BLOCKCHAIN USER DATA PRIVACY POLICY

by

NS Muhammad Sibghat Ullah

Supervisor

Col Imran Makhdoom, PhD

A thesis submitted to the faculty of Electrical Engineering Department Military College of Signals, National University of Sciences and Technology, Rawalpindi as part of the requirements for the degree of MS in Electrical Engineering

JUNE 2023

Abstract

The potential for revolutionizing data storage and sharing through blockchain technology is immense. However, the decentralized and permanent nature of blockchains presents a significant challenge to user data privacy. Our research paper aims to tackle this issue head-on by thoroughly examining various blockchain platforms and applications methods of handling user data. We have explored privacy-enhancing technologies and protocols available for blockchain, discussed the trade-offs involved in maintaining user privacy, and analyzed legal and regulatory frameworks such as the GDPR, CCPA, and the Australian Privacy Act that apply to user data privacy in the blockchain context. Our findings have culminated in the establishment of a user data privacy policy for blockchain platforms and applications, outlining best practices for collecting, using, and safeguarding user data on the blockchain. Our policy considers technical, legal, and regulatory considerations to provide a comprehensive and assertive approach to user data privacy in the blockchain ecosystem. Lastly, we have identified further challenges and opportunities for research and provided expert recommendations for enhancing data privacy in blockchain-based systems.

Declaration

I certify that the work *“**Blockchain user data privacy policy**”* exhibited in this thesis has not been submitted in support of any other award or educational qualification either at this institution or elsewhere.

Acknowledgements

All praise and gratitude to Almighty Allah for granting me the blessings and guidance to complete this exploratory work.

I would like to extend my heartfelt appreciation to my supervisor, Col Imran Makhdoom, Ph.D., for his exceptional support throughout my thesis. His guidance, expertise, and constant availability have been invaluable in the successful completion of my MS degree. I am truly grateful for his unwavering assistance.

Furthermore, I would like to express my deepest gratitude to my beloved Parents and wife, for their endless care, love, and unwavering support. Their presence and encouragement during both challenging and exciting times have been a source of strength and motivation.

I am also thankful to my Commanding officer, colleagues, and well-wishers who have provided encouragement, advice, and assistance along the way. Their support has played a significant role in my academic journey.

May Allah reward everyone involved for their contributions, and may this work prove beneficial to the community at large.

Dedication

I dedicate my work to,

My parents who always encouraged my higher education, for their prayers, love and motivation and sacrifices all along.

My supervisors and commanding officer for their support and patience during all the phases of my MS.

Table of Contents

Abstract .... **iii**

Declaration .... **v**

Acknowledgements .... **vi**

Dedication .... **vii**

Table of Contents .... **viii**

List of Figures .... **x**

List of Acronyms .... **xi**

INTRODUCTION **1**

1.1 Research objectives 1

1.2 Significance 2

1.3 Thesis organization 2

BACKGROUND AND CONCEPTUAL FRAMEWORK **4**

2.1 Blockchain Evolution 4

2.2 Blockchain Types 5

2.3 Blockchain Applications 7

THREATS AND SECURITY RISKS IN BLOCKCHAIN **9**

3.1 Threats to Blockchain 9

3.2 Issues in privacy preservation of blockchain 11

3.3 Security risks of blockchain 13

LITERATURE REVIEW **14**

4.1 Data privacy laws and regulations 14

4.2 Previous work 15

4.3 Problem statement 16

THE POLICY **18**

5.1 Introduction 18

5.2. Data collection and use 20

5.3. Data retention 23

5.4. Data Security 23

5.5. Data subject rights 27

5.6. Data controller and processor obligations 42

5.7. Compliance with data privacy laws and regulations 49

5.8. Contact information 54

5.9. Organizations' policies and updates 57

5.10. Effective date and acceptance of the policy 59

CONCLUSION AND FUTURE WORK 64

6.1 Conclusion 64

6.2 Future Work..64

REFERENCES.. 66

List of Figures

Figure 2.1: Public Blockchain 5
Figure 2.2: Private Blockchain 5
Figure 2.3: Consortium Blockchain..6
Figure 2.4: Blockchain Applications 8

List of Acronyms

General Data Protection Regulation	GDPR
California Consumer Privacy Act	CCPA
Health Insurance Portability and Accountability Act	HIPAA
Payment Card Industry Data Security Standard	PCI DSS
Personal Information Protection and Electronic Documents Act	PIPEDA
Protection of Personal Information Act	POPI
Personal Data Protection Law	PDPL
Data Protection Act	DPA
Personal Data Protection Law	PDPL
Internet of Things	IoT
Replicated State Machine Layer	RSML
Data Protection Impact Assessment	DPIA
Data Protection Authority	DPA
Data Protection Officer	DPO
Subject Access Request	SAR
Comma-Separated Values	CSV
Extensible Markup Language	XML
JavaScript Object Notation	JSON

Chapter 1

INTRODUCTION

Blockchain technology can potentially revolutionize data storage and sharing [1]. However, the decentralized nature of blockchains and the fact that data is often stored permanently and immutable raise concerns about user data privacy. In this research paper, we explore the issue of user data privacy in the context of blockchain technology. With a particular focus on how different blockchain platforms and applications handle user data, we review the current state of the art regarding privacy-enhancing technologies and protocols for blockchain and discuss the challenges and trade-offs involved in preserving user privacy. We also examine the various legal and regulatory frameworks that apply to user data privacy in the blockchain context, such as the EU General Data Protection Regulation (GDPR) [2], the California Consumer Privacy Act (CCPA) [3], and the Australian Privacy Act [4], and consider the implications of these frameworks for blockchain-based applications. Based on our analysis, we define a user data privacy policy for blockchain platforms and applications, outlining best practices for collecting, using, and protecting user data on the blockchain. Our policy aims to provide a comprehensive approach to user data privacy in the blockchain ecosystem, addressing technical, legal, and regulatory considerations. Finally, we have discussed the challenges and opportunities for further research and provided recommendations for improving data privacy in blockchain-based systems.

1.1 Research objectives

The objectives of a data privacy policy for blockchain technology include the following:

1.1.1. Protecting personal data: Ensuring that personal data is handled responsibly and ethically and protects it from unauthorized access or misuse.

1.1.2. Complying with data privacy regulations: Ensuring that the organization complies with relevant data privacy regulations, such as the GDPR in the European Union and CCPA in the USA.

1.1.3. Building trust with users: Ensuring that users know how their personal data is being used and building trust with them through transparent and responsible data handling practices.

1.1.4. Mitigating the risk of data breaches: Reducing the risk of data breaches and unauthorized access to personal data.

1.1.5. Maintaining the organization's reputation: Protecting the organization's reputation by demonstrating a commitment to responsible data handling practices.

1.1.6. Promoting the ethical use of personal data: Ensuring that personal data is used in a way that respects the rights and privacy of individuals.

1.2 Significance

The study will:

1.2.1. Provide valuable insights into the challenges and opportunities of implementing user data privacy policies on blockchain platforms.

1.2.2. Provide a foundation for further research and development of best practices in blockchain user data privacy policies.

1.2.3. Contribute to the development of effective blockchain user data privacy policies that can protect user data and enhance user trust/ engagement.

1.2.4. Help to address the growing concerns about user data privacy in the context of blockchain technology.

1.3 Thesis organization

The thesis is organized into six chapters:

1.3.1. Chapter 1 serves as the introduction, providing an overview of the research topic. It includes an introduction to the subject matter, presents the research objectives and questions that will be addressed, discusses the significance and motivation behind the study, and outlines the overall structure of the thesis.

1.3.2. Chapter 2 focuses on the background and conceptual framework of blockchain. It explores the evolution of blockchain technology, different types of blockchains, and their applications in various industries.

1.3.3. Chapter 3 delves into the threats and security risks associated with blockchain. It examines the potential vulnerabilities and risks that blockchain systems may face, including threats to blockchain transactions' integrity, privacy, and security.

1.3.4. Chapter 4 presents a comprehensive literature review covering the relevant data privacy laws and regulations that impact blockchain technology. It also includes an analysis of previous work done in the field, highlighting critical studies and research findings.

1.3.5. Chapter 5 is dedicated to the policy aspect of the thesis. It discusses the specific policy considerations and frameworks related to blockchain technology, addressing governance, compliance, and regulatory challenges.

1.3.6. Chapter 6 focuses on future directions and provides a conclusion to the thesis. It outlines potential future work and research directions that can build upon the current study's findings. The chapter concludes by summarizing the main findings and contributions of the research.

Following this organizational structure, the thesis aims to comprehensively understand blockchain technology, its associated threats and security risks, relevant data privacy laws and regulations, and the policy landscape. It also highlights potential future avenues for research and concludes with a summary of the overall study.

Chapter 2

BACKGROUND AND CONCEPTUAL FRAMEWORK

This chapter provides a comprehensive background and conceptual framework for understanding blockchain technology. It explores the evolution of blockchain, the different types of blockchain architectures, and the wide-ranging applications of blockchain across various industries. By delving into these foundational aspects, this chapter sets the stage for a deeper exploration of the threats, security risks, and privacy preservation challenges associated with blockchain technology in subsequent chapters.

2.1 Blockchain Evolution

Blockchain technology has evolved significantly since it was first introduced in 2008 with the launch of the Bitcoin network. Some key developments in the evolution of blockchain technology include:

2.1.1. "Blockchain 1.0" generally refers to systems that aim to facilitate peer-to-peer transactions while utilizing cryptographic methods to guarantee data security and integrity. [5]. One of the most renowned instances of Blockchain 1.0 is the Bitcoin network, which facilitates direct transactions between peers without the need for a central authority.

2.1.2. "Blockchain 2.0" generally refers to the second generation of blockchain technology, which builds upon the foundations of Blockchain 1.0 by adding additional functionality and capabilities [6]. This platform has the ability to store and execute self-executing smart contracts written in code. The Ethereum network is a popular instance of Blockchain 2.0 technology.

2.1.3. "Blockchain 3.0" generally refers to the third generation of blockchain technology, which builds upon the foundations of Blockchain 2.0 by adding additional capabilities and improvements [7]. This includes providing significant support for more complex apps and using advanced cryptographic techniques to improve security and privacy.

2.1.4. "Blockchain 4.0" generally pertains to the fourth generation of blockchain technology that is currently in its early development phase. [8]. Blockchain 4.0 is expected to build upon the foundations of previous generations of blockchain technology by adding additional capabilities and improvements, such as increased scalability, faster transaction speeds, and enhanced privacy and security features.

2.2 Blockchain Types

There are several versions of blockchain technology [9] [10], including:

2.2.1. Public blockchains: Decentralized networks provide a safe and assured platform for individuals to participate confidently and contribute actively. Examples include Bitcoin and Ethereum [11].

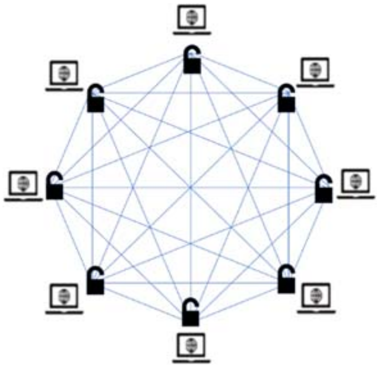


Figure 2.1: Public Blockchain

2.2.2. Private blockchains: Decentralized networks are exclusively accessible to authorized participants [12] [13]. Private blockchains are often used in enterprise settings where organizations want to share and process data securely and transparently but still want to keep the data confidential.

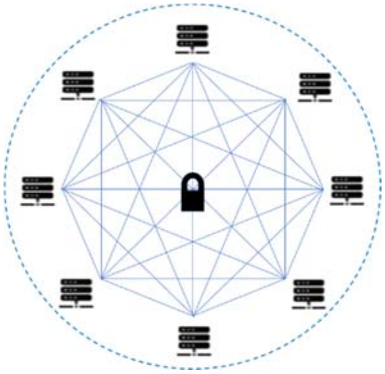


Figure 2.2: Private Blockchain

2.2.3. Consortium blockchains: These are decentralized networks that are partially open and partially closed [14] [15]. Consortium blockchains are often used in situations where a group of organizations wants to collaborate but needs to trust one another fully [16].

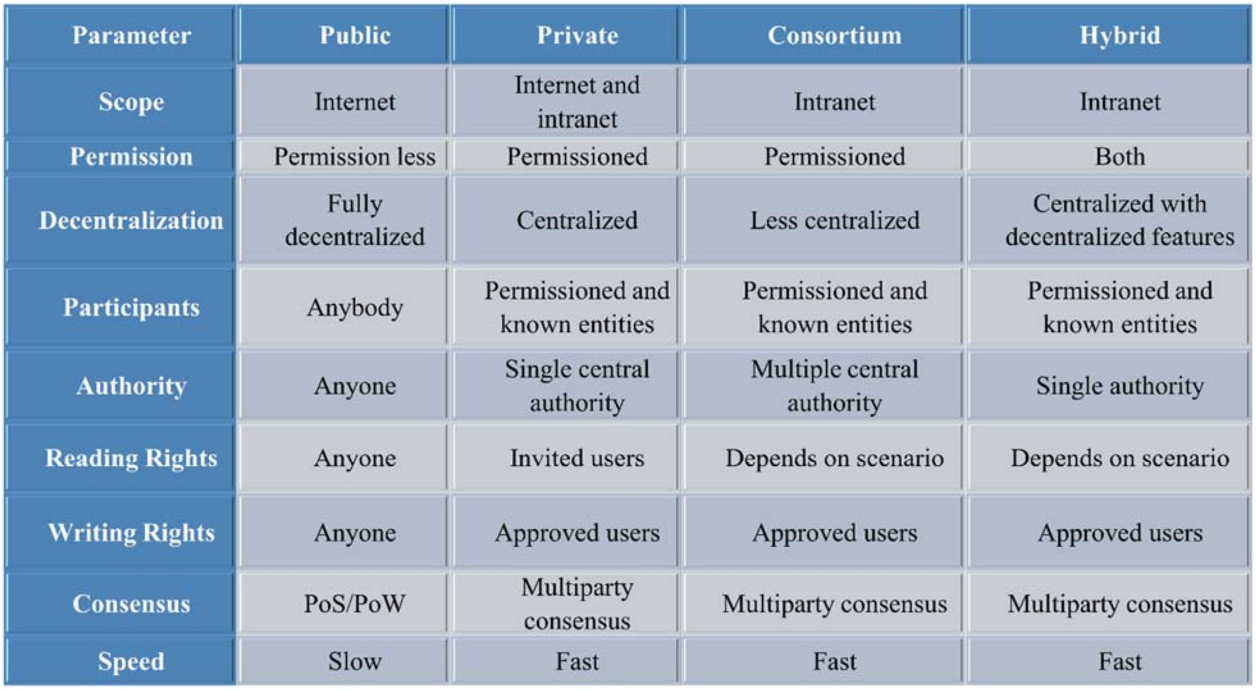
Figure 2.3: Consortium Blockchain

2.2.4. Hybrid blockchains: The seamless integration of elements from public and private blockchains is a hallmark of these networks [17] [18]. Hybrid blockchains are commonly utilized by organizations that wish to share information with the public while still retaining some degree of control over who can access it.

