 2020.
- [274] S. Villagra, G. De Benedetti, T. Bruno, L. Fernández, and N. Outeda, "Teaching software engineering: An active learning experience," in *2020 IEEE Congreso Bienal de Argentina (ARGENCON)*, pp. 1–6, 2020.

- [275] G. Moser, R. Vallon, M. Bernhart, and T. Grechenig, “Teaching Software Quality Assurance with Gamification and Continuous Feedback Techniques,” in *2021 IEEE Global Engineering Education Conference (EDUCON)*, pp. 505–509, 2021.
- [276] P. Rattadilok, C. Roadknight, and L. Li, “Teaching Students About Machine Learning Through a Gamified Approach,” in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 1011–1015, 2018.
- [277] A. Bucchiarone, A. Cicchetti, E. Loria, and A. Marconi, “Towards a Framework to Assist Iterative and Adaptive Design in Gameful Systems,” in *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, pp. 78–84, 2021.
- [278] C. Ebert, A. Vizcaino, and R. Grande, “Unlock the Business Value of Gamification,” *IEEE Software*, vol. 39, no. 6, pp. 15–22, 2022.
- [279] B. R. Maxim, S. Brunvand, and A. Decker, “Use of role-play and gamification in a software project course,” in *2017 IEEE Frontiers in Education Conference (FIE)*, pp. 1–5, 2017.
- [280] E. M. Jiménez-Hernández, J. A. Jiménez-Murillo, M. A. Segura-Castruita, and I. González-Leal, “Using a Serious Video Game to Support the Learning of Tree Traversals,” in *2021 9th International Conference in Software Engineering Research and Innovation (CONISOFT)*, pp. 238–244, 2021.
- [281] B. Nagaria, B. C. Evans, A. Mann, and M. Arzoky, “Using an Instant Visual and Text Based Feedback Tool to Teach Path Finding Algorithms: A Concept,” in *2021 Third International Workshop on Software Engineering Education for the Next Generation (SEENG)*, pp. 11–15, 2021.
- [282] O. Margalit, “Using Computer Programming Competition for Cyber Education,” in *2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE)*, pp. 104–107, 2016.
- [283] K.-J. Stol, M. Schaarschmidt, and S. Goldblit, “Gamification in software engineering: The mediating role of developer engagement and job satisfaction,” *Empirical Software Engineering*, vol. 27, no. 2, p. 35, 2022.
- [284] G. Đambić, T. Kešćec, and D. Kučak, “A Blended Learning with Gamification Approach for Teaching Programming Courses in Higher Education,” in *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 843–847, 2021.
- [285] Q. Mi, J. Keung, X. Mei, Y. Xiao, and W. K. Chan, “A Gamification Technique for Motivating Students to Learn Code Readability in Software Engineering,” in *2018 International Symposium on Educational Technology (ISET)*, pp. 250–254, 2018.
- [286] R. Malhotra, M. Massoudi, and R. Jindal, “An Innovative Approach: Coupling Project-Based Learning and Game-Based Learning Approach in Teaching Software Engineering Course,” in *2020 IEEE International Conference on*

