IJWR

Blockchain Technology and GDPR Compliance: A Comprehensive Applicability Model

Abouzar Arabsorkhi[a*], Elham Khazaei[b]

[a] Assistant Professor, Department of ICT security, Iran Telecommunications Research Institute, Tehran, Iran; abouzar_arab@itrc.ac.ir

[b] Department of IT Management, University of Tehran, Tehran, Iran; Elham.khazaei@ut.ac.ir

ABSTRACT

This study investigates the potential of blockchain technology to support compliance with the General Data Protection Regulation (GDPR). By integrating blockchain's core features, such as transparency, immutability, and data encryption, with GDPR principles like data minimization and accuracy, the research develops a comprehensive applicability model. This model serves as a Reference Framework for evaluating blockchain systems' alignment with GDPR requirements. The study employs a meta-synthesis method and qualitative content analysis of 67 articles, culminating in a detailed examination of 31 selected articles. The findings reveal that blockchain technology can significantly enhance GDPR compliance, particularly in securing personal data and ensuring transparency. Importantly, the research introduces a novel model validated by a panel of 13 experts, which identifies and prioritizes key areas where blockchain can effectively support GDPR requirements. This model provides valuable insights for policymakers, industry leaders, and technology developers, emphasizing blockchain's strategic role in enhancing data protection under GDPR.

*Keywords— **Blockchain Applications, Blockchain Vs. GDPR, Data Protection Regulation, Meta-synthesis, Applicability Model, Blockchain & GDPR Compliance.***

1. Introduction

Blockchain technology has rapidly gained attention across various industries due to its ability to improve data management through increased security, transparency, and trust. Unlike traditional systems, blockchain's decentralized and immutable nature offers a new way to handle data. However, this same technology creates challenges when used under strict data protection laws, such as the General Data Protection Regulation (GDPR) [50].

GDPR is designed to protect individuals' privacy by enforcing rules on how personal data is collected, stored, and managed. Key GDPR requirements include the right to have data erased, the right to data portability, and the need for clear consent before data processing. These rules often conflict with the permanent nature of blockchain, making it difficult to comply with the regulation.

This paper focuses on the conflict between blockchain's immutability and GDPR's requirements, particularly the challenge of erasing or changing data once it is recorded on a blockchain. As blockchain is increasingly adopted in areas where data privacy is crucial, finding a way to reconcile these differences is essential [50].

The goal of this study is to explore the challenges and possible solutions for making blockchain systems comply with GDPR. By analyzing existing studies and legal perspectives, this paper aims to provide practical insights for developers, legal experts, and policymakers on how to use blockchain technology without violating GDPR [54].

To understand how blockchain can work within the framework of the GDPR, this paper will present comparative tables that detail both the supportive and challenging aspects of blockchain in meeting GDPR requirements. These discussions aim to find a balance between leveraging the technological advantages of blockchain and adhering to strict data protection laws. Therefore, we have introduced each of the topics of blockchain and GDPR in the section called Background as follows:

doi http://dx.doi.org/10.22133/ijwr.2024.459490.1221

Citation A. Arabsorkhi, E. Khazaei, "Blockchain Technology and GDPR Compliance: A Comprehensive Applicability Model", *International Journal of Web Research*, vol.7, no.2,pp.49-63, 2024, doi: http://dx.doi.org/10.22133/ijwr.2024.459490.1221.

*Coressponding Author

Article History: Received: 25 December 2023; Revised: 28 February 2024; Accepted: 9 March 2024.

2. Background

2.1. Blockchain Technology: A New Paradigm in Digital Transactions

Introduction to Blockchain Technology

Blockchain technology represents a revolutionary shift in processing information and conducting transactions. At its core, blockchain is a distributed ledger technology (DLT) that records transactions across multiple computers, ensuring security, immutability, and decentralization. Unlike traditional systems that rely on a central authority, blockchain operates through a consensus mechanism among participants to validate transactions, which are then recorded in blocks [48].

The decentralized nature of blockchain eliminates the need for intermediaries, thereby reducing costs and increasing efficiency. Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction data. This structure ensures that once data is recorded, it is incredibly difficult to alter without changing all subsequent blocks, making the blockchain highly secure and tamper-resistant. This characteristic of immutability is a significant advantage over traditional databases where data can be more easily manipulated [48]. Moreover, the consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensures that all participants in the network agree on the validity of transactions before they are added to the ledger. This distributed consensus process not only enhances security but also fosters trust among users who may not know each other. Blockchain's applications extend beyond cryptocurrencies, including supply chain management, healthcare, finance, and voting systems, showcasing its potential to transform various industries [1].

Structure and Functionality

Each block on the blockchain contains a list of transactions, is timestamped when it is completed, and cryptographically linked to the previous block. This linkage forms a chain of blocks, or a blockchain, making it resistant to data alteration because any change in one block would require alterations in all subsequent blocks, which is practically infeasible.

The cryptographic linkage between blocks is achieved through hash functions, which generate a unique fixed-size string of characters based on the input data of each block. Any modification to the data in a block results in a completely different hash value, ensuring the integrity and security of the blockchain. The hash of each block includes the hash of the previous block, thereby creating a chain where altering a single block would necessitate changing the hash values of all following blocks. This interconnectedness significantly enhances the security of the blockchain, making unauthorized changes extremely difficult [28].

Furthermore, the timestamp in each block ensures that transactions are recorded in a chronological order, providing a transparent and verifiable history of all transactions. This transparency is one of the key features that distinguishes blockchain technology from traditional databases, where transaction histories can be more easily obfuscated or altered. The combination of cryptographic security and chronological ordering makes blockchain a robust solution for applications requiring high levels of data integrity and transparency [28].

Applications Across Sectors

Blockchain's impact spans many industries, significantly improving efficiency, transparency, and trust [2, 50]. In finance, it supports cryptocurrencies and makes payments faster and cheaper. Blockchain provides a secure and transparent way to record transactions, reducing the need for intermediaries and central authorities and lowering transaction costs. For example, blockchain technology is used in cross-border payments, making them quicker and more affordable than traditional methods [49].

In supply chain management, blockchain improves traceability and accountability by creating a secure record of a product's journey from its origin to the consumer. This is important for ensuring products are genuine, preventing fraud, and meeting regulatory requirements. For instance, blockchain can track food items from the farm to the table, ensuring safety and allowing quick action if there is contamination [51].

In healthcare, blockchain secures patient data and ensures privacy. By creating a decentralized and unchangeable record of patient information, blockchain can make medical records more accurate, improve data sharing among healthcare providers, and prevent data breaches. In real estate, blockchain makes property transactions simpler by providing clear and verifiable records of ownership, reducing the risk of fraud, and streamlining the buying and selling process [52].