2.2.5. Sidechains: There are separate blockchains linked to the main one for exchanging assets or information [19] [20].

2.2.6. Layer 2 solutions: These protocols operate on top of the main blockchain, enabling increased scalability and faster transaction processing times [21]. Examples include the Lightning Network for Bitcoin and Ethereum's Plasma.

It is important to note that these types of blockchain technology are only a few among the many available. The specific type of blockchain that is most appropriate for a given application will depend on the needs and constraints of that application.



Parameter	Public	Private	Consortium	Hybrid
Scope	Internet	Internet and intranet	Intranet	Intranet
Permission	Permission less	Permissioned	Permissioned	Both
Decentralization	Fully decentralized	Centralized	Less centralized	Centralized with decentralized features
Participants	Anybody	Permissioned and known entities	Permissioned and known entities	Permissioned and known entities
Authority	Anyone	Single central authority	Multiple central authority	Single authority
Reading Rights	Anyone	Invited users	Depends on scenario	Depends on scenario
Writing Rights	Anyone	Approved users	Approved users	Approved users
Consensus	PoS/PoW	Multiparty consensus	Multiparty consensus	Multiparty consensus
Speed	Slow	Fast	Fast	Fast

Table 2.1: Comparison of blockchain

2.3 Blockchain Applications

Blockchain technology can revolutionize various industries and applications [22] [23]. There are various potential applications for blockchain technology, such as:

2.3.1. Financial services: Blockchain technology has the potential to enable secure, transparent, and unchangeable financial transactions, such as moving funds, finalizing trades, and managing the issuance and monitoring of financial instruments.

2.3.2. Supply chain management: With the use of blockchain technology, it's possible to keep track of the movement of goods and materials along the supply chain. This allows for efficient and transparent tracking of products, from their initial raw materials stage all the way to the end-consumer.

2.3.3. Identity and access management: Blockchain technology can create secure and decentralized systems for verifying and managing identity and access, enabling more secure and efficient authentication and authorization processes.

2.3.4. Healthcare: The use of blockchain technology can ensure the secure storage and management of healthcare records and other sensitive medical data. This facilitates more efficient and secure sharing of information among healthcare providers.

2.3.5. Government and public sector: Blockchain technology can be used to improve transparency, efficiency, and accountability in government and public sector operations, including the management of public records, voting systems, and the distribution of benefits and services.

2.3.6. Internet of Things (IoT): Blockchain can secure and regulate data from interconnected devices, enabling safer and more efficient communication.

Here are some instances that showcase the potential uses of blockchain technology [24]. As technology continues to mature and evolve, new and innovative uses for blockchain will likely emerge.

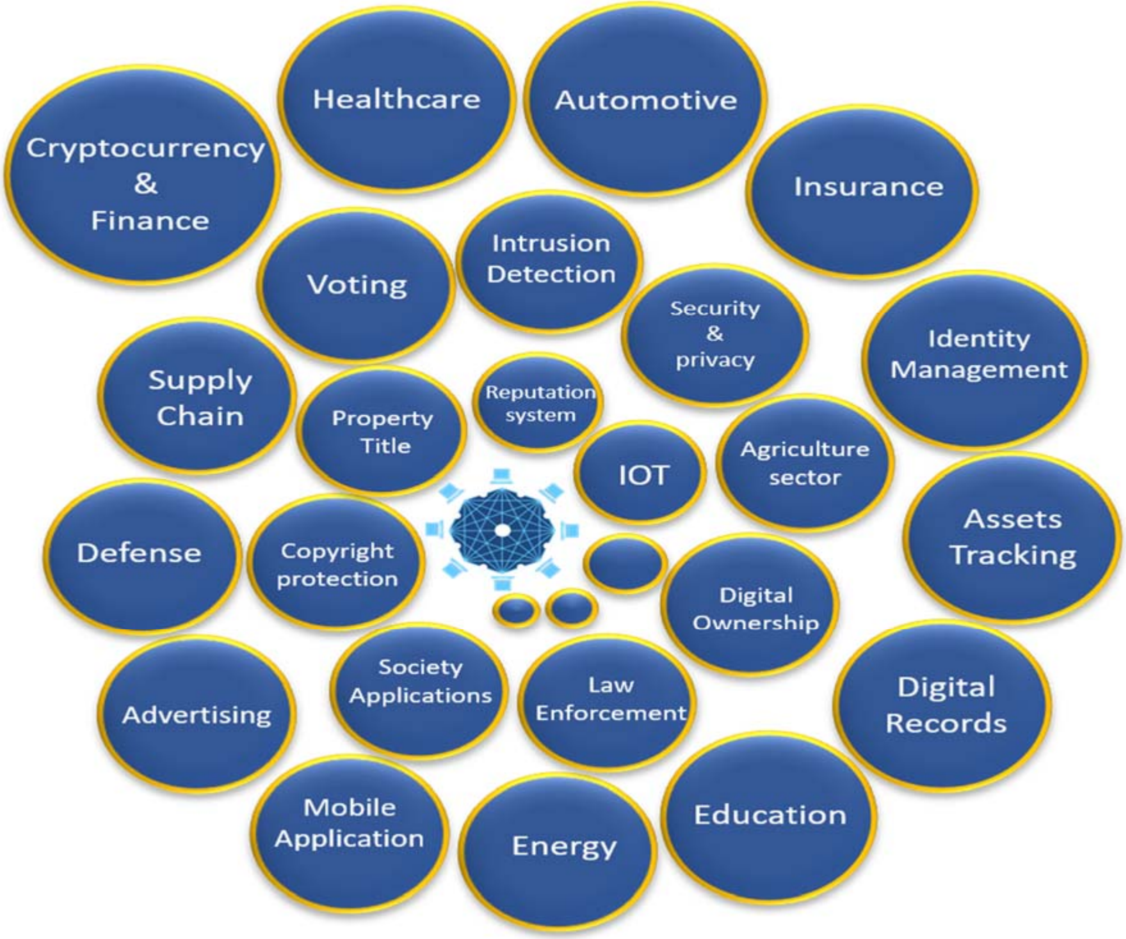


Figure 2.4: Blockchain Applications

Chapter 3

THREATS AND SECURITY RISKS IN BLOCKCHAIN

This chapter explores the various threats and security risks associated with blockchain technology. As blockchain systems gain prominence and are adopted in different sectors, it becomes crucial to understand the potential vulnerabilities and risks that can compromise the integrity, confidentiality, and availability of blockchain networks. By examining the threats to blockchain, the issues related to privacy preservation, and the security risks inherent in blockchain technology, this chapter aims to provide a comprehensive overview of the challenges that need to be addressed to ensure the secure and trustworthy operation of blockchain systems.

3.1 Threats to Blockchain

A blockchain is a type of ledger made up of interconnected data blocks that are distributed and decentralized. In a blockchain, each block consists of transactions and is linked to the previous block using a cryptographic hash function. The blocks are stored across numerous computers or nodes within the network, with cryptographic techniques used to secure the data contained within them. There are several layers in a blockchain, each with its own vulnerabilities and potential attack surfaces [25] [26]:

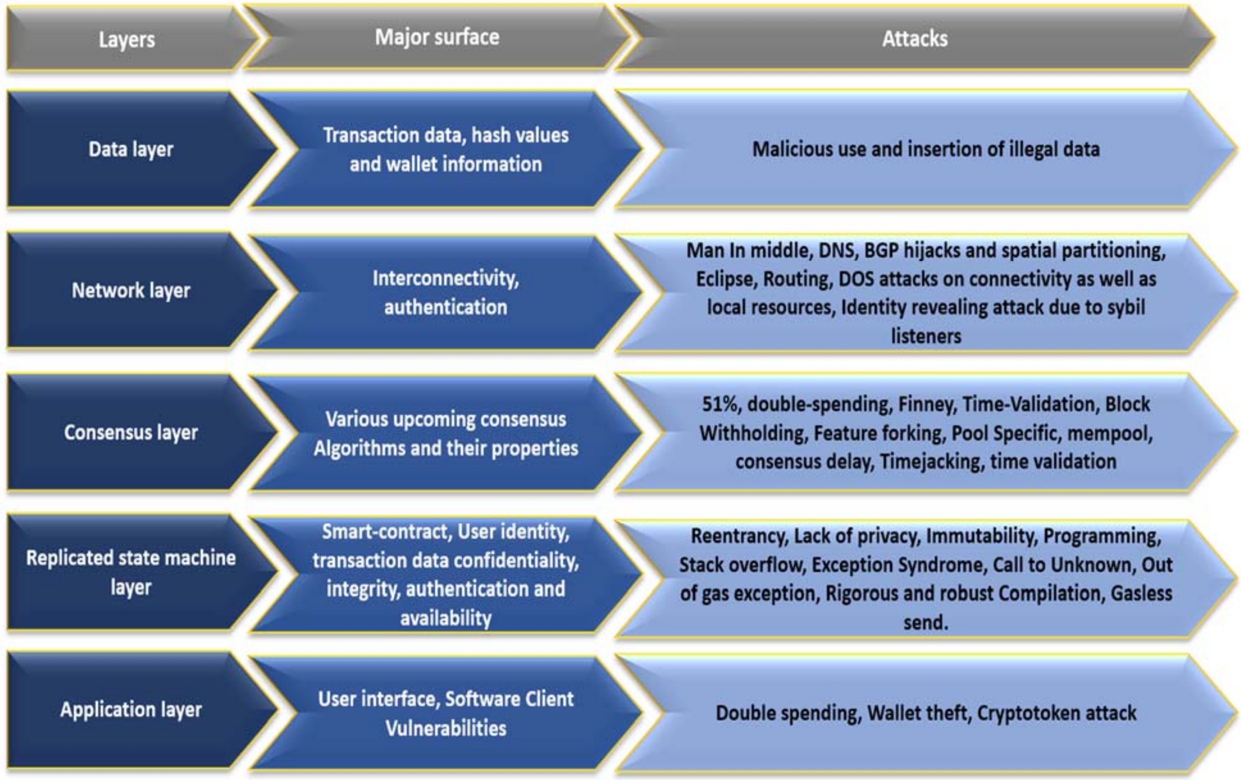
3.1.1. Data layer: This is where the actual data is stored. This data is typically organized into blocks and linked together through cryptographic hash functions in a blockchain. Vulnerabilities at this layer include a lack of anonymity, weak or stolen private keys, or vulnerabilities in smart contracts.

3.1.2. Network layer: This is where the blockchain is implemented and maintained. The network layer consists of the computers or nodes that make up the network and the software that allows them to communicate and validate transactions. Vulnerabilities at this layer include hacking, malware, insider threats, or phishing attacks.

3.1.3. Consensus layer: The purpose of this layer is to ensure that regulations are followed when adding new transactions to the blockchain. Vulnerabilities at this layer include flaws in the consensus algorithm or attacks on the network that aim to compromise the integrity of the data.

3.1.4. The replicated state machine layer: The Replicated State Machine Layer (RSML) is a crucial element in various blockchain systems. It ensures the distributed ledger's consistency and integrity, making it an essential component. RSML is a critical target for attackers who seek to compromise the security and reliability of the blockchain.

3.1.5. Application layer: Applications can be built on top of the blockchain, utilizing the underlying platform's data and functionality. Vulnerabilities at this layer include vulnerabilities in the applications themselves or in the interface between the applications and the blockchain.



Layers	Major surface	Attacks
Data layer	Transaction data, hash values and wallet information	Malicious use and insertion of illegal data
Network layer	Interconnectivity, authentication	Man In middle, DNS, BGP hijacks and spatial partitioning, Eclipse, Routing, DOS attacks on connectivity as well as local resources, Identity revealing attack due to sybil listeners
Consensus layer	Various upcoming consensus Algorithms and their properties	51%, double-spending, Finney, Time-Validation, Block Withholding, Feature forking, Pool Specific, mempool, consensus delay, Timejacking, time validation
Replicated state machine layer	Smart-contract, User identity, transaction data confidentiality, integrity, authentication and availability	Reentrancy, Lack of privacy, Immutability, Programming, Stack overflow, Exception Syndrome, Call to Unknown, Out of gas exception, Rigorous and robust Compilation, Gasless send.
Application layer	User interface, Software Client Vulnerabilities	Double spending, Wallet theft, Cryptotoken attack

Figure 3.1: Blockchain Attacks

It is important to mention that these layers are not always entirely separate, and there may be some overlap among them. Other layers or attack surfaces may also be specific to a blockchain implementation. To address potential weaknesses and malicious actions towards a blockchain, it is crucial to establish strong security protocols, including robust encryption, controlled access, and routine security assessments. It is also essential to educate users about the importance of protecting their data and the risks of sharing sensitive information with unauthorized parties.

3.2 Issues in privacy preservation of blockchain

Several issues can potentially compromise the privacy of data stored on a blockchain [27] [28]:

3.2.1. Lack of anonymity: Many blockchain networks, such as Bitcoin and Ethereum, do not offer strong anonymity protections for users, which means it may be possible to trace the actions and transactions of specific users on the network. This can risk users' privacy, especially if sensitive personal or financial data is involved.

3.2.2. Weak or stolen private keys: Private keys are an absolute requirement for accessing and managing data on a blockchain network. Their loss, theft or compromise poses a grave threat to the privacy of the data stored on the network.

3.2.3. Vulnerabilities in smart contracts: Smart contracts can have flaws that compromise agreement terms by allowing unauthorized access or data manipulation.

3.2.4. Lack of regulatory oversight: The protection of data privacy on blockchain networks is facing mounting challenges. The only viable solution is to establish more laws and regulations that are exclusively focused on safeguarding the privacy of data on these networks.

3.2.5. Data breaches: Blockchain networks can be vulnerable to data breaches, leading to unauthorized access or disclosure of sensitive data.

3.2.6. Data mining: Some parties may attempt to mine data from blockchain networks to gather information about users or transactions. This could lead to the unauthorized collection and analysis of sensitive personal data.

3.2.7. Public networks: Maintaining privacy for sensitive data on public blockchain networks is highly challenging due to their openness to anyone who wishes to view the stored information, including unauthorized parties.

3.2.8. Lack of privacy features: Many blockchain networks need to offer built-in privacy features, which make it difficult to protect the privacy of data stored on these networks.

3.2.9. Data retention: Some blockchain networks do not have mechanisms to delete or erase data, meaning that data stored on these networks may be retained indefinitely. This can pose a risk to data privacy, mainly if it is sensitive or personal.

3.2.10. Centralization: Some blockchain networks are centralized, meaning a single entity or group controls them. This can make it easier for these entities to access and control the data stored on the network, which can risk users' privacy.

3.2.11. Data aggregation: There is a real risk of unauthorized data gathering and examination of sensitive personal information when parties attempt to combine data from multiple sources to obtain a more complete understanding of users or transactions. This must be avoided at all costs.

3.2.12. Data interoperability: Some blockchain networks are not designed to be interoperable with other networks, making it difficult to share data between networks and potentially leading to the duplication or fragmentation of data. This can pose a risk to data privacy, as it may be more vulnerable to unauthorized access or disclosure.

