Comparative Studies: Blockchain Technology Applications in GDPR - Representing an Applicability Model

Elham Khazaei
Faculty of IT Management
University of Tehran
Tehran, Iran
Elham.khazaei@ut.ac.ir

Abouzar Arabsorkhi*
Associated professor, Department of ICT security
Iran Telecommunications Research Institute
Tehran, Iran
Abouzar_arab@itrc.ac.ir

2024 10th International Conference on Web Research (ICWR) | 979-8-3503-9498-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICWR61162.2024.10533322

***Abstract*— The application of blockchain technology in the context of the General Data Protection Regulation (GDPR) has emerged as a significant and challenging area of research in recent years. Many believe that blockchain capabilities can be leveraged to comply with GDPR principles. This study focuses on the specific capabilities of blockchain technology and addresses the unique data protection challenges in the information age, aiming to identify and represent these relationships through an applicability model. The goal of this research is to present a model for evaluating and selecting blockchain applications that are aligned with GDPR requirements. This model is developed through a meta-synthesis method and qualitative content analysis of 67 articles that concentrate on the potential applications of blockchain in GDPR across various countries. These applications are defined based on an analysis of key blockchain capabilities such as transparency, immutability, and data encryption. Further, this study maps these capabilities to key GDPR requirements such as data minimization and accuracy, analyzing them from both facilitating and inhibiting perspectives. Ultimately, based on qualitative content analysis and an in-depth study of 31 articles selected through the Critical Assessment of Methods of Protein Structure Prediction method (CASP), this research offers a comprehensive model for understanding and leveraging blockchain technology in a manner that complies with GDPR requirements. according to this, the study contributes to the understanding of blockchain technology's applicability in meeting GDPR requirements, offering insights for policymakers, industry stakeholders, and technology developers on the strategic implementation of blockchain for data protection.**

Keywords*— Blockchain Applications, Blockchain Vs. GDPR, Blockchain Applications in GDPR, Blockchain Adoption in GDPR, Blockchain & Data Protection Requirements, Blockchain & GDPR Compliance

I. INTRODUCTION

In the rapidly evolving digital landscape, the advent of blockchain technology has emerged as a cornerstone, bringing in a new era of decentralized and transparent transactions. At its core, "blockchain" is a distributed ledger technology that enables the recording of transactions across a network of computers in a manner that is secure, immutable, and without the need for a central authority [1]. This groundbreaking technology also changes how information is handled, stored, and retrieved, demonstrated by a connected series of "blocks". Each block includes a list of transactions, a timestamp marking its creation, and a secure link to the previous block. Because each block has data from the one before it, they create a continuous "chain," with each block supporting the one prior, as a result, the addition of each block to the blockchain strengthens the entire chain [28].

Blockchain technology is on a remarkable rise, mirroring the broader trend of technological progress that touches every aspect of our daily lives. Its applications extend across various fields such as finance, accounting, insurance, supply chain management, energy, advertising and media, legal, real estate, healthcare, and IoT. This diversity underscores blockchain's potential to revolutionize industries by enhancing efficiency, transparency, and trust [2]. This growing trend is not just a technological marvel but also a reflection of the increasing importance, investment, and influence of digital technologies across governments, industries, and businesses globally, it has a strong impact on every industry or product line that relies on storage and information and also can facilitate the governance systems [3]. However, the rapid development and adoption of blockchain have also brought to the forefront critical concerns regarding security and privacy. The digital age has seen an exponential increase in data generation, necessitating robust mechanisms to ensure the integrity and confidentiality of information. This has prompted governments worldwide to move towards the formulation and enforcement of comprehensive data protection laws, with the General Data Protection Regulation (GDPR) in the European Union being a prime example [30, 44]. GDPR sets a global benchmark for personal data protection [4]. The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in the European Union (EU) on May 25, 2018. It aims to protect the personal data of individuals within the EU and the European Economic Area (EEA). The regulation impacts not only organizations based in the EU but also those outside the EU that offer goods or services to, or monitor the behavior of, EU data subjects [25]. GDPR emphasizes transparency, security, and accountability by data processors and controllers, providing individuals with greater control over their personal data. Key elements include Lawfulness, Fairness, and Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Confidentiality (Security), and Accountability which are related to Article 5, which establishes the key principles related to the processing of personal data. The introduction of the General Data Protection Regulation (GDPR) [5] represents a significant step towards addressing data privacy concerns by granting citizens stringent control over their personal data and requiring entities that manage or process data to clearly state their purposes and obtain explicit consent [6]. This legislation compels operators and service centers to meet