In legal affairs, blockchain can be used for smart contracts—agreements that automatically execute when certain conditions are met [3]. These contracts reduce the need for middlemen and lower the chances of disputes. Additionally, the Internet of Things (IoT) benefits from blockchain by providing a secure way for devices to communicate, improving data security, and enabling decentralized networks of smart devices [2].

Challenges and Potential

Despite its benefits, blockchain's adoption raises significant concerns, particularly regarding privacy and security. The technology's ability to create immutable records raises questions about data correction and deletion, especially in light of evolving privacy laws. For instance, regulations like the General Data Protection Regulation (GDPR) in Europe require the right to be forgotten, which conflicts with blockchain’s fundamental principle of immutability. Addressing this issue requires innovative solutions, such as off-chain storage or advanced cryptographic techniques that allow data to be effectively erased or modified without compromising the integrity of the blockchain.

Moreover, the increasing complexity and scale of blockchain networks necessitate robust security measures to prevent breaches and unauthorized access. As blockchain systems grow, they become more attractive targets for cyberattacks. Ensuring the security of these networks involves not only safeguarding against external threats but also managing internal risks, such as vulnerabilities in the consensus mechanisms or smart contract codes. Advanced security protocols and continuous monitoring are essential to maintaining the integrity and reliability of blockchain systems.

Additionally, scalability remains a significant challenge for blockchain technology. As more transactions are added to the blockchain, the network can become slower and less efficient. Solutions such as splitting network into smaller parts, off-chain transactions, and layer-two protocols are being developed to address these issues, but they are still in the early stages of implementation. Overcoming scalability challenges is crucial for blockchain to handle the transaction volumes required by global applications, ensuring that it can support widespread adoption across various sectors [3].

2.2. The General Data Protection Regulation (GDPR): Setting New Standards for Privacy

Background and Objectives

The General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, was established to safeguard personal data within the European Union (EU) and the European Economic Area (EEA) [25]. The scope of GDPR extends well beyond the EU's geographical boundaries, impacting any organization worldwide that processes the personal data of EU citizens. This wide-reaching regulation aims to enhance individual privacy rights and ensure that data handling practices are transparent and secure [25].

The primary objective of GDPR is to give individuals greater control over their personal data. This is achieved by enforcing a set of strict rules on those who collect, store, and manage this data, referred to as data controllers and processors. The regulation mandates that these entities must ensure the data they handle is processed legally, transparently, and for legitimate purposes. Additionally, it requires that personal data is kept secure and protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage [5].

Furthermore, GDPR introduces the requirement for clear consent to be obtained from individuals before processing their personal data. This consent must be explicit and informed, giving individuals a more tangible grasp of how their data is being used. Organizations must also provide easy options for individuals to withdraw consent at any time, reinforcing the control individuals have over their personal data [7].

By setting these new standards, GDPR not only protects individual privacy but also reshapes the way organizations across the globe approach data privacy. The regulation's stringent requirements and substantial penalties for non-compliance emphasize the importance of data protection in today's digital age, encouraging organizations to adopt higher standards of data privacy [25].

Core Principles

The GDPR is built around several key principles: Lawfulness, Fairness, and Transparency; Purpose Limitation; Data Minimization; Accuracy; Storage Limitation; Integrity and Confidentiality (Security); and Accountability. These principles ensure that personal data is processed securely, lawfully, and only for the intended purpose. Moreover, they demand that data is accurate, stored only as long as necessary, and managed in a way that ensures confidentiality and security [25].

Impact on Organizations

The implementation of the General Data Protection Regulation (GDPR) has profound implications for organizations worldwide, necessitating a comprehensive overhaul of their data protection measures. To comply with GDPR, organizations must implement stringent data protection protocols, conduct regular audits to ensure compliance, and maintain complete transparency in their data processing activities. This means that any entity that handles personal data must not only protect it from misuse but also clearly document how the data is collected, stored, used, and shared [30, 44].

Compliance with GDPR also requires organizations to appoint a Data Protection Officer (DPO) if they are involved in large-scale processing of personal data or special categories of data such as health records. The DPO is responsible for overseeing data protection strategies and ensuring compliance with GDPR requirements. This role is critical in bridging the gap between regulatory bodies and the organization, ensuring that all practices adhere strictly to the new standards [53].

The advantages of adhering to GDPR extend beyond avoiding substantial fines; they also include fostering greater trust with consumers. In today's digital landscape, consumers are increasingly aware of data privacy concerns and prefer companies that effectively safeguard their personal information. By complying with GDPR, organizations not only fulfill legal obligations but also improve their market reputation and competitive edge.

3. Research Goals

The main objective of this study is to create an in-depth comparative analysis of technical alternatives for integrating blockchain, with the aim of establishing a conceptual framework for identifying and selecting blockchain applications within the General Data Protection Regulation (GDPR) framework. To support this main objective, our research is structured around several key sub-objectives:

1. In-depth Exploration and Analysis: We will conduct a thorough exploration and analysis of the various technical blockchain development options that have been utilized for GDPR compliance in different countries. This will include a detailed examination of how these technologies have been adapted and implemented across various jurisdictions to meet GDPR requirements.
2. Development of an Applicability Model: Based on an exhaustive review of best practices, we aim to develop and propose an Applicability Model. This model will serve as a comprehensive guide for the identification and selection of the most appropriate blockchain applications for GDPR purposes. Our model will be grounded in the insights gained from global best practices, ensuring its relevance and utility for stakeholders.
3. Effectiveness Analysis of Blockchain Applications**:** A critical component of our research will involve analyzing the effectiveness of each blockchain application in the context of GDPR. This analysis will not only assess the technical feasibility but also evaluate the real-world impact of blockchain applications on enhancing GDPR compliance. Our focus will be on identifying the applications that demonstrate the most significant potential for improving data protection and privacy in line with GDPR standards.

By achieving these objectives, our research aims to contribute significantly to the body of knowledge on blockchain technology and GDPR. We intend to provide valuable insights for policymakers, industry stakeholders, and technology developers, facilitating informed decision-making and strategic planning in the adoption and implementation of blockchain applications for GDPR compliance.

4. Methodology

This study employs a qualitative content analysis approach, tailored for contexts where quantitative methods are impractical. The qualitative content analysis offers a nuanced interpretation of textual data, through a systematic process of coding and identifying patterns, without the constraints of predefined categories [10, 11]. This method was chosen due to the novelty of our research area—applications of blockchain technology within GDPR frameworks—and the scarcity of existing theoretical literature. Our approach prioritizes a data-driven analysis, steering clear of predetermined classifications to organically derive insights from the gathered data. The research unfolds in 4 interconnected phases, detailed in Figure 1, to systematically explore the subject matter and generate findings grounded in the data. The first phase focuses on identifying pertinent literature and data, setting the stage for detailed examination.