3.2.13. Data governance: Some blockchain networks need clear rules or policies to manage data, making it challenging to ensure data privacy stored on these networks.

3.2.14. Data provenance: It can be challenging to determine the provenance, or origin, of data on a blockchain network, making it harder to ensure the privacy and integrity of that data.

3.2.15. Data privacy regulations: Some countries have strict data privacy regulations that may not be compatible with blockchain technology. This can challenge organizations that want to use blockchain networks to store or process personal data.

3.2.16. Interoperability with legacy systems: Some legacy systems may need to be compatible with blockchain technology, making it challenging to integrate blockchain networks with these systems and potentially leading to the duplication or fragmentation of data. This can pose a risk to data privacy, as it may be more vulnerable to unauthorized access or disclosure.

3.2.17. Data complexity: Privacy on a blockchain network is a major challenge due to the intricate nature of the stored data. Extra measures must be taken to safeguard sensitive or well-organized information and ensure absolute privacy.

3.2.18. Quantum computing: The potential threat that quantum computers could pose to the security of blockchain networks cannot be ignored. Although the impact on data privacy remains uncertain, it is crucial to acknowledge the potential risk and take proactive measures to mitigate it. However, it is also important to consider that as quantum computers continue to develop, they may also present an opportunity to enhance the security of blockchain technology.

To protect data privacy on a blockchain, use strong security protocols and encryption, limit access, and conduct regular security checks. Seek legal guidance to comply with legal requirements. Be cautious when sharing sensitive information on blockchain networks.

3.3 Security risks of blockchain

Following is a summarized table representing the security risks of blockchain [29] [30] [31] [32]:

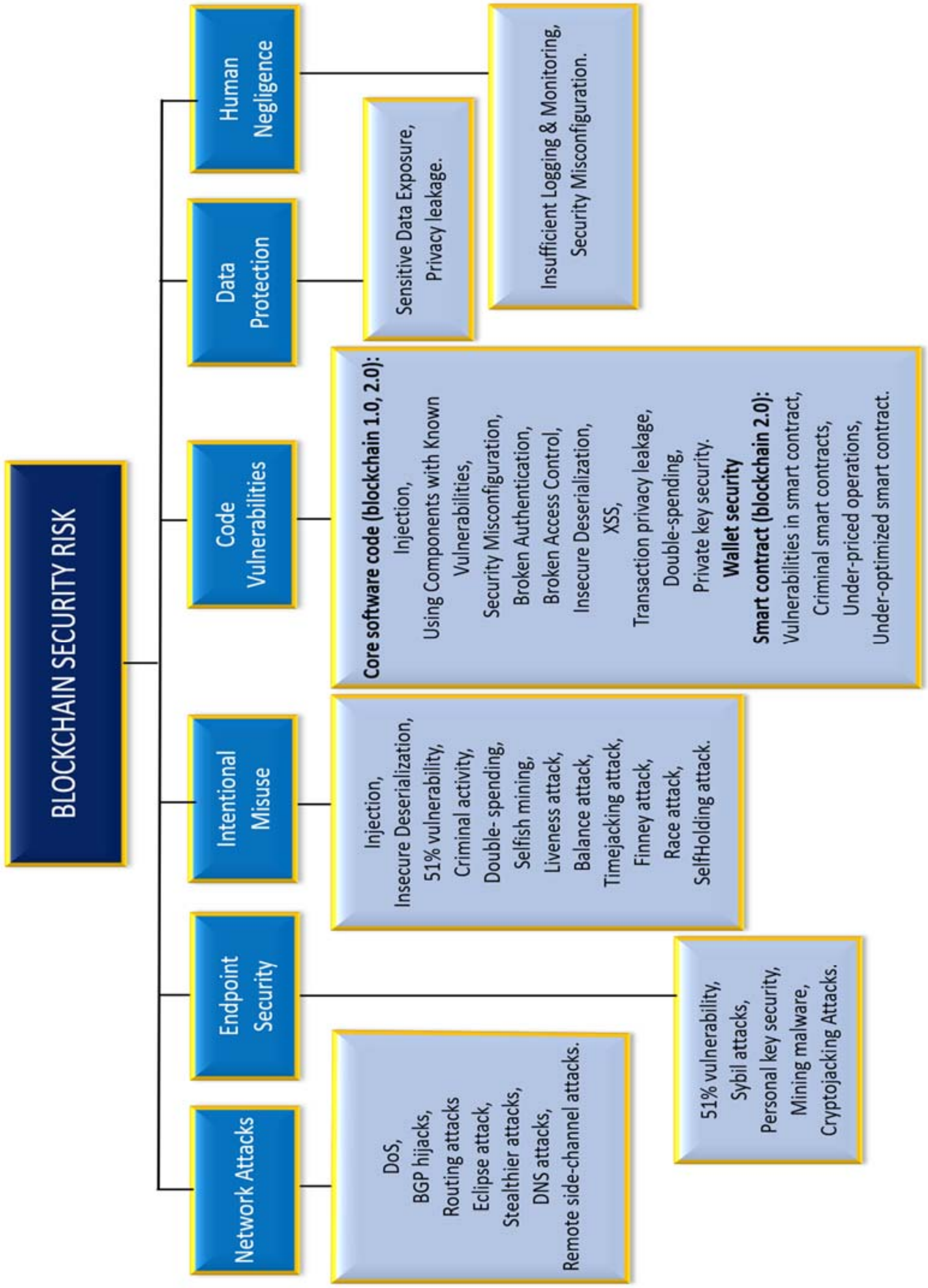


Figure 3.2: Blockchain Security Risks

Chapter 4

LITERATURE REVIEW

This chapter presents a comprehensive literature review focusing on data privacy laws and regulations, previous work conducted in the field, and the problem statement addressed in the thesis. Data privacy laws and regulations play a critical role in shaping the legal and ethical landscape surrounding the protection of personal information within the context of blockchain technology. By examining these laws and regulations, we gain insights into the regulatory frameworks and compliance requirements that impact the design and implementation of privacy policies in blockchain systems. Additionally, this chapter reviews the existing body of work and research related to data privacy in blockchain, identifying key findings, methodologies, and gaps in knowledge. Finally, the chapter concludes by articulating the problem statement that the thesis aims to address, setting the stage for the subsequent chapters where proposed solutions and analysis will be presented.

4.1 Data privacy laws and regulations

Here is a list of 10 data privacy laws and regulations that are widely considered to be significant and influential:

- General Data Protection Regulation (GDPR) [2]
- California Consumer Privacy Act (CCPA) [33]
- Health Insurance Portability and Accountability Act (HIPAA) [34]
- Payment Card Industry Data Security Standard (PCI DSS) [35]
- Personal Information Protection and Electronic Documents Act (PIPEDA) [36]
- Protection of Personal Information Act (POPI) [37]
- UAE Data protection law [38]
- Personal Data Protection Law (PDPL) [39]
- Data Protection Act (DPA) [40]
- Personal Data Protection Law (PDPL) [41]

Several common points are found across many data privacy laws and regulations regarding user data privacy. These common points include:

4.1.1. Collection and usage of personal data: Many data privacy laws and regulations set out rules for collecting and using personal data [42], including obtaining explicit consent from individuals before collecting or using their personal data and specifying the purposes for which personal data can be collected and used.

4.1.2. Data security: Organizations are obligated by privacy laws and regulations to take necessary technical and organizational measures to safeguard personal data against unauthorized access, disclosure, or destruction.

4.1.3. Data retention: Many data privacy laws and regulations set out rules for the retention of personal data, including requirements for the length of time that personal data must be kept and the conditions under which it must be deleted or destroyed.

4.1.4. Data subject rights: Various data privacy laws and regulations grant individuals specific rights concerning their personal data. These rights must be respected and include the ability to access, rectify, erase, or restrict the processing of their personal data.

4.1.5. Data breaches: It is mandatory for organizations to ensure that individuals and regulatory authorities are informed about any data breaches that may impact their personal data, in accordance with multiple privacy laws and regulations.

4.1.6. Data controller and processor obligations: Many data privacy laws and regulations set out specific responsibilities for organizations that control or process personal data, including contract requirements and other legal instruments between data controllers and data processors.

4.1.7. Penalties and sanctions: Many data privacy laws and regulations provide penalties and sanctions for organizations that violate data privacy rules, including fines, criminal penalties, and other enforcement measures.

4.2 Previous work

Developing a comprehensive blockchain user data privacy policy has been a significant research and development focus in recent years. The rise in utilization of blockchain technology necessitates heightened measures to secure user data from any unauthorized breach or tampering. One of the main areas of focus in this field has been the development of privacy-focused regulations and standards, such as the European Union's General Data Protection Regulation (GDPR) [2]. The GDPR sets out specific requirements for protecting personal data, including the right to erasure, data portability, and privacy by design. Other regulations and standards, such as the California Consumer Privacy Act (CCPA) [3], aim to enhance privacy by giving individuals greater control over their personal data.

Technical solutions, such as encryption techniques and privacy coins, have also been proposed to enhance privacy in the blockchain ecosystem. Encryption techniques, such as homomorphic encryption [43] [44], zero-knowledge proofs, and multiparty computation [45] [46], allow user data to be encrypted and kept secure while preserving the integrity and reliability of the underlying blockchain [47]. Privacy coins like Monero and Zcash use cryptographic methods to hide transaction details and users' identities.

Another approach to enhance privacy in the blockchain ecosystem is by using decentralized identity solutions. Decentralized identity solutions, such as Self-Sovereign Identity (SSI) [48], allow users to manage their own digital identities and data, giving them greater control over their personal information [49]. This approach also enhances privacy and security by eliminating the need for a centralized party to manage and store user data.

Privacy-focused blockchain platforms, such as Enigma [37] and Ocean Protocol [38], have also been developed to provide secure and decentralized data privacy and management solutions. These platforms allow individuals and organizations to control and monetize their data while preserving privacy and security.

Governance solutions, such as ring signatures [50] [51]and stealth addresses [52], have also been proposed to enhance privacy in the blockchain ecosystem. Ring signatures allow a group of users to have public keys. A sender can use any key from this group to create a signature on a transaction without revealing their identity. Stealth addresses [53] enable the recipient of a transaction to be the only one who can see the details of the transaction, such as the amount and the sender's identity.

4.3 Problem statement

Blockchain technology has the power to revolutionize the storage and exchange of data. However, it presents significant challenges when it comes to protecting user privacy. As more organizations adopt blockchain technology, there is a growing need for clear and effective policies to protect user data privacy on these networks.

However, blockchain technology's complex and decentralized nature can make implementing effective user data privacy policies challenging. In addition, there needs to be clear guidance on ensuring compliance with top data privacy regulations and laws, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

As a result, there is a need for a comprehensive and effective blockchain user data privacy policy that addresses the unique challenges of this technology and ensures compliance with relevant data privacy regulations and laws. This policy should provide clear guidance on the collection, use, storage, and protection of user data on blockchain networks and the rights and responsibilities of data controllers and data processors.

Chapter 5

THE POLICY

This chapter presents a comprehensive policy framework for ensuring data privacy within blockchain technology. The policy encompasses key components such as principles, objectives, and scope, and addresses the challenges of implementation and enforcement. The chapter aims to provide practical guidance to organizations in establishing effective privacy guidelines and practices within blockchain systems.

5.1 Introduction

5.1.1. Purpose

This blockchain user data privacy policy aims to establish the rules and guidelines for collecting, using, and storing personal data on our blockchain network [54]. This policy delineates the kinds of personal information that might be gathered, the objectives for which personal data might be collected and utilized, and the precautions that ought to be taken to safeguard personal data against unauthorized access, disclosure, or destruction [55]. This policy also details the rights of individuals pertaining to their personal data, such as the right to access, correct, delete, or restrict the processing of their information. Additionally, this policy specifies the obligations of organizations and any third parties that work with them in relation to personal data, including requirements for contracts and other legal instruments between data controllers and data processors. Finally, this policy outlines the steps that should be taken to ensure compliance with relevant data privacy laws and regulations, including any penalties or sanctions for non-compliance.

5.1.2. Scope

The scope of the policy is to establish clear guidelines and procedures for protecting user data privacy in the blockchain ecosystem. The policy aims to ensure that all user data is collected, stored, and used in compliance with legal and regulatory requirements and that effective security protocols and procedures are in place to safeguard against potential data breaches or unauthorized access. The policy will also provide transparent and accessible information to users about how their data is being collected, stored, and used, and establish clear consequences for non-compliance. The policy aims to promote trust, transparency, and accountability among all stakeholders in protecting user data privacy in the blockchain ecosystem.

5.1.3. Definitions of critical terms

a. **Personal data:** It pertains to any information linked to a recognizable or identifiable individual. This can encompass, among other things, names, addresses, email addresses, phone numbers, and other identifying particulars.

b. **Blockchain network:** Blockchain network refers to distributed ledger technology storing, transmitting, and processing data.

c. **Data controller:** The individual or organization in charge of deciding how personal data is managed, including the goals and methods utilized, is known as a data controller.

d. **Data processor:** An entity that handles personal information for a data controller is referred to as a data processor.

e. **Data subject:** A data subject refers to a person whose personal data is collected, utilized, or retained.

f. **Consent:** Consent means agreeing to have personal data processed, with full awareness of the details.

g. **Data retention:** Data retention refers to the specific duration that personal data is stored, as well as the exact circumstances under which it is erased or disposed of.

h. **Data protection impact assessment (DPIA):** A DPIA is a procedure that organizations undertake to recognize and evaluate potential threats to the privacy of personal data.

i. **Data breach:** A data breach is a serious violation of privacy, commonly referred to as unauthorized access, use, disclosure, or destruction of personal data.

j. **Data portability:** An individual has the right to obtain their personal information in a format that is easily readable by machines and commonly used, and to transfer it to another entity responsible for managing data.

k. **Technical and organizational measures:** Personal data is protected from unauthorized access, disclosure, or destruction through the implementation of both technical and organizational measures by organizations.

l. **Data subject rights:** Data subject rights are the entitlements of individuals in connection with their personal data. These rights include accessing, correcting, deleting, or limiting the handling of their personal data.

m. Penalties and sanctions: Penalties and sanctions refer to the consequences that organizations may face for violating data privacy laws and regulations, including fines, criminal penalties, and other enforcement measures.

n. Data protection authority (DPA): A DPA is a regulatory body that enforces data privacy laws and regulations.

o. Data protection officer (DPO): In an organization, a DPO holds the responsibility of ensuring compliance with data privacy laws and regulations.

p. Personal data processing: Processing personal data encompasses a range of activities, such as collecting, utilizing, storing, and deleting said data.

q. Privacy by design: Incorporating privacy considerations into the initial design and development of products, services, and systems is known as privacy by design.

r. Privacy by default: Privacy by default refers to setting privacy controls to the highest level so that individuals do not have to take additional steps to protect their personal data.

s. Sensitive personal data: Personal data that falls under the category of sensitive information is granted special protection under data privacy laws and regulations. This includes details about a person's race or ethnicity, political views, religious or philosophical beliefs, membership in a trade union, health condition, or sexual orientation.

t. Third-party: An entity that processes personal data on behalf of a data controller or processor but is not themselves a controller or processor is known as a third-party organization.