high standards of data privacy and security, emphasizing the importance of GDPR compliance in the development of information services [7]. In this context, the role of blockchain in GDPR presents a unique intersection of challenges and opportunities [1]. Blockchain's inherent characteristics of decentralization, immutability, and transparency [8, 9] can potentially support GDPR's objectives of data protection and user privacy. However, the application of blockchain technology also encounters conflicts with GDPR principles, such as the right to erasure ('right to be forgotten') and data minimization, necessitating innovative solutions to reconcile these differences.

Understanding the applications and conflicts of blockchain within the GDPR framework requires a nuanced analysis. comparative tables format in the paper can clarify how blockchain can both support GDPR compliance and challenge its implementation, offering insights into potential resolutions that harmonize the technological benefits of blockchain with the stringent requirements of data protection laws.

II. Research Goals

The primary goal of this study is to develop a comprehensive comparative analysis of the technical alternatives available for blockchain integration, aimed at establishing a conceptual framework for the identification and selection of blockchain applications within the context of the General Data Protection Regulation (GDPR).

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.

III. 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 is particularly 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 three interconnected phases, detailed in Fig.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 I.

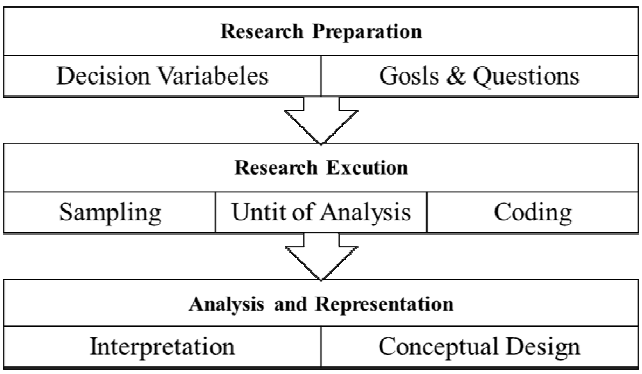

Fig. 1. Research Framework

TABLE I. 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, Blockchain Applications in GDPR, Blockchain Adoption in GDPR, Blockchain & Data Protection Requirements, Blockchain & GDPR Compliance
Resource Analysis & Filtering	Primary search (67 articles) and selected articles (31 articles).

The final 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.

IV. RELATED WORKS

In this study, to identify the application of blockchain technology and assess its frequency in meeting the GDPR requirements, initially, a table is presented 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 II. 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 III delves into the technological capabilities of blockchain. This analysis highlights the technical capacities of 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 II, 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.

V. FINDING

Table IV presents how blockchain technology aligns with GDPR requirements. It simplifies understanding the connection between blockchain features and GDPR principles by indicating which blockchain capabilities meet GDPR requirements with a "YES". The numbers in parentheses show how often blockchain can help follow GDPR rules, based on analysis from 31 selected articles. These articles were chosen using a CASP method [27], focusing on their relevance to our study. The table highlights which aspects of blockchain can help or hinder GDPR compliance. We then detail how blockchain relates to GDPR's data processing principles, identifying 12 key blockchain features that support GDPR compliance, such as Distributed Systems, Decentralization, and Data Encryption, among others [16]. Some blockchain features might not fully align with GDPR [23]. The research involved digital and physical searches to gather and review articles thoroughly.