In the second phase, we carefully select sources and systematically analyze content using the meta-synthesis technique, which helps in summarizing and interpreting qualitative data from various studies. This method, detailed by Sandelowski & Barroso [12], organizes the analysis process effectively, which is shown for clarity and depth in the presentation of findings through Table 1. Each source in this search must include at least one keyword from the items presented in Table 1. Given that the research topic has been of great interest to researchers in recent decades, all scientific

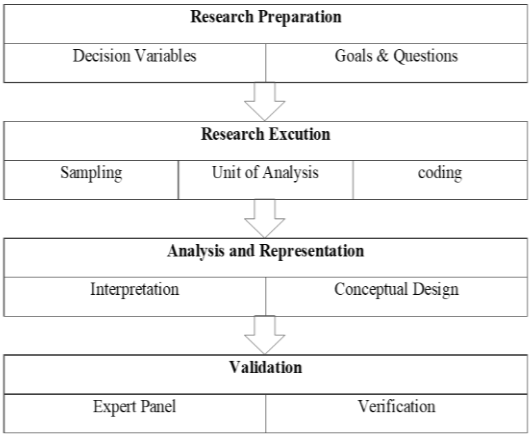

Figure 1. Research Framework

documents and international references such as theses and scholarly articles published in the past 10 years (2013-2023) have been explored. According to the method of meta-synthesis illustrated in Figure 2, the following steps were taken:

1. Selecting sources in a way that the final selected sources can represent a comprehensive overview of essential content in the research topic.
2. Identifying target texts and reviewing them several times to gain a proper understanding of the overall content.
3. Extracting meaningful units and categorizing them under headings called codes.
4. Summarizing and categorizing codes under concept titles and selecting suitable labels for them.
5. Sorting concepts into fewer themes based on similarities and differences in concepts, and ultimately selecting a suitable title that covers the resulting concepts. The selected documents were thematically coded in qualitative data analysis software, MAXQDA.

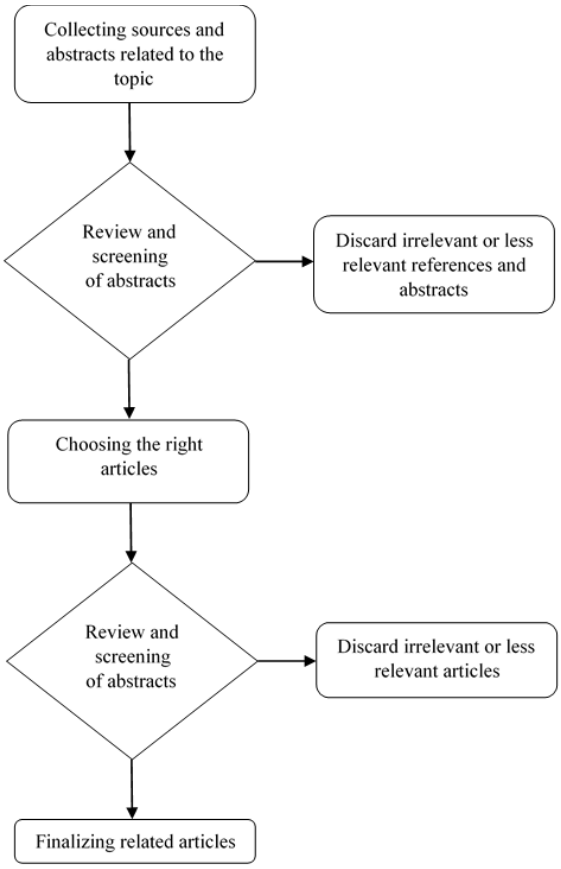
Collecting sources and abstracts related to the topic
Review and screening of abstracts
Discard irrelevant or less relevant references and abstracts
Choosing the right articles
Review and screening of abstracts
Discard irrelevant or less relevant articles
Finalizing related articles

Figure 2.A simple diagram of the process of searching and selecting related final documents and articles

The third phase involves a comparative analysis of findings through intra-case and inter-case studies, aiming to evaluate and rank blockchain applications in GDPR requirements. This step seeks to uncover patterns and differences among applications, enhancing our understanding of their significance and impact on GDPR compliance in our comparative study.

In the final phase, we aimed to measure and validate the model developed from the qualitative study. To do this, we formed a panel of 13 experts. This panel included 4 faculty members who have published articles or books on blockchain communication and GDPR, and 9 experts who are actively involved in research projects related to the application of blockchain technology in GDPR. After collecting experts' opinions and their fuzzy analysis in the third round, the areas of applicability of blockchain technology to support GDPR requirements and the priority of each of them were determined, and the results are presented in the form of a table.

5. Related Works

In this study, to identify the application of blockchain technology and assess its frequency in meeting GDPR requirements, we initially present a table describing the results of the reviewed articles on blockchain capabilities, along with brief explanations for each. Then, for the sake of completeness, we find it necessary to briefly outline the fundamental principles of GDPR [31], which are explained in Table 2. These requirements form the backbone of GDPR, ensuring that personal data is processed safely, lawfully, and transparently, providing a framework for data protection that organizations must adhere to within the European Union and for EU citizens' data processed outside the EU [26, 34].

In a comprehensive review, Table 3 delves into the technological capabilities of blockchain. This analysis highlights the technical capacities of

Table 1. The scope and direction of research analysis on the applications of blockchain technology in meeting the GDPR requirements

Scientific Databases	IEEE Xplore, Scopus, ScienceDirect, Emerald, ProQuest, Springer, MDPI, ACM
Resource Types	scientific-research journals; International conferences and related white papers
Keywords	Blockchain Applications, Blockchain Vs. GDPR, Data Protection Regulation, Meta-synthesis, Applicability Model, Blockchain & GDPR Compliance.
Resource Analysis & Filtering	Primary search (67 articles) and selected articles (31 articles).