5.2. Data collection and use

5.2.1. Types of personal data collected

Types of personal data that may be collected in a blockchain should depend on the specific purposes for which the data is being collected and the nature of the services provided on the blockchain network [56]. Here is a list of the various kinds of personal information that may be gathered through a blockchain application:

a. Contact information: This includes names, addresses, email addresses, and telephone numbers.

b. Identifying information: This covers identification numbers issued by the government, such as passport and driver's license numbers.

c. **Profile information:** This includes job titles, professional affiliations, and other information individuals provide about themselves in their profiles.

d. **Communication data:** This includes the content of emails, messages, and other communications sent through the blockchain network.

e. **Location data:** This includes information about the location of individuals when they use the blockchain network.

f. **Demographic data:** This includes information about an individual's age, gender, race, or ethnicity.

g. **Behavioral data:** This includes information about an individual's habits, preferences, and interests.

h. **Personal data obtained with the individual's consent:** It is essential to get the consent of individuals before collecting and storing their personal data on the blockchain [57] [58]. By obtaining the individual's consent, organizations or companies should collect and store personal data responsibly [59].

i. **Personal data that has been encrypted:** Encrypt personal data before it is stored on the blockchain to protect the privacy of individuals. This makes it more difficult for unauthorized parties to access or view the data.

Types of personal data that should not be collected in a blockchain include:

a. **Sensitive personal data:** The information comprises financial records, medical data, and social security details [56]. These types of data are considered particularly sensitive and should be handled with care to protect the privacy of individuals.

b. **Personal data that is not necessary to provide a service:** Organizations and companies should restrict the gathering and retention of personal data to the minimum required for the provision of their services [60]. It is imperative to refrain from collecting and storing personal data that is not essential in order to mitigate the risk of privacy breaches.

c. **Personal data of children:** It is generally not appropriate to collect and store the personal data of children on the blockchain [61]. Children may not have the same level of understanding of privacy issues and may be more vulnerable to privacy breaches.

d. **Data collected without consent.:** Organizations and companies must always obtain the consent of individuals prior to collecting and storing their personal data on the blockchain [62]

[57]. Collecting and storing personal data without the individual's consent violates their privacy rights.

e. **Personal data obtained through deceptive or misleading means:** Organizations or companies should be transparent about the personal data they collect and should not use deceptive or misleading means to obtain personal data [59].

5.2.2. Purpose of collecting personal data

The purpose of collecting personal data in a blockchain application depends on the specific services provided by the application and the needs of the organization operating the application [63] [64]. Some everyday purposes for collecting personal data in a blockchain application include the following:

a. **To facilitate transactions:** Personal data can be collected to verify individuals' identities and facilitate transactions on the blockchain [65].

b. **To provide customer support:** Personal data can be collected to communicate with individuals and support them, such as answering questions or resolving issues.

c. **To enhance the user experience:** Personal data can be collected to understand users' preferences and needs and to improve the user experience by providing personalized services or recommendations.

d. **To comply with legal obligations:** Personal data can be collected to comply with legal obligations, such as anti-money laundering regulations or know-your-customer requirements.

e. **To analyze and improve the blockchain application:** Personal data can be collected to analyze the usage of the blockchain application and identify opportunities for improvement, but it should be with consent.

5.2.3. Obtaining consent for data collection

Obtaining consent for data collection is an essential aspect of data privacy and is often required by data privacy laws and regulations [58] [66] [59]. To obtain consent for data collection in a blockchain application, the following steps should be taken:

a. **Clearly explain the purposes:** It is important to be transparent about the reasons for collecting personal data and to ensure that individuals understand how their personal data will be used [67] [68].

b. **Option to opt-out:** Individuals should be allowed to decline to collect their personal data and opt out of data collection at any time [69].

c. **Clear and simple language:** The language used to obtain consent should be easy to understand and free from jargon.

d. **Explicit consent:** In some cases, explicit consent may be required, such as when collecting sensitive personal data or when the data will be shared with third parties [66] [57]. In these obtaining an explicit statement of consent is necessary.

e. **Record of consent:** Keep a record of the consent obtained, including the date, time, and method of obtaining consent [70]. This can be used to demonstrate compliance with data privacy laws and regulations.

5.3. Data retention

Data retention refers to the length of time an organization keeps personal data. It is essential to specify the length of time that personal data will be retained and the conditions under which it will be deleted [71] [72]. Some considerations for data retention in blockchain applications may include the following:

5.3.1. Legal requirements: In some cases, the law may require data retention for tax or financial reporting purposes.

5.3.2. Business purposes: Personal data can be retained for as long as necessary for the blockchain application's business purposes, such as facilitating transactions or providing customer support with the data subject's consent [73].

5.3.3. Data subject requests: Every person has the right to request the deletion of their personal information [74], and organizations should have a process to handle such requests [75].

5.3.4. Data security: The removal of personal data that no longer serves a purpose or poses a security risk is essential. This applies particularly to situations where the blockchain network's security has been compromised.

It is imperative to note that the data retention criteria may vary depending on the type of blockchain application.

5.4. Data Security

5.4.1. Technical and organizational measures to protect personal data

Organizations must take immediate action to ensure the protection of personal data from unauthorized access, use, disclosure, or destruction. Both technical and organizational measures must be implemented without delay, particularly in the case of blockchain applications. These measures could include:

a. **Encryption:** Encrypt personal data to protect it from unauthorized access or interception [76].

b. **Access controls:** To safeguard personal data, it's important to implement access controls that include user authentication and authorization. This helps ensure that only authorized individuals can gain access [77].

c. **Use strong passwords and two-factor authentication:** Use strong passwords and two-factor authentication [78] to protect the network, making it more difficult for unauthorized parties to gain access.

d. **Network security:** Implement network security measures, such as firewalls [15] and intrusion detection systems, to protect personal data from external threats.

e. **Physical security:** Implementing physical security measures, such as secure data centers and access controls to physical premises, to protect personal data from unauthorized access.

f. **Data backup and disaster recovery:** Organizations should Implement data backup and disaster recovery measures to ensure that personal data is not lost in a system failure or disaster.

g. **Data minimization:** Implement data minimization practices [79], such as only collecting the personal data necessary for specific purposes, to reduce the risk of data breaches.

h. **Data processing agreements:** Establishing data processing agreements with third parties is crucial for organizations to protect personal data when it is shared externally [80].

5.4.2. Data breach

Organizations should be familiar with the relevant laws and regulations regarding data breach notification. They should have a plan for handling notification in the event of a security incident involving the blockchain [81]. This should include procedures for determining the scope of the breach, identifying the individuals who may be affected, and determining the appropriate course of action to take to mitigate the breach's impact [82]. If a data breach occurs, it is important to follow these steps:

a. Data breach response plan

The process for responding to a data breach should involve the following steps [83] [84]:

- **Identification of the scope of breach:** Organizations should determine the scope of a data breach involving blockchain networks [85].

- **Assess the situation:** Organizations should assess the situation to determine the extent of the breach and the types of data that may have been compromised. This should involve examining the blockchain network and related systems to identify unauthorized access or activity.
- **Identify the cause:** Organizations should attempt to identify the cause to understand how the breach occurred and what steps are needed to prevent similar breaches in the future.
- **Determine the extent:** Organizations should determine the extent by examining the data that may have been accessed or compromised. This should involve reviewing records of data transactions on the blockchain and determining which data may have been exposed.
- **Identify affected individuals:** Organizations must identify the individuals whose personal information may have been compromised during the data breach. This should involve reviewing records of data transactions on the blockchain and identifying the individuals the breach may have impacted.
- **Containment of the breach:** If there's a breach, act fast to contain it and stop any more unauthorized access or information disclosure. This may mean shutting down systems, revoking data access, or other actions to prevent further harm.
- **Investigation of the breach**: Organizations should investigate the cause of the data breach and take steps to prevent similar breaches from occurring.
- **Remediation of the breach:** It is imperative for companies to take responsibility for the aftermath of a data breach and provide necessary assistance to those impacted. This includes offering credit monitoring and other forms of support to mitigate the effects of the breach.
- **Notifying authorities:** In some cases, data breaches should be reported to authorities, such as data protection authorities or law enforcement. The requirements for reporting data breaches may vary depending on the specific data privacy laws and regulations that apply to the blockchain application.
- **Notification to media:** In some cases, it is necessary to notify the media of a data breach, mainly if it affects many individuals or has significant consequences.

b. Notification process

- **Responsibility for the notification:** The organization or company that holds the personal data is accountable for notification. This involves notifying the relevant data protection authorities, affected individuals, and other parties affected by the breach [86]. The specific individuals or departments within the organization responsible for notification may vary depending on the size and structure of the organization and the laws and regulations that apply. Organizations must have a transparent and robust process for responding to data breaches, including clear roles and responsibilities for notification.

- **Methods of notification:** The notification process for a data breach is contingent upon numerous factors including the specific circumstances and regulatory requirements [87]. Some standard methods of notification include:
  - **Email:** One of the most common notification methods is email. This should involve emailing affected individuals or relevant authorities, providing information about the data breach, and any steps the organization has taken in response.
  - **Postal mail:** In some cases, the notification may be made via mail, particularly if the organization must notify many individuals or email addresses are unavailable.
  - **Telephone:** Notification may also be made via telephone, particularly in cases where the data breach is severe or the organization needs to communicate with affected individuals promptly.
  - **Website:** Organizations may also use their website to provide information about data breaches, including details of the breach and any steps the organizations take in response.
  - **Social media:** In some cases, organizations may use social media platforms to provide information about data breaches and to communicate with affected individuals.
- **Timeline for notification:** The timeframe for informing individuals about a data breach can differ based on the particular situation and the laws and regulations that pertain to the company [81] [88]. Organizations may sometimes be required to notify relevant authorities and affected individuals within a particular timeframe. In contrast, in other cases, there may be more flexibility regarding the timing of notification.

In general, the timeline for notification should be as short as possible to minimize the impact of the data breach and ensure that affected individuals are informed of the breach promptly. This may involve notifying authorities and affected individuals immediately after the breach has been identified to provide an adequate response.

In cases where the data breach is grave or may have significant consequences for affected individuals, the timeline for notification should be shorter. In such cases, it is necessary to notify authorities and affected individuals as soon as possible to mitigate the breach’s impact.

5.5. Data subject rights

5.5.1. Right to access personal data

Organizations are obligated to grant individuals access to their personal data [89] [90]. The following elements are included regarding the right to access personal data:

a. Explanation

One key aspect of blockchain technology is that it allows for secure and transparent data storage and transfer. Anyone with the necessary authorization and access to the relevant blockchain network can access personal data stored on the blockchain. Everyone has the right to access their personal data and exercise this right [91] [92]. However, the specific process for making a subject access request (SAR) and accessing this personal data may differ depending on how the data is stored and used on the blockchain. To exercise their right of access in a blockchain context, individuals may need to take the following steps:

- Identify the organization or company holding their personal data on the blockchain. This involves contacting the organization directly or discovering more about the blockchain network on which the data is stored.
- Make a subject access request (SAR) to the organization or company [91] [92]. This involves sending a written request or filling out an online form.
- Provide proof of identity to the organization, as required. This involves submitting identification documents or other forms of verification.
- Wait for the organization to access personal data. The organization must provide the individual with a copy of their personal data and information about its use.

b. Process for accessing personal data

To gain access to personal data within a blockchain context, individuals must strictly follow the provided procedure. [91]:

- **Submit a request:** Individuals who wish to access their personal data on the blockchain should submit a request through the organization's online portal or by contacting the organization directly.
- **Review the request:** The organization should review the request to determine whether the individual has a legitimate need to access the data.

- **Approve or deny the request:** If the organization determines the individual's legitimate need to access the data, the request should be approved. If the request is not approved, the organization should inform the individual of the decision and the reasons for the denial.
- **Provide access to the data:** If the request is approved, the organization should provide the individual with access to their personal data within a reasonable timeframe set by that organization to provide personal data.
- **Monitor access to the data:** The organization should monitor access to the personal data to ensure that it is used responsibly and transparently.

It is worth noting that the specific process for making a SAR and accessing personal data on the blockchain may vary depending on the organization or company holding the data and the specific blockchain network being used. It may be helpful for individuals to contact the organization directly to learn more about the process and any necessary forms or documentation.

c. Timeframe for responding to requests

The organization must respond to a subject access request (SAR) within one month of receiving the request [93]. This timeframe can be extended by two months if the request is particularly complex, or the organization has received many SARs [94].

However, the organization must inform the individual of any such extension within one month of receiving the request and explain the reasons for the extension.

It is worth noting that these timeframes apply to requests for access to personal data that the organization is processing. If a third party is processing the data, the organization should request the data from the third party and may have to extend the timeframe for responding to the SAR to consider this.

d. Exceptions to the right to access personal data

Some of the exceptions to the right of access include [95] [96]:

- **Legal privilege:** Personal data subject to legal privileges, such as communications between a lawyer and client, is exempt from the right of access.
- **Personal data of another individual:** If access to an individual's personal data would reveal another individual's personal data, the organization should refuse the request.

Nevertheless, the organization is obligated to furnish the individual with a justification for withholding the data.

- **Prevention or detection of crime**: Personal data used to prevent or detect crime should be exempt from the right of access. The organization should still give an explanation to the individual as to why the data is being withheld.

It is worth noting that these exceptions are intended to balance the individual's right of access with other essential interests. The organization must carefully consider whether an exception applies in each case and must provide the individual with an explanation of any decision to withhold access to personal data.

e. Fees for accessing personal data:

The fees charged by an organization for accessing personal data on the blockchain will vary based on the details of the request and the expenses incurred in fulfilling it [97]. In case the person asks for more copies of the information, the organization can charge a reasonable fee that covers administrative expenses [98]. Individuals should contact the organization directly to learn more about any fees that may be charged.

5.5.2. Right to rectify personal data

Every person possesses the right to rectify their personal information in case it requires modification for increased accuracy or completeness. [42] [99]. Following elements are included about the right to rectify personal data:

a. Explanation

Individuals can request that the organization or company holding their personal data and ask for it to be corrected [100]. The organization is required to correct personal data without undue delay. Moreover, it is imperative to inform all external parties who have obtained the information about the rectification, unless such action would entail an unreasonably excessive amount of effort.

b. Techniques for Personal Data rectification

There are several ways in which data can be rectified or corrected on a blockchain:

- **Use of smart contracts:** To rectify data on a blockchain use smart contracts to delete or modify the data [101]. By implementing smart contracts, it is absolutely possible to automate the modification or deletion of data on the blockchain.
- **Use of off-chain data storage:** In some cases, storing sensitive or personal data off the blockchain may be more practical than modifying it on the blockchain [102]. This can allow the

data to be more quickly updated or deleted while maintaining a secure and immutable record on the blockchain [103].

- **Use of data encryption:** Encrypting data on the blockchain can help protect individuals' privacy while still allowing the data to be stored on the blockchain [76]. This can involve using a public key to encrypt the data, which can then be decrypted using a private key.
- **Use of data anonymization:** Data anonymization involves removing or masking personal identifiers from data, such as names, addresses, or phone numbers [104]. This can help protect individuals' privacy while still allowing the data to be stored on the blockchain [105].
- **Use of data access controls:** By implementing access controls, it is possible to limit who has access to sensitive or personal data on the blockchain [77] [15]. This can help protect individuals' privacy and ensure that those with a legitimate need only access the data.