A. 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].

B. 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.

TABLE II. 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 III. 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]

TABLE IV. BLOCKCHAIN CAPABILITIES AND GDPR DATA PROCESSING PRINCIPLES RELATIONSHIP

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%

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].

C. 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].

D. 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 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].

E. 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].

F. 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].

G. 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].

H. 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 Fig.2. 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

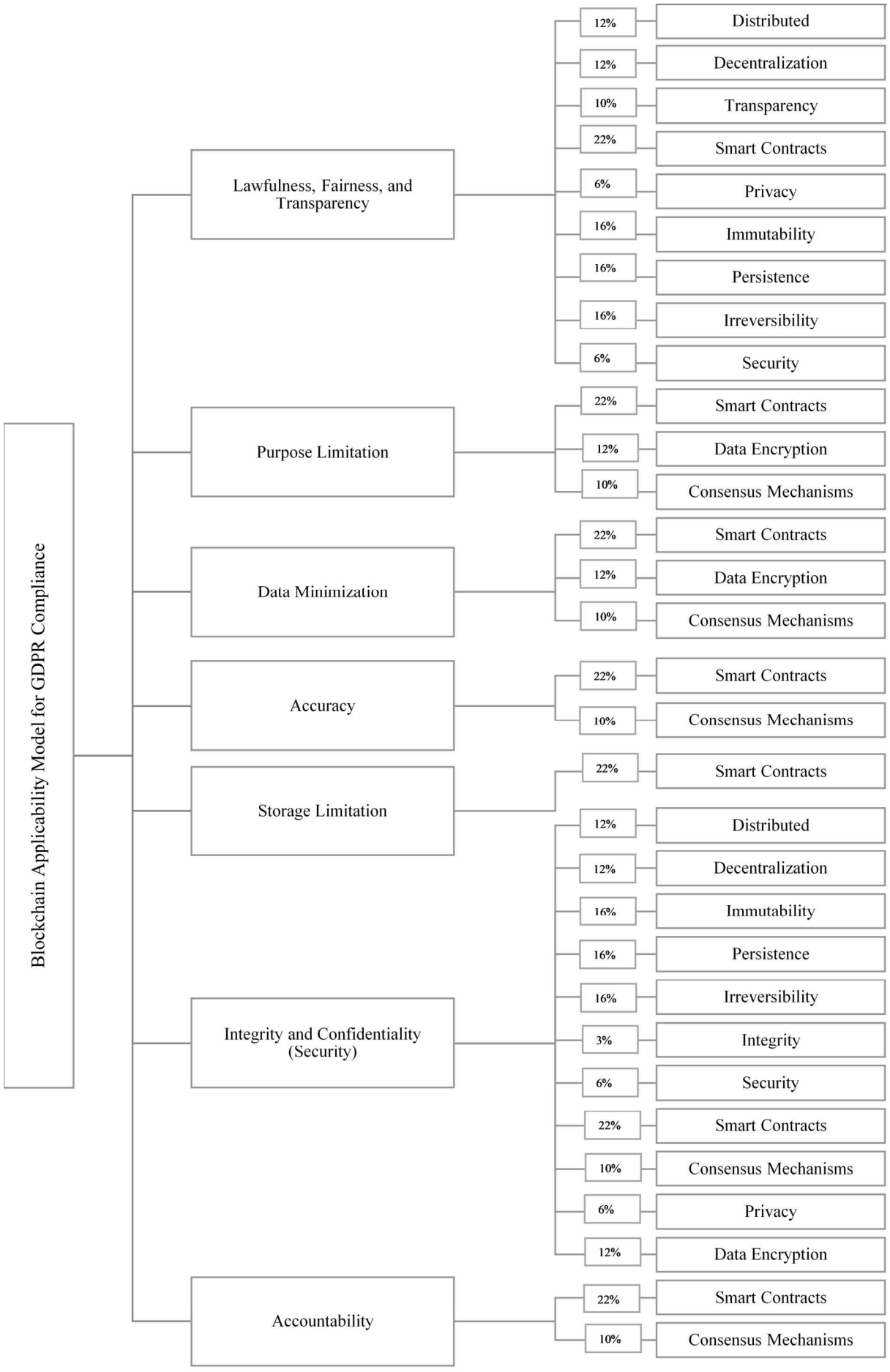

Fig. 2. Blockchain Applicability Model for GDPR Compliance

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.