Table 2. GDPR Principles

GDPR Principles	***Brief Explanation***	***Ref***	***GDPR Articles***
Lawfulness, Fairness, and Transparency	Processing must be lawful, fair, and transparent to the data subject.	[24], [6]	art.5(1), art.6, art.12-14
Purpose Limitation	Data must be gathered for clear, specific, and lawful purposes, and should not be processed further in ways that deviate from these initial purposes.	[24], [6]	art.5(1)(b)
Data Minimization	Data collection should be sufficient, pertinent, and restricted to the extent required for the intended processing purposes.	[17], [24], [6]	art.5(1)(c), art.16, art.17
Accuracy	Personal data must be precise and, if required, regularly updated to ensure accuracy.	[24], [6]	art.5(1)(d), art.17
Storage Limitation	Personal data should be retained in a format that allows for the identification of data subjects only for the duration required to fulfill the purposes for which the personal data are processed.	[17], [24], [6],[32]	art.5(1)(e), art.17
Integrity and Confidentiality (Security)	Personal data must undergo processing in a manner that guarantees adequate security measures, safeguarding against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.	[24], [6]	art.5(1)(f), art.32
Accountability	The controller is responsible for and must be able to demonstrate compliance with, the above principles.	[1], [25], [6]	art.5(2), art.24, art.28
Right to be forgotten and Right to erasure	Individuals are entitled to request the deletion of their personal data under specific circumstances, such as when the data is no longer needed for its original purpose or when the individual retracts their consent.	[6], [37]	Art.17

Table 3. Blockchain Capabilities

Blockchain Capabilities	***Brief Explanation***	***Ref***
Distributed	Data is stored across a network of nodes.	[28], [23], [21],[29]
Disintermediation	Enables direct transactions between parties without intermediaries.	[13], [25], [21].[29]
Traceability	Complete transaction history is trackable and auditable.	[44], [13], [21]
Decentralization	Eliminates the need for a central authority, ensuring a distributed control and management system.	[28], [13], [23],[32]
Transparency	Transactions and data are visible to all participants.	[13], [18],[29]
Immutability	Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring data integrity.	[28], [13], [23]
Persistence	Once data is recorded on the blockchain, its persistence ensures it cannot be tampered with or subjected to unauthorized changes.	[13], [19], [23]
Irreversibility	To reverse or undo transactions once they have been recorded and confirmed on the blockchain, ensuring the permanence and immutability of data.	[13], [19],[29]
Authenticity	To verify that a user or application is indeed the entity it claims to be. It ensures that the identity or origin of the user or application is genuine and trustworthy.	[13], [19],[29]
Non-Repudiation	To ensure that a party cannot deny the authenticity or validity of a transaction or communication, providing assurance and accountability for actions taken	[13], [21],[29]
Integrity	To ensure that information remains accurate, consistent, and unaltered throughout its lifecycle, thus maintaining its reliability and trustworthiness	[13], [21],[29]
Security	Uses cryptographic techniques to secure data transactions, making them tamper-proof and secure.	[28], [15], [21]
Smart Contracts	Self-executing contracts with the terms directly written into code, automating and enforcing agreements.	[28], [13], [23]
Consensus Mechanisms	Ensures all participants agree on the validity of transactions, maintaining network integrity.	[20], [21], [23]
Privacy	Offers mechanisms like private transactions and permissioned blockchains to protect user data.	[23, [20], [21]
Scalability	Efforts to improve blockchain's ability to handle large volumes of transactions efficiently.	[14], [21], [22]
Data Encryption	Protects information by transforming it into an unreadable format, which can only be deciphered with a secret key.	[23], [18], [4]
Pseudonymization	A method to replace private identifiers with fake identifiers or pseudonyms to protect privacy while maintaining record integrity.	[14], [18]

blockchain technology that catalyze investment in and application of this technology, not solely within the scope of GDPR but also extending to various sectors and industries. These technological capabilities are pivotal in securing a competitive edge and establishing distinctiveness among blockchain beneficiaries compared to other applied technologies, owing to their inherent dynamism and the considerable challenge in imitation.

Concurrently, the GDPR mandates, delineated in Table 2, impose essential obligations on data controllers and data processors to ensure data protection. Additionally, the GDPR specifies particular responsibilities for the Data Subject [33]. Failure to adhere to any of these mandates is deemed a legal violation by individuals, organizations, businesses, industries, or service operators, potentially incurring severe repercussions, including the revocation of licenses/certificates, and imposition of financial penalties, among others. These mandates have been legislated by the Parliament of the European Union, endorsed by the Parliaments of North American countries, and ratified by the Parliaments of Southeast Asian and Pacific countries, making compliance compulsory for all entities within the ICT ecosystems of these region.

6. Finding

Table 4 shows how blockchain technology fits with GDPR requirements, making it easier to see the connection between blockchain features and GDPR rules. It says which blockchain abilities meet GDPR rules with a "YES." The numbers in brackets show how often blockchain can help follow GDPR rules, based on a look at 31 selected articles. These articles were picked using a CASP method, focusing on how they relate to our study. The table points out which parts of blockchain can help or hurt GDPR compliance. We then explain how blockchain relates to GDPR's data processing rules, picking out 12 main blockchain features that help with GDPR compliance, like Distributed Systems, Decentralization, and Data Encryption. However, some blockchain features might not fully fit with GDPR. Our research involved looking through articles digitally and physically to get all the relevant information.

6.1. Lawfulness, Fairness, and Transparency

Blockchain transparency improves GDPR compliance by allowing data processing activities to be easily seen and checked [4]. Smart contracts also align with GDPR's lawfulness principle since they only execute transactions when certain legal conditions are fulfilled, ensuring that data processing via smart contracts is legally justified [41, 42]. Furthermore, blockchain's privacy features support GDPR's requirement for lawful data processing by enhancing data protection and ensuring compliance with legal standards [43].

6.2. Purpose Limitation

Under the GDPR, it is required that personal data be collected only for clear, specific, and legitimate reasons [39], and not used in ways that don't match these reasons. Once data is put on a blockchain, it cannot be changed or deleted. However, smart contracts can help adhere to GDPR's Purpose Limitation principle by setting specific conditions for data use [35]. Additionally, blockchain's consensus mechanisms align with this principle by enforcing agreed-upon conditions for data processing and verification, ensuring that data sharing and processing within the network comply with the original purpose of data collection, thus meeting GDPR standards [34].

6.3. Data Minimization

The capabilities of distributed systems, disintermediation, and decentralization, inherent to blockchain technology, are not aligned with the GDPR's Data Minimization principle. This principle dictates that only the necessary amount of personal data for processing purposes should be collected [31]. Blockchain's nature involves duplicating data across many nodes in a distributed network, which could conflict with the goal of data minimization. Moreover, the decentralized structure and the removal of intermediaries mean that data is stored and managed across a widespread network, complicating efforts to restrict the volume of data held on the blockchain [46]. However, Smart Contracts and Consensus Mechanisms in blockchain tech help adhere to the GDPR's Data Minimization rule. Smart Contracts automate processes, ensuring only vital data for transactions is collected, reducing personal data. Consensus Mechanisms like PoW or PoS verify transactions before adding them to the blockchain, ensuring only necessary data is included. By automating and validating data transactions, they cut down on unnecessary data storage and processing, and sticking to GDPR's Data Minimization rule [45].