Organizations can effectively rectify blockchain data by using these approaches while maintaining individuals' privacy and security.

c. Process for rectifying personal data

The process that should be followed for rectifying personal data on the blockchain [106] [107] include :

- **Identify the data that needs to be rectified:** The first step in the process is to identify the specific data that needs rectification and the reason for the rectification. This may involve reviewing the data and consulting with relevant parties to determine what needs to be done.
- **Determine the appropriate approach for rectifying the data:** Based on the nature of the data and the reason for the rectification, organizations should determine the most appropriate method for rectifying the data.
- **Necessary approvals or permissions:** Depending on the nature of the data and the parties involved, it is necessary to seek the approval or consent of relevant authorities or individuals before proceeding with the rectification.
- **Implement the rectification:** Organizations can implement the rectification once all necessary approvals and permissions have been obtained. This may involve updating the data on the blockchain or deleting it, depending on the chosen approach.

- **Confirm the rectification:** Once the rectification has been completed, organizations should confirm that the data has been successfully rectified and that any necessary updates or changes have been made.

It is worth noting that the specific process for requesting the rectification of personal data on the blockchain may vary depending on the organization or company holding the data and the specific blockchain network being used. It may be helpful for individuals to contact the organization directly to learn more about the process and any necessary forms or documentation.

d. Timeframe for responding to requests

Organizations holding an individual's personal data must respond to a request for rectification without undue delay and, in any case, within one month of receiving the request [93]. In the event of a complicated request or high volume of requests, the processing timeline may be extended by two months.

Organizations must inform individuals of any extension within a month of receiving the request and provide a clear explanation for the delay. Non-compliance can result in severe consequences. It is worth noting that these timeframes apply to requests for rectifying personal data on blockchain that the organization is processing. If a third party is processing the data, the organization may need to request the data from the third party and may have to extend the timeframe for responding to the request to take this into account.

Organizations must prioritize promptly responding to requests for rectification, not just to meet legal obligations, but to ensure the accuracy and up datedness of individuals' personal data.

e. Exceptions to the right to rectify personal data

Some of the exceptions to the right of rectification include the following [108]:

- **Legal privilege:** Personal data that is subject to legal privileges, such as communications between a lawyer and client, is exempt from the right of rectification.
- **Personal data of another individual:** If rectifying an individual's data would reveal another individual’s data, organizations may refuse the request. However, organizations must still provide the individual with an explanation of why the data is being withheld.
- **Prevention or detection of crime:** Personal data is used to prevent or detect crime and may be exempt from the right of rectification. However, organizations must still provide the individual with an explanation of why the data is being withheld.

It is worth noting that these exceptions are intended to balance the individual's right of rectification with other essential interests. Organizations must carefully consider whether an exception applies in each case and must provide the individual with an explanation of any decision to refuse the request.

f. Notification of rectification

It is mandatory for organizations or companies that hold personal data to notify any third parties who have received the data of any corrections requested by the person concerned unless it is impracticable or requires an excessive amount of effort. Failure to comply with this requirement will result in legal consequences.

To notify third parties of the rectification, organizations should contact the third parties directly or update any systems or databases to which the third parties have access. Organizations have the responsibility to guarantee the accuracy and currency of rectified personal data in all contexts where it is applied.

It is worth noting that the specific process for informing third parties of the rectification of personal data may vary depending on the organization or company holding the data and the specific blockchain network being used. It may be helpful for individuals to contact the organization directly to learn more about the process and any necessary forms or documentation.

5.5.3. Right to erase personal data

Every person has the right to request the deletion of their personal data. [109], also known as the "right to be forgotten." [74] Following elements can be included regarding the right to erase personal data:

a. Explanation

To exercise this right, individuals can request that the organization or company hold their personal data and ask for it to be erased [110]. The organization must expeditiously dispose of personal data unless there exists a justifiable cause to retain it, such as for the prevention or detection of criminal activity [111].

b. Techniques to erase data

Erasing personal data from a blockchain can be challenging due to the technology's decentralized and immutable nature [112]. Here are a few approaches that can be used to erase personal data from a blockchain:

- **Use of smart contracts:** One way to erase data from a blockchain is to use smart contracts to delete the data. Smart contracts are self-executing code-based agreements between buyers and sellers. The use of smart contracts enables the feasible automation of data deletion on the blockchain.
- **Use of off-chain data storage:** In some cases, storing sensitive or personal data off the blockchain may be more practical, rather than trying to delete it from the blockchain. This can allow the data to be more easily deleted while maintaining a secure and immutable record on the blockchain.
- **Use of data encryption:** Encrypting data on the blockchain can help protect individuals' privacy while still allowing the data to be stored on the blockchain. This can involve using a public key to encrypt the data, which can then be decrypted using a private key. The encrypted data can be made inaccessible by deleting the private key, effectively "erasing" it from the blockchain.
- **Use of data anonymization:** Data anonymization involves removing or masking personal identifiers from data, such as names, addresses, or phone numbers. This can help protect individuals' privacy while still allowing the data to be stored on the blockchain. By deleting the data that links the anonymized data to specific individuals, the data can be effectively "erased" from the blockchain.
- **Use of data access controls:** By implementing access controls, limiting access to sensitive or personal data on the blockchain is possible. This can help protect individuals' privacy and ensure that the data is only accessed by those with a legitimate business need for it. By revoking access to the data, it can be effectively "erased" from the blockchain for those users.

c. Process for erasing personal data

The process for erasing personal data from a blockchain will depend on the specific characteristics of the blockchain and the tools and technologies being used. Here are the general steps that should be involved in the process:

- **Identify the personal data that needs to be erased:** The first step is to identify the specific personal data that needs to be erased. This should involve reviewing the data stored on the blockchain and identifying any data that is no longer needed or that should not have been collected or stored in the first place.

- **Determine the appropriate approach for deleting the data:** Once the personal data to be erased has been identified, the next step is determining the proper approaches and techniques for deleting the data.
- **Implement the data deletion process:** Once the approaches and techniques for deleting the data have been determined, the next step is implementing the strategy. This may involve using specialized tools to update the data on the blockchain or delete it.
- **Confirm that the data has been deleted:** After the data deletion process has been completed, it is essential to confirm that the data has been successfully deleted. This should involve reviewing the blockchain to ensure that the data is no longer present or using specialized tools to verify the deletion.

By following these steps, organizations can effectively erase personal data from a blockchain in an efficient and secure way. However, it is essential to note that the deleted data may still be accessible through copies of the blockchain made before the deletion. Organizations should ensure that all the documents have also been deleted before confirming the data subject regarding the deletion of data.

d. Timeframe for responding to requests

Organizations are required to promptly respond to a request for erasure within one month of receipt. If the request is complex or multiple similar requests are received, an extension of up to two months may be granted. However, the organization must clearly explain the extension and notify the individual within one month of the request. Failure to comply with these requirements may result in consequences.

It is important to mention that the specified timeframes are only applicable to requests for the removal of personal data processed by the organization itself. If a third party is involved in processing the data, the organization may need to retrieve the data from the third party and thus require more time to respond to the request.

Organizations have an obligation to promptly address requests for erasure, not just for legal compliance but also as a best practice. Failing to do so means the individual's personal data is still being processed or utilized by the organization. This is unacceptable and must be rectified as soon as possible.

e. Exceptions to the right to erase personal data

Some of the exceptions to the right of erasure include:

- **Legal purposes:** In certain circumstances, personal information that is required for legal claims may not be subject to the right to be forgotten.
- **Personal data of another individual:** The organization retains the right to refuse requests for the deletion of personal data if doing so would reveal the personal data of another individual. However, organizations must still provide the individual with an explanation of why the data is being withheld.
- **Prevention or detection of crime:** Personal data is used to prevent or detect crime may be exempt from the right of erasure. However, organizations must still provide the individual with an explanation of why the data is being withheld.

It is worth noting that these exceptions are intended to balance the individual's right of erasure with other essential interests. The organization must carefully consider whether an exception applies in each case and provide the individual with an explanation of any decision to refuse the request.

f. Notification of erasure

If personal data is requested to be removed, it is mandatory for any organization or company holding the data to inform all third parties who have obtained the data, unless it is not practical or requires an excessive amount of effort.

The organization must take direct action to inform all third parties of the erasure or update any systems and databases they have access to. It is imperative that the organization ensures all personal data being erased is removed from every context in which it was being used. This responsibility falls solely on the organization, and it must be carried out with utmost care and diligence.

Individuals must keep in mind that the process of informing third parties about the erasure of personal data can vary based on the organization or company responsible for the data and the blockchain network being used. It is imperative that individuals directly contact the organization to obtain comprehensive information regarding the process, as well as any necessary forms or documentation.

5.5.4. Right to restrict processing of personal data

Individuals have the right to demand that their personal information be restricted instead of being completely erased [113] [114]. Following elements can be included:

a. Explanation

Individuals have the right to demand restrictions on the handling of their personal data. This means that their information may solely be utilized for explicit and clearly defined objectives.

In some cases, the organization may be required to restrict the processing of personal data if certain conditions are met, such as if the individual has challenged the accuracy of the personal data or if the processing is unlawful. In other cases, the organization may have the discretion to decide whether to grant the request for restriction.

Organizations must have a transparent and robust process in place for responding to requests for the restriction of processing personal data to ensure that they can protect the rights of individuals and comply with their legal obligations.

b. Techniques to restrict personal data

There are a few approaches that can be used to restrict the processing of personal data on a blockchain:

- **Use of data access controls:** By implementing access controls, it is possible to limit who has access to sensitive or personal data on the blockchain. This can help protect individuals' privacy and ensure that the data is only accessed by those with a legitimate business need for it.
- **Use of data minimization:** Organizations should collect and store only the necessary personal data to achieve their objectives, reducing data on the blockchain and mitigating processing risk. Failure to comply can have severe consequences, so data minimization should be a fundamental aspect of data management practices.
- **Use of data anonymization:** Data anonymization removes personal identifiers like names, addresses, and phone numbers to protect privacy while keeping data on the blockchain. This restricts personal data processing by removing links to specific individuals.
- **Use of data access requests:** Individuals have the right to demand access to their personal data and restrict its processing in certain circumstances. By implementing processes for handling such requests and allowing individuals to opt-out of the processing of their data, organizations can effectively restrict the processing of personal data on the blockchain.

- **Use of data de-identification:** Data de-identification involves removing or masking personal identifiers from data to make it unlikely that the data could be linked to a specific individual. This can be done through data perturbation or generalization, which can help protect individuals' privacy while still allowing the data to be stored on the blockchain.
- **Use of data aggregation:** Data aggregation involves combining data from multiple sources, making it challenging to identify specific individuals. By aggregating data on the blockchain, it is possible to reduce the amount of personal data stored and restrict the processing of personal data.
- **Use of data tagging:** Data tagging involves adding tags or labels to data on the blockchain, which can be used to identify the data and control how it is processed. Limiting the processing of personal data can be achieved by implementing specific tags to restrict access to it.
- **Use of data partitioning:** Data partitioning involves dividing data on the blockchain into smaller units or "partitions" that can be processed separately. By restricting access to certain partitions, it becomes feasible to limit the handling of personal data.

To ensure data integrity and security on a blockchain, organizations must implement specific techniques to limit the processing of personal data. However, it's crucial to note that the most suitable approach or combination of techniques will vary based on the unique characteristics of the blockchain and the data being processed.

c. Process for restricting processing

Individuals can request the restriction of their personal data processing by following a specific process:

- **Make a written request:** The request for restriction of processing should be made in writing, either by letter or email. The request should specify the grounds for the request and the specific processing activities the individual seeks to restrict.
- **Submit any necessary documentation:** The individual may need to submit specific documentation supporting their requests, such as identification documents or proof of their relationship to the personal data in question.
- **Submit the request to the relevant organization:** The request should be submitted to the organization or company processing the personal data. It is important to provide contact information so the organization can respond to the request.

- **Wait for a response:** The organization should respond to the request for restriction of processing within a reasonable timeframe, which may be specified by law or best practice. If the organization approves the request, it is imperative that they strictly restrict the processing of personal data in accordance with the request. Conversely, if the request is rejected, the organization is obliged to notify the individual of their right to appeal and provide them with the reasons for the refusal without delay.

Organizations must have a clear protocol to address requests for limiting personal data processing on blockchain and protect individuals' rights. The process may vary based on laws and regulations and the specifics of the request.

d. Timeframe for responding to requests

The timeframe within which the organization will respond to requests for the restriction of personal processing data may be required by law or best practice. In general, the organization should respond to the request within a reasonable timeframe, considering the request's complexity and the case's specific circumstances.

When individuals request the restriction of their personal data processing, organizations must respond promptly, within one month. If the request is complex or multiple requests are submitted, the organization reserves the right to prolong the response time by up to two months. Nevertheless, the requester must be informed of the extension and the reason behind it within one month of their original request.

Organizations need to be aware of their legal obligations when handling requests to restrict data on blockchain. They must safeguard individuals' rights and be prepared to address such requests appropriately.

e. Exceptions to the right to restrict processing

There may be exceptions where processing personal data is necessary for certain specified purposes, such as:

- **The exercise of the right of freedom of expression and information:** The processing of personal data may be necessary for the exercise of the right of freedom of expression and information, such as in the case of journalists or other individuals who use personal data in the course of their work.

- **The fulfillment of a legal obligation:** The processing of personal data may be necessary for fulfilling a legal obligation, such as in the case of organizations that are required to maintain certain records or to report certain information to authorities.
- **Protecting the public interest:** The processing of personal data may be necessary to protect the public interest, such as in organizations responsible for public health or safety.
- **The exercise or defense of legal claims:** The processing of personal data may be necessary for the exercise or defense of legal claims, such as in the case of organizations involved in legal proceedings.
- **Personal data of another individual:** It may not always be feasible to restrict the handling of personal data, especially if doing so would jeopardize the privacy of another individual or impede the lawful objectives of the enterprise.

The exceptions to the right to restrict the processing of personal data will depend on the laws and regulations that apply to the organization and the case’s specific circumstances. Organizations must be familiar with their legal obligations in this regard to ensure that they can respond effectively to requests to restrict personal data processing and protect individuals' rights.

f. Notification of restriction:

Organizations must inform third parties who have obtained personal data about the restrictions on processing. This action is crucial to ensure the safety of the information and put an immediate halt to any further processing or disclosure of the data.

In order to safeguard personal data and prevent any further processing or disclosure of it, organizations must promptly inform any third parties who have received the data about the restriction. It is important to note that the process of notification may vary depending on applicable laws and regulations and specific circumstances of each case.

The notification should be made in writing, such as by email or letter, or by other means, such as via telephone or the organization's website. The notification should include information about the restriction on processing and any instructions for how the third party should handle the personal data considering the restriction.

It is worth noting that the specific process for notification will depend on the laws and regulations that apply to the organization and the case’s specific circumstances. Organizations should be familiar with their legal obligations to ensure that they can protect the rights of individuals and comply with their legal obligations. It is important to note that the requirements for the right to restrict processing may vary depending on the specific data privacy laws, regulations, and techniques that apply to the blockchain application.