- Technology, Engineering, Management for Societal Impact Using Marketing, Entrepreneurship and Talent (TEMSMET)*, pp. 1–5, 2020.
- [287] J. Skalka, M. Drлік, J. Obonya, and M. Cápay, “Architecture Proposal for Micro-Learning Application for Learning and Teaching Programming Courses,” in *2020 IEEE Global Engineering Education Conference (EDUCON)*, pp. 980–987, 2020.
- [288] N. Silvis-Cividjian, “Awesome Bug Manifesto: Teaching an Engaging and Inspiring Course on Software Testing (Position Paper),” in *2021 Third International Workshop on Software Engineering Education for the Next Generation (SEENG)*, pp. 16–20, 2021.
- [289] I. Makarova, A. Pashkevich, and K. Shubenkova, “Blended Learning Technologies in the Automotive Industry Specialists’ Training,” in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 319–324, 2018.
- [290] D. de Paula Porto, G. M. de Jesus, F. C. Ferrari, and S. C. P. F. Fabbri, “Initiatives and challenges of using gamification in software engineering: A Systematic Mapping,” *Journal of Systems and Software*, vol. 173, p. 110870, 2021.
- [291] E. Vlahu-Gjorgievska, M. Videnovik, and V. Trajkovik, “Computational Thinking and Coding Subject in Primary Schools: Methodological Approach Based on Alternative Cooperative and Individual Learning Cycles,” in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 77–83, Dec. 2018.
- [292] Y. C. Chan, C. Min Gan, C. Y. Lim, T. Hwa Tan, Q. Cao, and C. K. Seow, “Learning CS Subjects of Professional Software Development and Team Projects,” in *2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, pp. 71–77, Dec. 2022.
- [293] J. Figueiredo and F. J. García-Peñalvo, “Increasing student motivation in computer programming with gamification,” in *2020 IEEE Global Engineering Education Conference (EDUCON)*, pp. 997–1000, Apr. 2020.
- [294] F. A. Pratama, R. M. Silitonga, and Y.-T. Jou, “Rimigs: The impact of gamification on students’ motivation and performance in programming class,” *Indones. J. Electr. Eng. Comput. Sci*, vol. 24, no. 3, pp. 1789–1795, 2021.
- [295] N. Naik and P. Jenkins, “Relax, it’s a game: Utilising gamification in learning agile scrum software development,” in *2019 IEEE Conference on Games (CoG)*, pp. 1–4, IEEE, 2019.
- [296] J. Swacha and J. Szydłowska, “Does Gamification Make a Difference in Programming Education? Evaluating FGPE-Supported Learning Outcomes,” *Education Sciences*, vol. 13, p. 984, Oct. 2023.
- [297] M. E. Sousa-Vieira, J. C. López-Ardao, M. Fernández-Veiga, and R. F. Rodríguez-Rubio, “Study of the impact of social learning and gamification

- methodologies on learning results in higher education,” *Computer Applications in Engineering Education*, vol. 31, no. 1, pp. 131–153, 2023.
- [298] R. Monteiro, M. Souza, S. Oliveira, and E. Soares, “The Adoption of a Framework to Support the Evaluation of Gamification Strategies in Software Engineering Education:,” in *Proceedings of the 14th International Conference on Computer Supported Education*, (Online Streaming, — Select a Country —), pp. 450–457, SCITEPRESS - Science and Technology Publications, 2022.
- [299] V. Jusas, D. Barisas, and M. Jančiukas, “Game Elements towards More Sustainable Learning in Object-Oriented Programming Course,” *Sustainability*, vol. 14, p. 2325, Jan. 2022.
- [300] A. Bernik, D. Radošević, and G. Bubaš, “Introducing gamification into e-learning university courses,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 711–716, May 2017.
- [301] Y. Maher, S. M. Moussa, and M. E. Khalifa, “Learners on Focus: Visualizing Analytics Through an Integrated Model for Learning Analytics in Adaptive Gamified E-Learning,” *IEEE Access*, vol. 8, pp. 197597–197616, 2020.
- [302] F. A. Bachtiar, F. Pradana, B. Priyambadha, and D. I. Bastari, “CoMa: Development of Gamification-based E-learning,” in *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 1–6, 2018.
- [303] M. Laskowski, “Implementing gamification techniques into university study path - A case study,” in *2015 IEEE Global Engineering Education Conference (EDUCON)*, pp. 582–586, 2015.
- [304] M. Fuchs and C. Wolff, “Improving programming education through gameful, formative feedback,” in *2016 IEEE Global Engineering Education Conference (EDUCON)*, pp. 860–867, 2016.
- [305] A. Bucchiarone, K. M. L. Cooper, D. Lin, E. F. Melcer, and K. Sung, “Games and Software Engineering: Engineering fun, inspiration, and motivation,” *ACM SIGSOFT Software Engineering Notes*, vol. 48, no. 1, pp. 85–89, 2023.
- [306] A. Bucchiarone, T. Martorella, D. Colombo, A. Cicchetti, and A. Marconi, “POLYGLOT for Gamified Education: Mixing Modelling and Programming Exercises,” in *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, pp. 605–609, 2021.
- [307] F. Poecze and A. M. Tjoa, “Meta-Analytical Considerations for Gamification in Higher Education: Existing Approaches and Future Research Agenda,” in *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*, pp. 1–6, 2020.
- [308] I. Cabezas, “On combining gamification theory and ABET criteria for teaching and learning engineering,” in *2015 IEEE Frontiers in Education Conference (FIE)*, pp. 1–9, 2015.