VI. CONCLUSION

In 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.

REFERENCES

[1] Khushnood Bilal, et al., "Blockchain Technology: Opportunities & Challenges," in 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 2022.

[2] Wajde Baiod, et al., "Blockchain Technology and its Applications Across Multiple Domains: A Survey," Journal of International Technology and Information Management, p. 29, 2021.

[3] Adegboyega Ojo, et al., "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] SEJIN HAN, et al., "A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review," IEEE Open Access Journal, 2022.

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

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

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

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

[9] Unal Tatar, et al., "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 Saadatmand, "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 Arabsorkhi, et al., "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 Schellinger, et al., "Yes, I Do: Marrying Blockchain Applications with GDPR," in Hawaii International Conference on System Sciences, 2022.

[16] Gholamhossein Kazemi, et al., "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] Michèle Finck, "Blockchains and Data Protection in the European Union," EDPL, pp. 17-35, 2018.

[18] Javed Ahmed, et al., "Towards Blockchain-Based GDPR-Compliant Online Social Networks: Challenges, Opportunities and Way Forward," in Future of Information and Communication Conference, 2020.

[19] SMITA BANSOD, et al., "Challenges in making blockchain privacy compliant for the digital world: some measures," Indian Academy of Sciences, 2022.

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

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

[22] Qiheng Zhou, et al., "Solutions to scalability of blockchain: A survey," IEEE, 2020.

[23] Dodo Khan, et al., "Systematic literature review of challenges in blockchain scalability," Applied Sciences, 2021.

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

[25] Gianclaudio Malgieri, et al., "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 Hristov, et al., "The blockchain as a backbone of GDPR compliant frameworks," in 8th International Multidisciplinary Symposium, 2018.

[27] Andriy Kryshtafovych, et al., "Critical Assessment of Methods of Protein Structure Prediction (CASP) – Round XIV," pp. 1607-1617.

[28] Ahmad Haris, et al., "GDPR compliance verification through a user-centric blockchain," Computers and Electrical Engineering, vol. 109, 2023.

[29] Daudén-Esmel, Cristòfol, et al., "Blockchain-based access control system for efficient and GDPR-compliant personal data management," Computer Communications, p. 67–87, 2024.

[30] Suripeddi, Mani Karthik Suhas, et al, "Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing," Journal of Physics: Conference Series, 2021.

[31] Belen-Saglam, Rahime, et al., "A systematic literature review of the tension between the GDPR and public blockchain systems," Blockchain: Research and Applications, 2023.

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

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

[34] Shenglan Ma, et.al, "Nudging Data Privacy Management of Open Banking Based on Blockchain," IEEE, 2018.

[35] AKM Bahalul Haque, et al., "Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport," Applied Science, 2021.

[36] Gabriel Jaccard, et al., "GDPR & Blockchain: the Swiss take," Jusletter IT, 2018.

[37] Nguyen Binh Truong, et al., "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 15, 2020.

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

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

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

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

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

[43] Ruas, Inês Campos, et al., "Blockchain and the GDPR – the shift needed to move forward," 2023.

[44] Gonçalves, Ricardo Martins, et al., "Olympus: a GDPR compliant blockchain system," International Journal of Information Security, 2023.

[45] Mpyana Mwamba Merlec, et al., "A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR," Intelligent Sensors, 2021.

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

[47] Ricardo Neisse, et al., "A Blockchain-based Approach for Data Accountability and Provenance Tracking," in 12th International Conference on Availability, Reliability and Security, 2017.