5.5.5. Right to data portability

Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transfer their personal data to another organization [115] [116]. This right is known as the "right to data portability." In blockchain context, following elements can be included regarding the right to data portability:

a. Explanation

Individuals possess the unquestionable right to demand the transfer of their personal data to another entity, commonly known as the right to data portability. It is the responsibility of the respective organization or company to process this request and ensure that the individual's personal data is duly transferred.

In some cases, the organization may be required to transfer the personal data to another organization if certain conditions are met, such as if the personal data has been provided by the individual and is being processed by automated means. In other cases, the organization may have the discretion to grant the transfer request.

Organizations must have a transparent and robust process in place for responding to requests for the transfer of personal data to ensure that they can protect the rights of individuals and comply with their legal obligations. This is especially important in the context of blockchain, where personal data may be stored decentralized and may be more challenging to access and transfer.

To facilitate the transfer of personal data, it may be necessary for the organization to have systems in place for extracting and transferring the relevant data. It may also be necessary to ensure that the data is in a format that can be easily transferred and is secured during the transfer process.

b. Process for data portability

To request the transfer of their personal data, individuals should follow the following process:

- **Make a written request:** The request to transfer personal data should be made in writing, either by letter or email. The request should specify the grounds for the request and the specific data the individual seeks to transfer.
- **Submit any necessary documentation:** The individual may need to submit specific documentation supporting their requests, such as identification documents or proof of their relationship to the personal data.

- **Submit the request to the relevant organization:** The request should be submitted to the organization or company processing the personal data on blockchain. It is important to provide contact information so the organization can respond to the request.
- **Wait for a response:** The organization should respond to the request to transfer personal data within a reasonable timeframe, which may be specified by law or best practice. The organization may grant the request, in which case it will be required to transfer the personal data to the specified organization in accordance with the request. Alternatively, the organization may refuse the request, in which case it should provide the individual with the reasons for the refusal and inform them of their right to appeal the decision.

Organizations must establish a clear and reliable process for requesting the transfer of personal data in the context of blockchain, while safeguarding individual rights. It's crucial to keep in mind that this process can differ based on applicable laws and regulations and specific request details. Act now and ensure that your process actively requests the transfer of personal data.

c. Timeframe for responding to requests

Organization should respond to the request within a reasonable timeframe, considering the request's complexity and the case's specific circumstances.

Organizations must respond to personal data transfer requests within a month. Extensions of two months are allowed for complex requests, but the individual must be informed within the first month. Non-compliance can have legal consequences.

Responding promptly and effectively to personal data transfer requests is crucial for organizations to avoid infringement of individuals' rights and legal consequences. The response timeframe may vary based on applicable laws and circumstances.

d. Exceptions to the right to data portability

Several exceptions to the right to data portability may apply in certain situations. These exceptions are intended to balance the rights of the individual with the needs of the organization to process the data on blockchain. Here are some examples of exceptions to the right to data portability:

- **Necessity for performing a task in the public interest:** In some cases, the processing of personal data may be necessary to perform a job in the public interest. In these cases, the data controller may be justified in refusing to allow the data to be ported to another system or service.

- **Necessity for the exercise of official authority:** The processing of personal data may also be necessary for the exercise of official authority. In these cases, the data controller may be justified in refusing to allow the data to be ported to another system or service.
- **Risk of harming the rights and freedoms of others:** The data controller may also be justified in refusing to allow the data to be ported if doing so would risk damaging the rights and freedoms of others. This may include cases where the data contains sensitive or confidential information about other individuals.
- **Necessity for the establishment, exercise, or defense of legal claims:** The data controller may also be justified in refusing to allow the data to be ported if doing so would be necessary for the establishment, exercise, or defense of legal claims.

e. Format of the data

Personal data should be provided in a structured, commonly used, and machine-readable format. This means that the data should be organized in a logical and easy-to-understand manner and in a format that is widely accepted and can be quickly processed by computers.

This will enable the recipient organization to access and use the data quickly and help to ensure that the data is protected and secure during the transfer process to protect the data's privacy and confidentiality.

Some examples of structured, commonly used, and machine-readable formats include CSV (comma-separated values), XML (extensible markup language), and JSON (JavaScript object notation).

5.6. Data controller and processor obligations

5.6.1. Contractual obligations between data controllers and data processors

A data controller is the organization that decides how personal data is processed. They have the responsibility of determining the purposes and methods of data processing. In contrast, a data processor [117] is an organization that processes personal data on behalf of a data controller [118] [119].

Following elements can be included about the contractual obligations between data controllers and data processors:

a. Explanation of the roles of data controllers and data processors

Regarding the processing of personal data on a blockchain, data controllers have several responsibilities which include:

- Determine the purposes for which the personal data will be processed on the blockchain.
- Ensure that the processing of personal data on the blockchain is carried out in accordance with data protection laws.
- Ensure that appropriate technical and organizational measures are in place to protect personal data on the blockchain, such as using secure protocols and encryption.
- Respond to requests from individuals exercising their rights under data protection laws, such as the right to access or rectify their personal data on the blockchain.

On the other hand, data processors [120] are responsible for storing, organizing, or analyzing the personal data on the blockchain, depending on the specific instructions of the data controller. Data processors are required to:

- Process the personal data on the blockchain only in accordance with the instructions of the data controller.
- Ensure that appropriate technical and organizational measures are in place to protect personal data on the blockchain.
- Ensure that any third-party service providers with access to the personal data on the blockchain also comply with the data controller's instructions and have appropriate technical and organizational measures in place.
- Ensure that personal data on the blockchain is accurate and up to date.
- Ensure that personal data on the blockchain is kept only as long as necessary.
- Ensure that personal data on the blockchain is processed transparently and that data subjects are informed of their rights concerning processing their personal data.
- Ensure that appropriate measures are in place to enable data subjects to exercise their rights concerning processing their personal data on the blockchain.
- Ensure that personal data on the blockchain is kept confidential and is not disclosed to unauthorized parties.
- Ensure that applicable data protection laws and regulations process personal data on the blockchain.

- Ensure that any breaches of personal data on the blockchain are reported to the data controller and, if required, to the relevant supervisory authority and data subjects promptly.

b. Contractual obligations of data processors

Some of the critical contractual obligations [121] of data processors include:

- **Processing personal data only per the instructions of the data controller:** Data processors should follow the specific instructions of the data controller when processing personal data. This includes any instructions related to the purposes for which the data is being processed, the duration of the processing, and the security measures that must be put in place to protect the data.
- **Ensuring the security of personal data:** Data processors must put in place appropriate technical and organizational measures to protect the personal data they are processing. This may involve using secure protocols and encryption and implementing measures to prevent unauthorized access or disclosure of the data.
- **Responding to requests from individuals exercising their rights under data protection laws**: Data processors are needed to assist the data controller in fulfilling requests for accessing or correcting personal data.
- **Maintaining records of processing activities**: Data processors must keep records of their processing activities, including objectives, personal data types, and recipients. This is necessary and must be followed to avoid serious consequences.
- **Reporting personal data breaches:** Report any data violations immediately and cooperate fully during investigations.

It is worth noting that these contractual obligations are intended to protect individuals' rights and ensure that their personal data is processed securely and transparently. Data processors must adhere to these obligations to comply with privacy laws and regulations.

c. Monitoring of data processors

The person in charge of data must ensure that data processors are fulfilling their contractual obligations by implementing rigorous monitoring measures. This is important to ensure that the data processors comply with their legal obligations and protect individuals' personal data through data privacy laws and regulations.

There are a variety of measures that the data controller should take to monitor the compliance of data processors with their contractual obligations. These measures include:

- **Conducting regular audits or reviews:** The data controller should conduct periodic audits or reviews of the data processors to ensure they comply with their contractual obligations and protect individuals' personal data.
- **Imposing strict security requirements:** The data controller should impose strict security requirements on the data processors, including requirements for secure data storage and transmission, to protect individuals' personal data.
- **Requiring regular reporting:** The data controller should require the data processors to provide regular reports on their activities, including handling personal data, to ensure they comply with their contractual obligations.
- **Establishing clear protocols for responding to data breaches:** The data controller should establish clear protocols for responding to data breaches, including procedures for notifying the data controller and the individuals affected by the breach to ensure that the data processors comply with their contractual obligations.

Monitoring data processors is crucial to protect individuals' personal data and comply with legal responsibilities. Neglecting this responsibility puts data at risk.

d. Termination of data processing contracts

The data controller may terminate its contract with a data processor if it breaches the data processor's obligations. This may include a breach of the data processor's obligations under data privacy laws and regulations and a breach of the specific terms and conditions of the contract between the data controller and the data processor.

There are a variety of circumstances under which the data controller should decide to terminate its contract with a data processor. These circumstances include:

- **Non-compliance with data privacy laws and regulations:** The data controller may decide to terminate the contract if the data processor fails to comply with data privacy laws and regulations.
- **Breach of security obligations:** If the data processor fails to maintain adequate security measures to protect the personal data of individuals, such as by failing to implement appropriate safeguards or report a data breach, the data controller may decide to terminate the contract.
- **Failure to meet performance or service level agreements**: If the data processor fails to meet performance or service level agreements, such as by failing to provide timely or accurate data processing services, the data controller may decide to terminate the contract.

- **Material breach of the contract:** If the data processor commits a material breach of the contract, such as by failing to comply with the terms and conditions of the contract or by acting in a manner that is detrimental to the interests of the data controller, the data controller may decide to terminate the contract.

The data controller must have clear and robust contractual provisions to protect its interests and ensure the data processor complies with its obligations. The data controller should carefully consider the circumstances under which it may decide to terminate the contract with a data processor to ensure it can protect individuals' personal data and comply with its legal obligations.

5.6.2. Data protection impact assessments

a. Explanation of data protection impact assessments

DPIA assesses the impact of data processing on privacy/security. It's crucial for safeguarding sensitive information [122]. DPIAs are necessary because data processing activities, such as collecting, using, and storing personal data, can significantly impact individuals' privacy and security. To ensure the protection of individuals' privacy and security, organizations must conduct a DPIA to identify and evaluate potential risks. This is crucial in enabling them to take the necessary measures to reduce the risks to an acceptable level.

There are a variety of reasons [123] why DPIAs are necessary for the context of blockchain:

- **To comply with data privacy laws and regulations:** Many data privacy laws and regulations, such as the General Data Protection Regulation (GDPR) [122] and the California Consumer Privacy Act (CCPA) [124], require organizations to conduct DPIAs in certain circumstances. By conducting a DPIA, organizations can demonstrate that they are complying with their legal obligations and are taking appropriate measures to protect the personal data of individuals.
- **To identify and assess risks to the privacy and security of individuals:** DPIAs are an essential tool for organizations to assess and scrutinize the potential privacy and security threats that may arise from their data processing activities. This assessment helps in taking necessary measures to mitigate these risks, such as implementing safeguards and being transparent and informative to individuals.
- **To ensure that the data processing is proportionate and necessary:** Organizations must conduct DPIAs to assess the necessity and proportionality of their data processing activities. They

must also explore less invasive alternatives to ensure fairness, transparency, and respect for individuals' privacy rights.

Overall, DPIAs are an essential tool for organizations in the context of blockchain, as they help to ensure that the personal data of individuals is protected, and that the data processing is conducted fairly and transparently.

b. Triggers for conducting a data protection impact assessment

DPIA is crucial when handling personal data that may affect people's rights and freedoms [125] [126]. This is typically the case when the data processing activity involves using new technologies or processing sensitive personal data or when the data processing activity is large-scale or systematic.

Organizations must conduct a DPIA in the following circumstances:

- Cases where the data processing involves the use of new technologies, the processing of sensitive personal data, or the processing of large amounts of personal data.
- Protect data, especially personal information, with necessary precautions.
- Cases where the data processing involves using personal data to evaluate certain aspects of an individual's personal characteristics, such as their performance at work or creditworthiness.
- Cases where the data processing involves using personal data to make automated decisions, such as creditworthiness or employment.

It is worth noting that these are only a few examples of the circumstances under which a DPIA must be conducted [127]. Organizations need to be familiar with their legal obligations to ensure they can act DPIAs appropriately.

c. Process for conducting a data protection impact assessment

Several steps should be followed in conducting a data protection impact assessment (DPIA) [128] [129] [130]. These steps include:

- **Identifying the processing activities:** Before starting a DPIA, it is crucial to identify the data processing activities that will take place. This involves recognizing the personal information that will be gathered, the objectives for which it will be utilized, and the parties involved in the process.

- **Assessing the risks to privacy:** To conduct a DPIA, carefully evaluate potential risks that may compromise privacy and security. Identify risks, assess probability and severity, and determine the impact on individual rights and freedoms.
- **Determining the measures that will be taken to mitigate the risks**: To protect individuals' privacy and security during DPIA, implement safeguards like encryption and access controls. Be transparent about data processing activities. This is step three and requires care.
- **Consulting with relevant stakeholders:** Including all stakeholders in a DPIA is crucial for gathering valuable feedback and mitigating risks to address potential data privacy concerns effectively.
- **Documenting the DPIA:** The final step in conducting a DPIA is to document the results of the DPIA, including the data processing activities that will be carried out, the risks to the privacy and security of individuals, and the measures that will be taken to mitigate those risks.

Organizations must follow these steps to conduct a thorough and comprehensive DPIA and ensure that individuals' personal data is protected on blockchain, and that the data processing is carried out fairly and transparently.

d. Documentation of data protection impact assessments

Organizations should keep data protection impact assessments (DPIAs) to demonstrate compliance with data privacy laws and regulations and provide a record of the steps taken to protect personal data individuals on blockchain. The records that should be kept of DPIAs may vary depending on the specific data privacy laws and regulations that apply to the organization and the nature and scope of the data processing activities in blockchain.

Generally, organizations should keep records of DPIAs that include the following information:

- The processing activities require explicit information regarding the personal data collected, the purpose of its usage, and the parties responsible for its handling.
- The DPIA has identified potential risks to the privacy and security of individuals. The report outlines the likelihood and severity of these risks.
- Information about the measures taken to mitigate the risks to the privacy and security of individuals, such as the safeguards or controls implemented, or the transparency and notice provided to individuals.

- A summary of the findings of the DPIA and any recommendations made for improving data processing activities or mitigating the risks to the privacy and security of individuals.

The records of DPIAs should be kept securely and confidentially and made available to individuals or authorities as required by law or upon request. Organizations must provide individuals with a copy of their personal data upon request. In this case, the records of DPIAs may be made available to individuals to provide them with information about the data processing activities that have been carried out and the measures taken to protect their personal data. Similarly, data protection authorities may request access to the records of DPIAs to verify compliance with data privacy laws and regulations.

5.7. Compliance with data privacy laws and regulations

5.7.1. Compliance with top data privacy regulations and laws

a. Explanation of compliance

It is essential for organizations to clearly state their commitment to compliance with data privacy regulations and laws and outline the measures they will take to ensure compliance. This demonstrates the organization's commitment to protecting individuals' privacy and security and conducting their data processing activities fairly and transparently.