- [309] A. Bucchiarone, K. M. L. Cooper, D. Lin, A. Smith, and V. Wanick, “Fostering Collaboration and Advancing Research in Software Engineering and Game Development for Serious Contexts,” *ACM SIGSOFT Software Engineering Notes*, vol. 48, no. 4, pp. 46–50, 2023.
- [310] S. Ristov, N. Ackovska, and V. Kirandziska, “Positive experience of the project gamification in the microprocessors and Microcontrollers course,” in *2015 IEEE Global Engineering Education Conference (EDUCON)*, pp. 511–517, 2015.
- [311] A. Bernik, D. Radošević, and G. Bubaš, “Introducing gamification into e-learning university courses,” in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 711–716, 2017.
- [312] U. Schäfer, “Training scrum with gamification: Lessons learned after two teaching periods,” in *2017 IEEE Global Engineering Education Conference (EDUCON)*, pp. 754–761, 2017.
- [313] E. Petrov, J. Mustafina, and M. Alloghani, “Overview on Modern Serious Games for Regional and Minority Languages Promotion,” in *2017 10th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 120–123, 2017.
- [314] K. Tsalikidis and G. Pavlidis, “jLegends: Online game to train programming skills,” in *2016 7th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pp. 1–6, 2016.
- [315] M. Gamarra, A. Dominguez, J. Velazquez, and H. Páez, “A gamification strategy in engineering education—A case study on motivation and engagement,” *Computer Applications in Engineering Education*, vol. 30, no. 2, pp. 472–482, 2022.
- [316] R. Kadar, N. A. Wahab, J. Othman, M. Shamsuddin, and S. B. Mahlan, “A study of difficulties in teaching and learning programming: a systematic literature review,” *International Journal of Academic Research in Progressive Education and Development*, vol. 10, no. 3, pp. 591–605, 2021.
- [317] M. Fiore and M. Mongiello, “Using peer assessment leveraging large language models in software engineering education,” *International Journal of Software Engineering and Knowledge Engineering*, vol. 34, 2024.
- [318] L. A. Kartashova, A. M. Gurzhii, V. O. Zaichuk, T. M. Sorochan, and F. M. Zhuravlev, “Digital twin of an educational institution: an innovative concept of blended learning,” in *Proceedings of the symposium on advances in educational technology, aet*, 2020.
- [319] S. Razzaq, B. Shah, F. Iqbal, M. Ilyas, F. Maqbool, and A. Rocha, “Deep-classrooms: a deep learning based digital twin framework for on-campus classrooms,” *Neural Computing and Applications*, pp. 1–10, 2022.
- [320] R. Huang, A. Tlili, L. Xu, C. Ying, L. Zheng, A. H. S. Metwally, D. Ting,

- T. Chang, H. Wang, J. Mason, *et al.*, “Educational futures of intelligent synergies between humans, digital twins, avatars, and robots-the istar framework,” *Journal of Applied Learning & Teaching*, pp. 1–16, 2023.
- [321] OpenAI, “Gpt-4 technical report,” 2023.
- [322] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” 2019.
- [323] E. C. Garrido-Merchan, R. Gozalo-Brizuela, and S. Gonzalez-Carvajal, “Comparing bert against traditional machine learning models in text classification,” *Journal of Computational and Cognitive Engineering*, vol. 2, no. 4, pp. 352–356, 2023.
- [324] H. Touvron, L. Martin, K. Stone, P. Albert, A. Almahairi, Y. Babaei, N. Bashlykov, S. Batra, P. Bhargava, S. Bhosale, *et al.*, “Llama 2: Open foundation and fine-tuned chat models,” *arXiv preprint arXiv:2307.09288*, 2023.
- [325] E. C. Ciliberti, M. Fiore, and M. Mongiello, “Development of a metaverse platform for tourism promotion in apulia,” in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pp. 680–681, 2023.
- [326] M. Pradana and H. P. Elisa, “Metaverse in education: A systematic literature review,” *Cogent Social Sciences*, vol. 9, no. 2, p. 2252656, 2023.
- [327] A. Ni, S. Iyer, D. Radev, V. Stoyanov, W.-t. Yih, S. Wang, and X. V. Lin, “Lever: Learning to verify language-to-code generation with execution,” in *International Conference on Machine Learning*, pp. 26106–26128, PMLR, 2023.
- [328] B. Zhao, W. Jin, J. Del Ser, and G. Yang, “Chatagri: Exploring potentials of chatgpt on cross-linguistic agricultural text classification,” *arXiv preprint arXiv:2305.15024*, 2023.
- [329] M. Javaid, A. Haleem, and R. P. Singh, “Chatgpt for healthcare services: An emerging stage for an innovative perspective,” *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 3, no. 1, p. 100105, 2023.
- [330] M. Fiore, M. Gattullo, and M. Mongiello, “First steps in constructing an ai-powered digital twin teacher: Harnessing large language models in a metaverse classroom,” in *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, pp. 939–940, 2024.
- [331] M. Marques, S. F. Ochoa, M. C. Bastarrica, and F. J. Gutierrez, “Enhancing the student learning experience in software engineering project courses,” *IEEE Transactions on Education*, vol. 61, no. 1, pp. 63–73, 2017.
- [332] C. B. Seaman, “Qualitative methods in empirical studies of software engineering,” *IEEE Transactions on software engineering*, vol. 25, no. 4, pp. 557–572, 1999.
- [333] F. Rizal, H. Hidayat, P. Jaya, W. Waskito, H. Masdi, and U. Verawardina,