6.4. Accuracy

The GDPR mandates that personal data remain accurate and up-to-date, yet blockchain's immutability, persistence, and irreversibility are not compatible with this principle [35]. Once data is stored on a blockchain, it becomes impossible to modify or remove, creating a discrepancy between the blockchain's fixed data approach and the GDPR's requirement for data accuracy and correction. However, smart contracts provide a solution by enabling automated task execution based

Table 4. Usability of Blockchain Capabilities in GDPR Requirements

GDPR Principles ***Blockchain Capabilities***	***Lawfulness, Fairness, and Transparency***	***Purpose Limitation***	***Data Minimization***	***Accuracy***	***Storage Limitation***	***Integrity and Confidentiality (Security)***	***Accountability***
Distributed	YES (12%)					YES (12%)	
Disintermediation							
Traceability							
Decentralization	YES (12%)					YES (12%)	
Transparency	YES (10%)						
Immutability	YES (16%)					YES (16%)	
Persistence	YES (16%)					YES (16%)	
Irreversibility	YES (16%)					YES (16%)	
Authenticity							
Non-Repudiation							
Integrity						YES (3%)	
Security	YES (6%)					YES (6%)	
Smart Contracts	YES (22%)	YES (22%)	YES (22%)	YES (22%)	YES (22%)	YES (22%)	YES (22%)
Consensus Mechanisms		YES (10%)	YES (10%)	YES (10%)		YES (10%)	YES (10%)
Privacy	YES (6%)					YES (6%)	
Scalability							
Data Encryption		YES (12%)				YES (12%)	
Pseudonymization							
	32%	10%	6.5%	16%	3.5%	35%	22%

on specific conditions, such as user consent [36, 37]. This feature aligns with the GDPR's accuracy requirement, ensuring that personal data remains accurate and, when necessary, updated. Additionally, consensus mechanisms play a crucial role in maintaining data accuracy on the blockchain. By verifying transactions across multiple nodes before adding them to the blockchain, consensus mechanisms prevent fraudulent or inaccurate information from being recorded, thereby supporting the principle of accuracy [36].

6.5. Storage Limitation

The GDPR requires that personal data should not be kept longer than necessary for the purposes for which it was collected [39]. In blockchain systems, data is stored indefinitely across all nodes in the network, contributing to the immutability and persistence of the data [46]. This perpetual storage conflicts with the Storage Limitation principle, as data cannot be easily deleted or removed once added to the blockchain [40]. However, off-chain data storage solutions can comply with the GDPR's Storage Limitation principle by keeping personal data outside the blockchain [35, 40].

6.6. Integrity and Confidentiality (Security)

Blockchains are known for their unchangeable, lasting, and irreversible nature, providing an open and transparent platform for all users [46]. This capability guarantees the security and reliability of data stored within the blockchain network. Because data on the blockchain cannot be changed or deleted without agreement from everyone involved, its integrity remains intact over time. Additionally, the durability and permanence of blockchain transactions create a strong and dependable system where data is securely stored and easily accessible to authorized users, ensuring the integrity of shared information across the network [45].

6.7. Accountability

GDPR emphasizes data subjects' control over their personal information, with a designated controller responsible for managing data subject consent [40]. While the Blockchain operates on a decentralized framework accountability is thus distributed among various participants. Typically, entities like node operators, miners, and developers share responsibility for maintaining and managing the blockchain network's integrity and security. However, the level of accountability varies based on factors like the consensus mechanism used, governance structure, and assigned roles and responsibilities. Another incompatible capability of blockchain, which conflicts with GDPR accountability, is data encryption. Encrypting data before storing it on the blockchain is inconsistent with GDPR principles and may conflict with accountability and transparency requirements. These principles dictate that data should be managed in a manner that upholds the rights of data subjects and enables controllers to demonstrate compliance with regulations, regardless of data encryption [16]. Among the solutions that render blockchain compatible with GDPR, two notable approaches include the utilization of contracts and the adoption of private and permissioned blockchains [38], Because in permissioned blockchains, where access is restricted to specific entities, data controllership and accountability are clearer compared to public blockchains [44], and also the blockchain contract specifies who is allowed to read and update the contract variables [47].

6.8. Blockchain and GDPR: Conflicts and Synergies

The link between blockchain technology and the General Data Protection Regulation (GDPR) is complex. Blockchain's main parts—decentralization, transparency, and immutability—bring big benefits for GDPR. They help make data safe and clear, which are key parts of GDPR. But these same parts might also make problems with GDPR. For example, blockchain's way of keeping data unchangeable clashes with GDPR's idea of letting people forget their data. This means people can ask for their data to be erased, but blockchain can't do that. Also, blockchain's way of keeping all data might not fit with GDPR's idea of only keeping needed data. To solve these problems, new tech and rules are needed. One way is to make tech that makes data safer but still lets people check it without seeing everything. Another idea is to change how blockchain works so data can be erased without hurting the record. Another way is to use both blockchain and other ways to keep data, so that only needed data is on blockchain.

In the end, making blockchain fit with GDPR needs to find a balance, making the most of blockchain's good parts while still following the rules. This means people who make tech, rules, and business need to keep talking to make things better.

6.9. The conceptual model of the applicability of blockchain technology capabilities

The conceptual model of the applicability of blockchain technology capabilities in the degree of meeting the GDPR based on a meta-synthesis study has been developed in Figure 3. Based on this, the highest and lowest percentages of blockchain technology applicability have been displayed. significant blockchain features like smart contracts and consensus mechanisms can, under specific conditions, ensure compliance with regulatory standards. These capabilities, when effectively leveraged, provide a pathway to reconcile blockchain technology with legal frameworks, albeit within certain boundaries. Notably, smart contracts emerge as the most applicable blockchain feature, accounting for 23% of the utility in aligning with regulatory requirements, followed closely by immutability, persistence, and irreversibility, each holding 16%. This indicates a strong preference for features that ensure data reliability and permanence, despite their challenges with regulatory compliance.

Other notable aspects include distributed architectures and data encryption, both at 12%, and decentralization, also at 12%, underscoring the value of shared control and secure data management in regulatory contexts. Transparency and consensus mechanisms, each at 10%, highlight the importance of open processes and agreement protocols in meeting compliance standards. Meanwhile, security, at 6%, and integrity, at 3%, though less predominant, remain critical for establishing trust and ensuring data accuracy within blockchain systems. This detailed analysis emphasizes the potential for blockchain technology to be molded in a manner that respects the delicate balance between innovation and regulatory compliance. As we move forward, policymakers, technologists, and legal experts must collaborate closely, developing frameworks that harness blockchain's strengths while mitigating its limitations, ensuring a future where technology and regulation coexist in harmony for the greater good of data protection and privacy.