To ensure compliance with data privacy regulations and laws, organizations may take a variety of measures, such as:

- **Implementing appropriate safeguards and controls:** This includes encryption, access controls, and other security measures to protect the personal data of individuals on blockchain.
- **Providing transparency and notice to individuals:** This includes providing clear and concise privacy policies and notices to individuals about the data processing activities that will be carried out, as well as providing individuals with the opportunity to opt-out of certain data processing activities of blockchain if they choose.
- **Conducting data protection impact assessments:** This may include conducting DPIAs in accordance with data privacy laws and regulations to identify and assess the potential risks to the privacy and security of individuals on blockchain and to determine the measures that will be taken to mitigate those risks.
- **Training employees:** This includes training employees on data privacy laws and regulations and the organization's data protection policies and procedures for blockchain.

- **Establishing a data protection officer (DPO):** This includes appointing a DPO [131] responsible for overseeing the organization's compliance with data privacy laws and regulations and for monitoring the organization's data protection policies and procedures [132].

By taking these measures, organizations can demonstrate their commitment to compliance with data privacy regulations and laws and ensure they can protect individuals’ personal data fairly and transparently on blockchain.

b. Identification of applicable regulations and laws

Organizations need to identify the specific data privacy regulations and laws that apply to their processing of personal data. Many data privacy regulations and laws may apply to an organization, depending on the jurisdiction in which the organization is located and the nature and scope of the data processing activities.

Organizations should be familiar with the data privacy regulations and laws that apply to their processing of personal data to ensure compliance with those laws and protect individuals' personal data in blockchain.

c. Compliance with the rights of individuals:

Organizations should take several measures to ensure compliance with the rights of individuals regarding their personal data. Some of the measures that organizations may take to ensure compliance with the rights of individuals include:

- Providing individuals with access to their personal data.
- Allowing individuals to rectify their personal data.
- Allowing individuals to erase their personal data.
- Allowing individuals to restrict the processing of their personal data.
- Allowing individuals to request the transfer of their personal data to another organization.

By taking these and other measures, organizations can ensure compliance with the rights of individuals regarding their personal data on blockchain and demonstrate their commitment to protecting the privacy and security of individuals.

d. Compliance with data protection impact assessments

Organizations must take several measures to ensure compliance with data protection impact assessments (DPIAs). Some of the steps that organizations should take to ensure compliance with DPIAs include:

- **Conducting DPIAs as necessary:** This includes conducting DPIAs in accordance with data privacy laws and regulations whenever the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals [123]. This includes processing activities such as large-scale processing of sensitive personal data or using new or untested blockchain technologies.
- **Keeping records of DPIAs:** This includes keeping records of the DPIAs conducted and any recommendations or measures to mitigate the risks identified in the assessments. These records may be made available to individuals or authorities upon request.
- **Implementing the recommendations of DPIAs:** This includes taking the suggestions and measures identified in DPIAs and implementing them to mitigate the risks to the privacy and security of individuals. This includes measures such as implementing security controls or providing additional transparency and notice to individuals about data processing activities in blockchain applications.

Overall, by taking these and other measures, organizations should ensure compliance with data protection impact assessments and demonstrate their commitment to protecting the privacy and security of individuals.

e. Compliance with contracts with data processors:

Organizations must take measures to ensure compliance with their agreements. Some of the steps that organizations should take to ensure compliance with their contracts with data processors include:

- **Establishing clear contracts with data processors:** This includes establishing contracts with data processors that set out the roles and responsibilities of each party, as well as the measures that the data processors must take to protect the personal data of individuals.
- **Monitoring the compliance of data processors:** This includes monitoring the compliance of data processors with their contractual obligations, including their obligations to protect individuals' personal data and comply with data privacy laws and regulations.
- **Taking action in the event of a breach:** This includes taking action in the event of a breach of a data processor's contractual obligations, such as by terminating the contract with the data processor or taking other appropriate measures to ensure compliance.

It is important to note that the requirements for compliance with data privacy regulations and laws may vary depending on the specific rules and laws that apply to the blockchain application.

5.7.2. Penalties and sanctions for non-compliance

Following elements are included regarding penalties and sanctions [133] [134] for non-compliance:

a. Explanation of penalties and sanctions

Organizations need to understand the consequences of non-compliance with blockchain data privacy policy, as failure to comply with these can have severe implications for both the organization and the individuals whose personal data is being processed on blockchain.

Some of the consequences of non-compliance with data privacy policy may include the following:

- **Penalties and fines:** Penalties and fines should be imposed on organizations that fail to comply with their obligations [135]. These penalties can be substantial, imposed by regulatory authorities, or through private lawsuits from individuals or advocacy groups.
- **Reputational damage:** Non-compliance with blockchain data privacy policy can also result in reputational damage to an organization, as it may be perceived as not taking the privacy and security of individuals seriously. This can lead to losing trust and confidence in the organization and may result in losing customers or other stakeholders.
- **Legal liability:** Organizations that fail to comply with blockchain data privacy policy may also be exposed to legal liability for any harm that individuals suffer due to the non-compliance. This may include liability for damages, as well as other legal remedies.

Overall, it is essential for organizations to understand the consequences of non-compliance with blockchain data privacy policy and to take steps to ensure compliance to protect individuals' privacy and security and avoid any potential penalties or sanctions.

b. Types of penalties and sanctions

Penalties and sanctions that should be imposed for non-compliance with blockchain user data privacy policy include:

- **Fines:** Substantial fines should be imposed by regulatory authorities or through private lawsuits brought by individuals or advocacy groups on organizations that fail to comply with their obligations.
- **Imprisonment:** In some cases, non-compliance with blockchain user data privacy policy may be considered a criminal offense, and individuals violating these laws should be imprisoned.

- **Legal action:** Organizations that fail to comply with blockchain user data privacy policy may also be exposed to legal liability for any harm that individuals suffer due to the non-compliance. This includes liability for damages, as well as other legal remedies.

Overall, it is essential for organizations to understand the potential penalties and sanctions that should be imposed for non-compliance with blockchain user data privacy policy and to take steps to ensure compliance to avoid any potential penalties or sanctions.

c. Process for determining penalties and sanctions

The process for determining the appropriate penalties and sanctions for non-compliance with blockchain user data privacy policy may vary depending on the specific statute or law that has been violated and the jurisdiction in which the violation occurred.

Generally, the process for determining the appropriate penalties and sanctions for non-compliance should include the following:

- **Investigation:** The first step in determining the appropriate penalties and sanctions for non-compliance may be an investigation by a regulatory authority or other body to determine the nature and extent of the non-compliance. This may involve gathering evidence, interviewing individuals, and reviewing documents and other records.
- **Determination of liability:** Based on the investigation results, the regulatory authority or other body should determine that the organization is liable for non-compliance with blockchain user data privacy policy. This determination should be based on the evidence gathered during the investigation and the specific provisions of the statute or law that have been violated.
- **Imposition of penalties and sanctions:** If the organization is liable for non-compliance, the regulatory authority or other body should impose penalties and sanctions, such as fines, imprisonment, or other legal action. The penalties and sanctions imposed should depend on the severity of the non-compliance and any mitigating or aggravating factors.
- **Appeals process:** In many cases, organizations have the right to appeal the determination of liability or the imposition of penalties and sanctions. The appeals process may vary depending on the jurisdiction but generally involves presenting additional evidence or arguments supporting the organization's position.

Overall, organizations need to understand the process for determining the appropriate penalties and sanctions for non-compliance with blockchain user data privacy policy and to be familiar with any appeals process that may be available.

d. Notification of penalties and sanctions

This is important to ensure transparency and accountability and help individuals and authorities understand the consequences of non-compliance.

There are several ways that organizations may notify about any penalties and sanctions that are imposed for non-compliance with blockchain user data privacy policy. Some possible options include the following:

- **Public announcement:** In some cases, organizations may publicly announce any penalties and sanctions imposed for non-compliance. This may be done through a press release or other public statement and may be shared through the organization's website or social media channels.
- **Notification to individuals:** In some cases, organizations may be required to notify individuals whose personal data has been affected by non-compliance directly or through the relevant regulatory authority. This notification may be made through a letter, email, or other means of communication.
- **Notification to authorities:** Organizations may also be required to notify relevant authorities of any penalties and sanctions imposed for non-compliance with blockchain user data privacy policy. This may be done through a report or other formal notification and may be required by the relevant regulatory authority or other body.

It is important to note that the requirements for penalties and sanctions for non-compliance may vary depending on the specific data privacy laws and regulations that apply to the blockchain application.

5.8. Contact information

5.8.1. Contact details for inquiries and complaints

The following elements are included about contact details for questions and complaints [136]:

a. Explanation of the process for making inquiries or raising complaints

This is essential for organizations to have a transparent process in place for individuals to follow to make inquiries or submit complaints about processing their personal data. This process should be easily accessible and straightforward and designed to address any concerns or issues individuals may have in a timely and effective manner [137].

Some possible steps that organizations should include in their process for handling inquiries or complaints about the processing of personal data are:

- **Contact information:** Organizations should provide individuals with clear and easy-to-find contact information for making inquiries or raising complaints about processing their personal data. This may include a dedicated email address, phone number, or online form.
- **Response timeline:** Organizations should specify the timeframe for responding to inquiries or complaints about personal processing data, which may be required by law or best practice. This timeline should be reasonable and consider the complexity of the issue raised.
- **Handling of complaints:** Organizations should have a process in place for handling complaints about the processing of personal data, which may include a review of the complaint, an investigation into the issue raised, and a response to the individual making the complaint.
- **Appeals process:** In some cases, individuals may have the right to appeal a decision or response made by the organization about their inquiry or complaint. Organizations should have a transparent appeals process, including the steps individuals can follow to appeal and the timeline for doing so.

Overall, organizations need to have a straightforward and effective process for handling inquiries and complaints about processing personal data to address any concerns or issues that individuals may have in a timely and satisfactory manner.

b. Contact details

Organizations must provide various contact details that individuals can use to make inquiries or raise complaints about processing their personal data on blockchain. This will help ensure that individuals have multiple ways to reach out to the organization and address their concerns.

Some possible contact details that organizations may provide to individuals include:

- **Phone number:** Organizations should provide a dedicated phone number that individuals can use to make inquiries or raise complaints about processing their personal data. This number should be easily accessible and staffed by individuals trained to handle these questions and complaints.
- **Email address:** Organizations should also provide a dedicated email address that individuals can use to make inquiries or raise complaints about processing their personal data. This email address should be checked regularly and used to send responses to questions and complaints promptly.
- **Postal address:** Sometimes, individuals may prefer to make inquiries or raise complaints about processing their personal data through traditional mail. Organizations should provide a

postal address that individuals can use for this purpose and ensure that they have processes in place to handle these types of inquiries and complaints promptly and effectively.

Overall, organizations need to provide a range of contact details that individuals can use to make inquiries or raise complaints about processing their personal data to ensure that they have multiple ways to reach out to the organization and address their concerns.

c. Timeframe for responding to inquiries and complaints

Organizations should specify the timeframe within which they will respond to questions and complaints about personal data, as this can help ensure that they meet their obligations under data protection laws and best practices [138] [139]. Here are a few considerations for organizations to consider when determining the timeframe for responding to questions and complaints:

- **Nature of the question or complaint:** The complexity and nature of the question or complaint may affect the time it takes to respond. For example, a simple request for access to personal data may be easier to respond to than a complaint about a breach of data privacy rights.
- **Number of questions and complaints**: If the organization receives a high volume of queries and complaints, it may take longer to respond. Organizations must have processes to manage the volume of questions and complaints efficiently and effectively.

Generally, it is best practice for organizations to respond to questions and complaints as quickly as possible while ensuring they are thorough and accurate. This can help to maintain trust and confidence in the organization and its handling of personal data.

d. Notification of actions taken

Organizations should specify whether and how they will notify individuals of the actions taken in response to their inquiries or complaints about processing personal data. This will help to ensure transparency and accountability and to let individuals know the outcome of their questions or complaint.

There are several ways that organizations may choose to notify individuals of the actions taken in response to their inquiries or complaints. Some possible options are as following:

- **Written response:** Organizations may provide a written response to individuals, outlining the actions taken in response to their inquiry or complaint. This response may be sent by email, letter, or other means of communication and should provide a clear and concise explanation of the steps taken to address the issue raised.

- **Phone call:** In some cases, organizations may follow up with individuals by phone to provide more information or to discuss the outcome of their inquiry or complaint in greater detail.
- **Online notification:** Organizations may also use online tools, such as their website or social media channels, to notify individuals of the actions taken in response to their inquiries or complaints.

Overall, organizations need to specify whether and how they will notify individuals of the actions taken in response to their inquiries or complaints about the processing of personal data to ensure transparency and accountability and to let individuals know the outcome of their query or complaint.

5.9. Organizations' policies and updates

It is essential for the organizations to have their own blockchain user data privacy policies which will be depending upon their use of blockchain and service of personal data in accordance with this policy and existing laws and regulations.it is also essential for the organizations to keep their policies UpToDate.

5.9.1. Procedure for updating the policy

In a blockchain user data privacy policy by organizations, it is essential to include a procedure for updating the policy to ensure that it remains current and compliant with relevant data privacy laws and regulations [140]. The following elements can be included in the system for updating the policy:

a. Explanation of the need for updates:

Organizations must regularly update their data privacy policy to ensure that it remains current and compliant with relevant data privacy laws and regulations. This is because data privacy laws and regulations are constantly evolving, and organizations need to stay up to date with these changes to ensure that they are meeting their obligations and protecting the personal data of individuals.

There are several factors that organizations may need to consider when updating their data privacy policy, including:

- **Changes in data privacy laws and regulations:** As mentioned, data privacy laws and regulations are constantly evolving, and organizations must stay up to date to ensure that their policy is compliant. This may involve reviewing the policy regularly to identify any areas that need to be updated and making necessary changes promptly.

- **Changes in the organization's business practices:** Organizations may also need to update their data privacy policy in response to changes in their business practices, such as if they start collecting new types of personal data or changing the way they process personal data.
- **Changes in technology**: Advances in technology can also impact the way that organizations collect, use, and store personal data, and organizations need to update their data privacy policy to reflect these changes.

Overall, it is vital for organizations to regularly update their data privacy policy to ensure that it remains current and compliant with relevant data privacy laws and regulations and to protect the personal data of individuals.

b. Process for updating the policy:

When updating a data privacy policy, organizations must follow a clear and structured process to ensure that the policy remains current and compliant with relevant data privacy laws and regulations [141]. Some possible steps that organizations may follow in updating their policy may include:

- **Identifying changes:** The first step in updating a data privacy policy is to identify any changes that need to be made. This may involve reviewing the policy regularly to identify any areas that need to be updated and staying up to date with changes in data privacy laws and regulations and any changes in the organization's business practices or use of technology.
- **Assessing changes:** Once changes have been identified, organizations need to assess the impact of these changes on the policy and determine whether any updates are necessary. This may involve reviewing the procedure to ensure it is still relevant and compliant with the rules of applicable privacy laws and regulations and promptly making any changes required.
- **Consulting stakeholders:** It is also essential for organizations to consult with relevant stakeholders when updating their data privacy policy. This may include employees, customers, and other individuals whose personal data is collected and processed by the organization. Consulting with stakeholders can help to ensure that the policy reflects the needs and concerns of these individuals and can also help to build trust and confidence in the organization.

c. Notification of updates:

Organizations should specify how and when individuals will be notified of their data privacy policy updates. This will help to ensure transparency and accountability and to let individuals know about any changes that may affect their personal data.