- “Lack e-learning effectiveness: An analysis evaluating e-learning in engineering education,” *International Journal of Instruction*, vol. 15, no. 4, pp. 197–220, 2022.
- [334] M. Aniche, F. Mulder, and F. Hermans, “Grading 600+ students: a case study on peer and self grading,” in *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, pp. 211–220, IEEE, 2021.
- [335] H. Luo, A. Robinson, and J.-Y. Park, “Peer grading in a mooc: Reliability, validity, and perceived effects,” *Online Learning Journal*, vol. 18, no. 2, pp. 1–14, 2014.
- [336] S. Brown, P. Race, and C. Rust, *Using and experiencing assessment*. Kogan Page London, 1995.
- [337] K. Kumar, B. Sharma, G. J. Khan, S. Nusair, and K. Raghuwaiya, “An exploration on effectiveness of anonymous peer assessment strategy in online formative assessments,” in *2020 IEEE Frontiers in Education Conference (FIE)*, pp. 1–5, IEEE, 2020.
- [338] I. Ozkaya, “Application of large language models to software engineering tasks: Opportunities, risks, and implications,” *IEEE Software*, vol. 40, no. 3, pp. 4–8, 2023.
- [339] E. Frankford, C. Sauerwein, P. Bassner, S. Krusche, and R. Breu, “Ai-tutoring in software engineering education,” in *Proceedings of the 46th International Conference on Software Engineering: Software Engineering Education and Training*, pp. 309–319, 2024.
- [340] S. Rasnayaka, G. Wang, R. Shariffdeen, and G. N. Iyer, “An empirical study on usage and perceptions of llms in a software engineering project,” *arXiv preprint arXiv:2401.16186*, 2024.
- [341] V. D. Kirova, C. S. Ku, J. R. Laracy, and T. J. Marlowe, “Software engineering education must adapt and evolve for an llm environment,” in *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, pp. 666–672, 2024.
- [342] N. Meißner, S. Speth, J. Kieslinger, and S. Becker, “Evalquiz–llm-based automated generation of self-assessment quizzes in software engineering education,” in *Software Engineering im Unterricht der Hochschulen 2024*, pp. 53–64, Gesellschaft für Informatik eV, 2024.
- [343] V. Kozov, G. Ivanova, and D. Atanasova, “Practical application of ai and large language models in software engineering education,” *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 1, p. 690, 2024.
- [344] C. Arora, U. Venaik, P. Singh, S. Goyal, J. Tyagi, S. Goel, U. Singhal, and D. Kumar, “Analyzing llm usage in an advanced computing class in india,” *arXiv preprint arXiv:2404.04603*, 2024.
- [345] J. Cámara, J. Troya, L. Burgueño, and A. Vallecillo, “On the assessment of generative ai in modeling tasks: an experience report with chatgpt and uml,”

- Software and Systems Modeling*, vol. 22, no. 3, pp. 781–793, 2023.
- [346] R. Yilmaz and F. G. K. Yilmaz, “The effect of generative artificial intelligence (ai)-based tool use on students’ computational thinking skills, programming self-efficacy and motivation,” *Computers and Education: Artificial Intelligence*, vol. 4, p. 100147, 2023.
- [347] P. P. Ray, “Chatgpt: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope,” *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 21–54, 2023.