The conceptual model, Figure 2 presents the percentage convergence of each blockchain capability with the principles and requirements of GDPR. Accordingly, the highest applicability is related to smart contracts at 22%, while the lowest applicability is attributed to the Integrity capability at 3%. Specific conditions related to blockchain, such as technology architecture and deployment conditions, influence these priorities. This conceptual model was developed into a questionnaire and evaluated by a 13-member expert panel, including: 4 faculty members with publications in the field of blockchain communication and GDPR. 9 experts active in research projects on the application of blockchain technology within GDPR. After collecting expert opinions and performing fuzzy analysis in the third round, the level of applicability and the priority of each blockchain capability were determined, with the results presented in Table 5.

The results presented in Table 5 clearly demonstrate that the conditions for applying blockchain within GDPR do not necessarily align with the findings from qualitative studies. For instance, commonly used capabilities like Distributed, in the realm of Integrity and

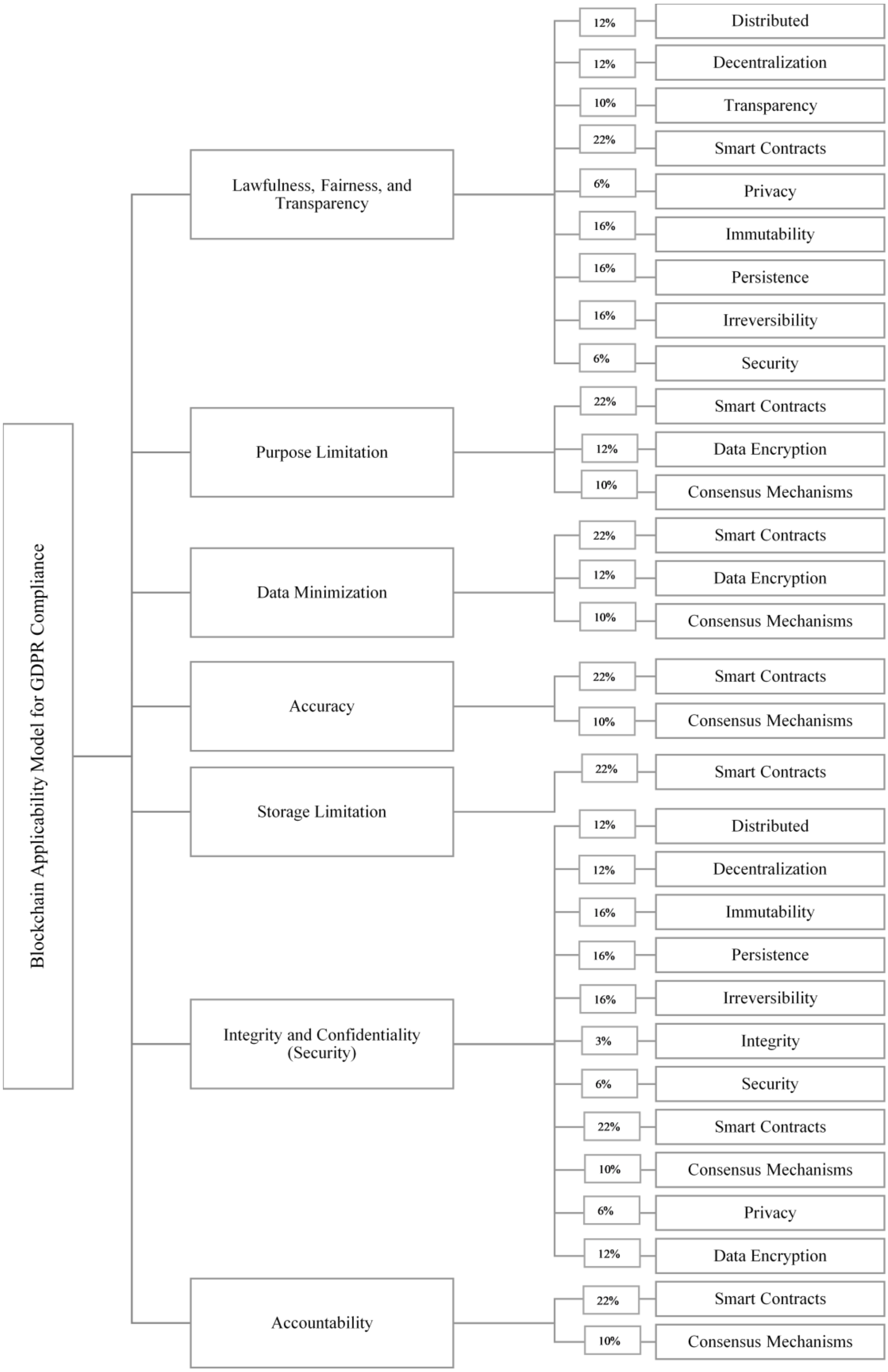

Figure 3. Blockchain Applicability Model for GDPR Compliance

Table 5. Research Results on the Priority Applications of Blockchain Capabilities in GDPR

Applicability Components		***Average Priority Given By Members***		***Difference***
Blockchain Capabilities	GDPR Principles	2nd Round	2rd Round	
Distributed	Lawfulness, Fairness, and Transparency	3.20	3.48	0.28
	Integrity and Confidentiality (Security)	3.12	2.74	-0,62
Decentralization	Lawfulness, Fairness, and Transparency	3.17	3.43	0.26
	Integrity and Confidentiality (Security)	3.56	3.68	0.12
Transparency	Lawfulness, Fairness, and Transparency	3.84	3.93	0.09
Immutability	Lawfulness, Fairness, and Transparency	3.26	3.48	0.22
	Integrity and Confidentiality (Security)	3.49	3.74	0.25
Persistence	Lawfulness, Fairness, and Transparency	3.43	2.88	-0.45
	Integrity and Confidentiality (Security)	3.57	3.85	0.28
Irreversibility	Lawfulness, Fairness, and Transparency	3.41	3.52	0.11
	Integrity and Confidentiality (Security)	3.26	3.58	0.32
Integrity	Integrity and Confidentiality (Security)	3.49	3.78	0.29
Security	Lawfulness, Fairness, and Transparency	3.44	2.93	-0.49
	Integrity and Confidentiality (Security)	3.21	3.28	0.07
Smart Contracts	Lawfulness, Fairness, and Transparency	3.45	3.86	0.41
	Purpose Limitation	3.87	3.93	0,06
	Data Minimization	3.01	3.33	0.32
	Accuracy	3.63	3.84	0.21
	Storage Limitation	3.17	3.42	0.25
	Integrity and Confidentiality (Security)	3.64	3.93	0.29
	Accountability	3.35	3.87	0.52
Consensus Mechanisms	Purpose Limitation	3.43	2.92	-0.49
	Data Minimization	3.12	2.66	-0.54
	Accuracy	3.65	3.79	0.14
	Integrity and Confidentiality (Security)	3.71	3.89	0.18
	Accountability	3.52	3.71	0.19
Privacy	Lawfulness, Fairness, and Transparency	3.32	2.86	-0.54
	Integrity and Confidentiality (Security)	3.40	3.47	0.07
Data Encryption	Purpose Limitation	3.51	3.83	0.32
	Integrity and Confidentiality (Security)	3.64	3.79	0.15

Confidentiality requirements, were excluded from the proposed framework. Based on the analysis, the Smart Contract capability in the domains of Purpose Limitation and Integrity and Confidentiality, and the Transparency capability in the domain of Lawfulness, Fairness, and Transparency, were identified as priority blockchain capabilities within the GDPR framework.

7. Discussion

Innovation plays a crucial role in advancing research, especially in fast-changing fields like blockchain and data protection. This study introduces new ideas not just by exploring how blockchain can work with GDPR, but also through fresh approaches in methodology, analysis, and model creation. By using advanced research methods and offering new perspectives on existing challenges, this research provides valuable insights and practical solutions for better integrating blockchain technology within strict data protection regulations.

7.1. Innovation in Methodology

One key difference in this study compared to others in the field is its use of the meta-synthesis method. This method has not been widely used in this area before. Meta-synthesis is highly structured for analyzing qualitative data, involving a detailed and targeted approach to selecting sources and ensuring they align with the research goals and questions. Given the study's exploratory and descriptive nature, which includes theme analysis within a clear research framework, meta-synthesis is particularly suitable. It involves examining and combining findings from other qualitative studies on similar topics. Since this study focuses on how blockchain technology can be applied within the requirements of GDPR, the meta-synthesis method fits perfectly with the research objectives.

7.2. Innovation in Analysis

Many articles in this field have discussed the relationship between blockchain capabilities and GDPR requirements in a straightforward way, often labeling them as either applicable or not. However, some blockchain features, like smart contracts, can sometimes address and even resolve certain challenges related to GDPR compliance. This study, using the meta-synthesis method, reinterprets these capabilities to find new and alternative connections. By repeatedly analyzing the data and results from selected qualitative studies using the CASP method, the study identifies new conditions for applicability and defines new relationships between blockchain and GDPR.

7.3. Innovation in Modeling

The study's model for blockchain applicability within GDPR requirements, as shown in the tabular format (Table 4) and visual representation (Figure 2), offers a new perspective. This analysis and categorization approach in the context of blockchain and GDPR is unique, with no similar examples found in the 67 articles reviewed.

8. Conclusion

Our analysis highlights the relationship between blockchain technology and GDPR compliance. Capabilities such as "Immutability," "Persistence," and "Irreversibility" pose challenges to adhering to GDPR's data rectification and erasure mandates. In contrast, "Smart Contracts" and "Consensus Mechanisms" show potential for regulatory alignment. The decentralized nature of blockchain architecture adds complexity to compliance efforts. However, our findings indicate that blockchain has the nuanced potential to meet legal standards, especially through the regulatory utility of smart contracts. Collaborative efforts among policymakers, technologists, and legal experts are crucial in developing frameworks that exploit blockchain's benefits while mitigating regulatory discrepancies, aiming for a harmonious balance between innovation and compliance in data protection and privacy. In conclusion, this research has faced several significant limitations that impacted the depth and scope of the study. Notably:

- **Limited access to experts:** There was a lack of availability of experts specifically working on the application of blockchain in the GDPR domain within the country.
- **Collaboration challenges:** Difficulty in accessing individuals involved in implementing blockchain platforms and willing to participate in this research project.
- **Access to legal professionals:** Limited access to legal experts familiar with data protection laws and blockchain technology.
- **Time constraints:** Experts who were available faced time limitations, posing challenges in engaging them in the iterative Delphi method for gathering insights.

Based on the conducted studies and identified knowledge gaps, future research should address the following areas:

- Developing a readiness maturity model and assessing the maturity level of blockchain platforms to meet GDPR compliance requirements.

- Exploring various technological approaches within blockchain platforms to ensure adherence to personal data protection principles and requirements.

Declarations

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

Authors' contributions

AR: Led the study design, coordinated the research activities, acquired and analyzed data, interpreted the results, handled the final revisions and submission process;

EK: Contributed to the study design, assisted with the interpretation of the results, drafting and revising the manuscript.

Conflict of interest

The authors declare that there are no conflicts of interest.

Acknowledgements

The authors would like to express their gratitude to the ICT Research Institute (Iran Telecommunication Research Center - ITRC) for their invaluable moral support as the leading research entity in Information and Communication Technology, in support of this research conducted under the blockchain program in the ICT sector.

References

[1] Bilal, K., Sajid, M., Singh, J., "Blockchain Technology: Opportunities & Challenges," in *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, 2022.

[2] Wajde B., Janet L., Aniket M., "Blockchain Technology and its Applications Across Multiple Domains: A Survey," *Journal of International Technology and Information Management*, p. 29, 2021.

[3] Adegboyega O., Samuel A., "Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries," in *Government 3.0 – Next Generation Government Technology Infrastructure and Services*, 2017, pp. 283-298.

[4] Seing H., Sooyong P., "A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review," *IEEE Open Access Journal*, 2022.

[5] Paul V., "The EU General Data Protection Regulation (GDPR): A Practical Guide," 2017.

[6] Fabio A. C., "The GDPR-Blockchain paradox: a workaround," in *1st workshop on GDPR compliant systems, co-located with 19th ACM International Middleware Conference*, 2018.

[7] Elif K.C, "Data Protection Around the World," in *Information Technology and Law Series*, 2021, pp. 1-6.

[8] Raffi T., "The Puzzle of Squaring Blockchain with the General Data Protection Regulation," *Jurimetrics*, p. 60, 2020.

[9] Unal T., Yasir G., "Law versus technology: Blockchain, GDPR, and tough tradeoffs," in *Computer Law & Security Review*, 2020.

[10] Kathleen M. Eisenhardt, "Building Theories from Case Study Research," *The Academy of Management Review*, vol. 14, pp. 532-550, 1989.

[11] Fatemeh S., "Configurations of platform organizations: Implications for complementor engagement," *Research Policy*, vol. 48, 2019.

[12] Dr. Barroso, Handbook for Synthesizing Qualitative Research, Springer Publishing Company, Inc, 2006.

[13] Matthieu Quiniou, Blockchain: The Advent of Disintermediation, 2019.

[14] Abouzar A., "Blockchain Applications for the Police Task Force of IRI: A Conceptual Framework Using Fuzzy Delphi Method," *Journal of Information Technology Management*, pp. 36-61, 2021.

[15] Benjamin S., Fabiane V., Nils U., Johannes S., "Yes, I Do: Marrying Blockchain Applications with GDPR," in *Hawaii International Conference on System Sciences*, 2022.

[16] Gholamhossein K., Mengiste S. A., "Conceptualization of A GDPR-Mining Blockchain-Based Auditor: A Systematic Review," in *The Seventh International Conference on Advances and Trends in Software Engineering*, 2021.

[17] Michele F., "Blockchains and Data Protection in the European Union," *EDPL*, pp. 17-35, 2018.

[18] Javed A., Sule Y., Mariusz N., "Towards Blockchain-Based GDPR-Compliant Online Social Networks: Challenges, Opportunities and Way Forward," in *Future of Information and Communication Conference*, 2020.

[19] Smita B., Lata R., "Challenges in making blockchain privacy compliant for the digital world: some measures," *Indian Academy of Sciences*, 2022.

[20] Florian Z., "Concepts for GDPR-Compliant Processing of Personal Data on Blockchain: A Literature Review," 2019.

[21] Don T., Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 2016.

[22] Qiheng Z., Huawei H., Zibin Z., "Solutions to scalability of blockchain: A survey," *IEEE*, 2020.

[23] Dodo K., Low T., Manzoor A., "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, 2021.

[24] Christopher F. M., Cosimo M., "The EU's General Data Protection Regulation (GDPR) in a Research Context," in *Fundamentals of Clinical Data Science*, 2018, pp. 55-71.

[25] Gianclaudio M., "The concept of fairness in the GDPR: a linguistic and contextual interpretation," in *IEEE/ACM 14th International Conference on Utility and Cloud Computing*, 2020.

[26] Peyo H., Willian D., "The blockchain as a backbone of GDPR compliant frameworks," in *8th International Multidisciplinary Symposium*, 2018.

[27] Andriy K., Torsten S., Maya T., Krzysztof F., John M., "Critical Assessment of Methods of Protein Structure Prediction (CASP) – Round XIV," pp. 1607-1617.

[28] Haris A., Gaganeet S. A., "GDPR compliance verification through a user-centric blockchain," *Computers and Electrical Engineering*, vol. 109, 2023.

[29] Cristòfol D. E., Jordi C., "Blockchain-based access control system for efficient and GDPR-compliant personal data management," *Computer Communications*, p. 67–87, 2024.

[30] Mani Karthik S., Pradnya P., "Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing," *Journal of Physics: Conference Series*, 2021.

[31] Rahime B., Enes A., Yang L., Shujun L., "A systematic literature review of the tension between the GDPR and public blockchain systems," *Blockchain: Research and Applications*, 2023.

[32] Michèle F., Blockchain and the General Data Protection Regulation, 2019.

[33] Asim J., "PRIVACY BETWEEN REGULATION AND TECHNOLOGY: GDPR AND THE BLOCKCHAIN," *IUS Law Journal*, pp. 47-59, 2022.

[34] Shenglan M., Chaonian G., Hao., Xia H., "Nudging Data Privacy Management of Open Banking Based on Blockchain," *IEEE*, 2018.

[35] AKM B. H., Bilal N., Najmul I., Sami H., "Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport," *Applied Science*, 2021.

[36] Gabriel Jaccard, Adrien T., "GDPR & Blockchain: the Swiss take," *Jusletter IT*, 2018.

[37] Nguyen B. T., Kai S., Gyu M., Yike G., "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 15, 2020.

[38] Yaman Salem., "GDPR-BLOCKCHAIN COMPLIANCE FOR PERSONAL DATA: REVIEW PAPER," *Journal of Theoretical and Applied Information Technology*, vol. 99, 2021.

[39] Michèle F.,, "Smart contracts as a form of solely automated processing under the GDPR," *International Data Privacy Law*, pp. 78-94, 2019.

[40] Gregory w., "Data Protection Issues for Smart Contracts," *HAL open science*, pp. 70-100, 2021.

[41] Karisma K., Pardis M. T., "Data protection governance framework: A silver bullet for blockchain-enabled applications," in *International Conference on Machine Learning and Data Engineering*, 2023.

[42] Luis-Daniel I., "On Blockchains and the General Data Protection Regulation," 2018.

[43] Ruas I., Ben D., "Blockchain and the GDPR – the shift needed to move forward," 2023.

[44] Gonçalves R. M., Miguel M. S., Paulo R., "Olympus: a GDPR compliant blockchain system," *International Journal of Information Security*, 2023.

[45] Mpyana M. M., Youn K. L., Seng-Phill H., "A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR," *Intelligent Sensors*, 2021.

[46] Satoshi N., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009.

[47] Ricardo N., Gary S., Igor N., "A Blockchain-based Approach for Data Accountability and Provenance Tracking," in *12th International Conference on Availability, Reliability and Security*, 2017.

[48] Zibin Z., Shaoan X., Hongning D. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 6th IEEE International Congress on Big Data, 2017.

[49] Mohd J., Abid H., Ravi P., Rajiv S., Shahbaz K., "A review of Blockchain Technology applications for financial services," BenchCouncil Transactions on Benchmarks, Standards and Evaluations, vol. 2, 2022.

[50] Sam C., Andrey G., Pop L., Samuel M., Roksana R., Tayseer S., Maria S., " Blockchain technology and its implications," OxJournal , 2023.

[51] Maher A.N. Agi, et al., "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," International Journal of Production Economics, vol. 247, 2022.

[52] Kianoush Kiania, "Blockchain-based privacy and security preserving in electronic health: a systematic review," National Center for Biotechnology Information, 2023.

[53]E. Comission, "Does my company/organisation need to have a Data Protection Officer (DPO)?".An official website of the European Union.

[54]Atefeh F., Abouzar A., "Providing a conceptual framework to identify and analyze the stakeholders and actors of the cryptocurrency ecosystem," Scientific Quarterly of National Security, pp. 245-276, 2021.

Abouzar Arabsorkhi received his Ph.D. in Information Systems Management from the University of Tehran. He is a faculty member at the Network and System Security Assessment Department of the Information and Communications Technology Research Institute. With over 20 years of research experience, he focuses on Security Management, Risk Management, Security Architecture, and Prototype Certification. His work includes developing security labs, blockchain platforms, and GDPR labs. He has led more than 18 applied research projects and teaches Information Systems and E-Commerce Security. His main research interests include the Internet of Things, blockchain, and emerging technology security.

Elham Khazaei earned a Bachelor's degree in Engineering from Tehran Central University and a Master's degree in IT Management with a focus on E-Business from University of Tehran. Her research areas include blockchain, the Internet of Things, and the metaverse. She explores the impact of emerging technologies such as blockchain, IoT, and the metaverse on business strategies.