There are several ways that organizations may choose to notify individuals of updates to their data privacy policy, including:

- **Email:** One option for organizations is to use email to notify individuals of updates to their policies. This can be an effective way to reach a large number of people quickly and efficiently and can be easily automated using email marketing software or other tools.
- **Website:** Organizations may also use their website to notify individuals of their data privacy policy updates. This could involve posting a notice on the homepage or other prominent locations or linking to the updated policy from relevant pages.
- **Other means:** In addition to email and the organization's website, there may be other means by which organizations can notify individuals of updates to their data privacy policy. For example, they may use social media, print materials, or other forms of communication to reach individuals.

d. Effective date of updates:

Organizations should specify the effective date of any updates to their data privacy policy. This will help to ensure that individuals are aware of when the updates will take effect and can help to ensure compliance with relevant data privacy laws and regulations.

There are several factors that organizations may need to consider when specifying the effective date of updates to their data privacy policy, including:

- **Legal requirements:** Some data privacy laws and regulations may require organizations to specify the effective date of updates to their policy.
- **Best practice:** Even if there are no legal requirements to specify the effective date of updates to a data privacy policy, it may be good practice to do so to ensure transparency and accountability. This can help build trust and confidence in the organization and help ensure that individuals know when the updates will take effect.

5.10. Effective date and acceptance of the policy

5.10.1. Date the policy takes effect:

It is essential to include the date the procedure takes effect to establish when the policy will be binding on the organization and individuals [142]. The following elements can be formed about the effective date of the process:

a. Explanation of the effective date:

Organizations must clearly explain the date their data privacy policy takes effect and how it will be applied. This will help to ensure transparency and accountability and to let individuals know when the policy will be in force and how it will affect them.

There are several factors that organizations need to consider when explaining the date that their data privacy policy takes effect, including:

- **The date of the policy:** Organizations should clearly state the date that their data privacy policy takes effect. This may be the date that the policy was first published, or it may be later if the policy has been updated.
- **How the policy will be applied:** Organizations should also explain how their data privacy policy will be applied. This may involve specifying the types of personal data covered by the procedure, the purposes for which the personal data will be used in blockchain, and the rights of individuals regarding their personal data.

b. Relationship to other policies:

Organizations are to specify the relationship of the effective date of their data privacy policy to any other policies that may be in place. This will help to ensure clarity and consistency and to let individuals know how the new policy will interact with any other policies that may be relevant.

There are several ways that organizations may choose to specify the relationship of the effective date of their data privacy policy to any other policies that may be in place, including:

- **Superseding other policies:** If the new data privacy policy is intended to supersede any other policies that may be in place, this should be clearly stated in the policy. This will help to ensure that individuals are aware that the new policy takes precedence over any other policies that may be relevant.
- **Replacing other policies:** If the new data privacy policy is intended to replace any other policies that may be in place, this should also be clearly stated in the policy. This will help to ensure that individuals are aware that the new policy will be the only policy that applies and that any other policies that may be relevant are no longer in force.
- **Complementing other policies:** In some cases, the new data privacy policy may be intended to complement any other policies that may be in place rather than replacing or superseding them. In this case, the relationship between the new policy and any other policies should be clearly explained in the procedure to ensure clarity and consistency.

c. Notification of the effective date:

Organizations should specify how and when individuals will be notified of the effective date of their data privacy policy. This will help to ensure that individuals are aware of when the procedure will take effect and can help to ensure compliance with relevant data privacy laws and regulations. There are several ways that organizations may choose to notify individuals of the effective date of their data privacy policy, including:

- **Email:** Organizations may choose to notify individuals of the effective date of their data privacy policy by sending an email to the individuals' registered email addresses. This can be an effective way to reach a large number of individuals quickly and efficiently.
- **Website:** Organizations may also choose to notify individuals of the effective date of their data privacy policy by posting a notice on their website. This can effectively reach a broad audience and is particularly useful if the organization has many online users.
- **Other means:** In addition to email and website notifications, organizations may also choose to notify individuals of the effective date of their data privacy policy through other means, such as by mail, phone, or in person. This can be particularly useful for organizations with a smaller number of users or organizations with a more personal relationship with their users.

5.10.2. Acceptance of the policy by the user:

It is essential to include a mechanism for individuals to accept the procedure to establish their agreement to be bound by its terms. The following elements can be formed about the acceptance of the policy by users:

a. Explanation of acceptance:

Organizations should clearly explain how individuals can accept their data privacy policy and the consequences of their acceptance. This will help to ensure that individuals are aware of their rights and obligations under the policy and can help to ensure compliance with relevant data privacy laws and regulations.

There are several ways that organizations may choose to explain how individuals can accept their data privacy policy, including:

- **Online acceptance**: Many organizations may allow individuals to accept their data privacy policy online, either through a form or by clicking on an "I agree" or similar button. This can be an efficient way to obtain acceptance and is particularly useful for organizations with many online users.

- **In-person acceptance:** In some cases, organizations may require individuals to accept their data privacy policy in person, either through a written signature or verbal agreement. This can be particularly useful for organizations with a more personal relationship with their users or with smaller users.
- **Implied acceptance:** In some cases, organizations may infer acceptance of their data privacy policy based on an individual's use of the organization's services or products. For example, an individual may be deemed to have accepted the policy if they continue to use the organization's services or products after being notified of the policy.

This will help to ensure that individuals are aware of their rights and obligations under the policy and can help to ensure compliance with relevant data privacy laws and regulations.

b. Methods of acceptance:

There are several methods that individuals can use to accept a data privacy policy, including:

- **Online acceptance:** Many organizations may allow individuals to accept their data privacy policy online, either through a form or by clicking on an "I agree" or similar button. This can be an efficient way to obtain acceptance and is particularly useful for organizations with many online users.
- **Physical acceptance:** In some cases, organizations may require individuals to accept their data privacy policy by signing a physical copy. This can be particularly useful for organizations with a more personal relationship with their users or with smaller users.
- **Oral acceptance:** In some cases, organizations may accept oral consent from individuals to accept their data privacy policy. This can be particularly useful for organizations with a more personal relationship with their users or with smaller users.
- **Written acceptance:** In some cases, organizations may accept written consent from individuals to accept their data privacy policy. This can be particularly useful for organizations with a more formal relationship with their users or organizations with more users.

c. Rejection of the policy:

If an individual does not accept a data privacy policy, it is up to the organization to determine the consequences of this non-acceptance. Some possible consequences could include the following:

- **Inability to use the service or application:** An organization may sometimes require individuals to accept their data privacy policy to use their services or products. If an individual does not get the procedure, they may be unable to use the service or application.

- **Limited access to certain features:** An organization may sometimes allow individuals to use their service or application without accepting the data privacy policy. However, it may limit their access to certain features or functionality once they get the procedure.
- **Termination of the service or application:** In some cases, an organization may terminate an individual's access to their service or application if they do not accept the data privacy policy.

d. Record of acceptance:

Organizations to specify how long they will keep a record of an individual's acceptance of their data privacy policy to ensure compliance with relevant blockchain data privacy laws and regulations and to demonstrate that they have obtained appropriate consent from their users. Some possible options for keeping a record of acceptance could include the following:

- **Online acceptance:** If individuals accept the data privacy policy online, the organization can keep a record of this acceptance by storing a copy of the acceptance form or the date and time the individual clicked on the "I agree" button. These records should be stored securely to protect the individual's privacy.
- **Physical acceptance:** If individuals accept the data privacy policy by signing a physical copy, the organization can keep a copy of the signed policy on file. These copies should be stored securely to protect the privacy of the individual.
- **Oral acceptance:** If individuals accept the data privacy policy orally, the organization should make a written record of this acceptance, including the date and time of the acceptance, the individual's name, and any relevant details of the conversation. These records should be stored securely to protect the individual's privacy.
- **Written acceptance:** If individuals accept the data privacy policy in writing, the organization should keep a copy of the written approval. These copies should be stored securely to protect the privacy of the individual.

Chapter 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

This research paper on blockchain user data privacy policy has highlighted the importance of protecting user privacy and security. By examining the current regulatory landscape and identifying key challenges, the paper has provided practical recommendations for policymakers, developers, and other stakeholders to ensure that blockchain technology is used in a way that respects user privacy. The paper has emphasized the need for privacy-preserving mechanisms, governance frameworks, and user education and awareness. It has called for ongoing research into emerging technologies and their impact on blockchain user data privacy policy. This paper aims to contribute to the ongoing blockchain user data privacy policy discussion and inspire further research and innovation in this important area.

6.2 Future Work

Several areas of future research could be explored to improve user data privacy policies for blockchain systems:

6.2.1. Blockchain governance frameworks: One area of research could be focused on developing governance frameworks for blockchain networks that incorporate privacy considerations. This could involve examining the governance structures of existing blockchain networks and identifying best practices for integrating privacy into these frameworks.

6.2.2. Regulatory compliance: Given the rapidly evolving regulatory landscape governing data privacy and security, there is a need for ongoing research into the regulatory requirements for blockchain networks. This could involve examining the regulatory frameworks in different jurisdictions and identifying best practices for compliance.

6.2.3. User awareness and education: As blockchain networks become more widespread, users need to be educated on the importance of data privacy and security. Future research could focus on developing effective user education and awareness campaigns to help users understand the risks associated with sharing data on the blockchain and how to protect their privacy.

6.2.4. Impact of emerging technologies: Finally, as emerging technologies such as artificial intelligence, the Internet of Things, and 5G networks become more prevalent, there is a need to examine the impact of these technologies on blockchain user data privacy policy. This could involve exploring the potential risks associated with the integration of these technologies into blockchain networks and identifying best practices for mitigating these risks.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9, 2008.

[2] "EU General Data Protection Regulation (GDPR)," *Official Journal of the European Union,,* p. L119/1, 2016.

[3] "California Consumer Privacy Act (CCPA)," *, California Legislative Information,* 2018..

[4] "Australian Privacy Act," *Australian Government,* 1988.

[5] S. Aggarwal and N. Kumar, "History of blockchain-Blockchain 1.0: Currency," in *Advances in Computers*, vol. 121, S. Aggarwal, N. Kumar and P. Raj, Eds., Elsevier, 2021, p. 147–169.

[6] S. Aggarwal and N. Kumar, "Blockchain 2.0: Smart contracts," in *Advances in Computers*, vol. 121, S. Aggarwal, N. Kumar and P. Raj, Eds., Elsevier, 2021, p. 301–322.

[7] V. Dhillon, D. Metcalf and M. Hooper, "Blockchain 3.0," in *Blockchain Enabled Applications*, Berkeley, CA: Apress, 2021, p. 247–288.

[8] A. G. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz and T. M. Alam, "A journey of WEB and Blockchain towards the Industry 4.0: An Overview," in *2019 International Conference on Innovative Computing (ICIC)*, 2019.

[9] P. K. Paul, "Blockchain Technology and its Types—A Short Review," *Int. J. Appl. Sci. Eng.,* vol. 9, 2021.

[10] C. Chen, S. B. Goyal and K. Ramaswamy, "BSPPF: Blockchain-based security and privacy preventing framework for Data Middle Platform in the era of IR 4.0," *J. Nanomater.,* vol. 2022, p. 1–14, 2022.

[11] D. Guegan, "Public blockchain versus private blockhain," 2017.

[12] R. Lai and D. LEE Kuo Chuen, "Blockchain – from public to private," in *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, Elsevier, 2018, p. 145–177.

[13] R. Stephen and A. Alex, "A Review on BlockChain Security," *IOP Conf. Ser. Mater. Sci. Eng.,* vol. 396, p. 012030, 2018.

[14] G. Vizier and V. Gramoli, "ComChain: Bridging the gap between public and consortium blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018.

[15] C. Xu, Z. Li and Q. Yu, "CFAC: An approach of chaincodes firewall combining access control in consortium blockchain," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, 2020.

[16] S. Li, Q. Xu, P. Hou, X. Chen, Y. Wang, H. Zhang and G. Rong, "Exploring the challenges of developing and operating consortium blockchains: A case study," in *Proceedings of the Evaluation and Assessment in Software Engineering*, New York, NY, USA, 2020.

[17] S. Zhu, H. Hu, Y. Li and W. Li, "Hybrid blockchain design for privacy preserving crowdsourcing platform," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019.

[18] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 2016.

[19] S. Johnson, P. Robinson and J. Brainard, "Sidechains and interoperability," 2019.

[20] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.,* vol. 149, p. 102471, 2020.

[21] C. Sguanci, R. Spatafora and A. M. Vergani, "Layer 2 Blockchain Scaling: a Survey," 2021.

[22] J. Abou Jaoude and R. George Saade, "Blockchain Applications – Usage in Different Domains," *IEEE Access,* vol. 7, p. 45360–45381, 2019.

[23] F. A. Sunny, P. Hajek, M. Munk, M. Z. Abedin, M. S. Satu, M. I. A. Efat and M. J. Islam, "A systematic review of blockchain applications," *IEEE Access,* vol. 10, p. 59155–59177, 2022.

[24] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications,* vol. 3, p. 100067, 2022.

[25] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta and B. Kang, "A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future," *IEEE Access,* vol. 7, p. 75845–75872, 2019.

[26] I. Homoliak, S. Venugopalan, Q. Hum and P. Szalachowski, "A Security Reference Architecture for Blockchains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019.

[27] S. Bansod and L. Ragha, "Challenges in making blockchain privacy compliant for the digital world: some measures," *Sadhana,* vol. 47, 2022.

[28] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access,* vol. 7, p. 164908–164940, 2019.

[29] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula and Z. Cai, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," *High-Confidence Computing,* vol. 2, p. 100048, 2022.

[30] T. T. Huynh, T. D. Nguyen and H. Tan, "A survey on security and privacy issues of blockchain technology," in *2019 International Conference on System Science and Engineering (ICSSE)*, 2019.

[31] Ihab, N. Ramadan and H. Ahmed, "Cybersecurity Risks of Blockchain Technology," *Int. J. Comput. Appl.,* vol. 177, p. 8–14, 2020.

[32] N. Gupta, "A deep dive into security and privacy issues of blockchain technologies," in *Handbook of Research on Blockchain Technology*, Elsevier, 2020, p. 95–112.

[33] *CCPA.*

[34] Office for Civil Rights (OCR), *The HIPAA privacy rule,* US Department of Health and Human Services, 2008.

[35] *Official PCI security standards council site,* 2022.

[36] Office of the Privacy Commissioner of Canada, *The personal information protection and electronic documents act (PIPEDA),* 2021.

[37] *Republic of South Africa,* 2013.

[38] *Data protection laws - The Official Portal of the UAE Government.*

[39] *Data protection,* 2011.

[40] *تفاصيل النظام.*

[41] "The principles," 2022.

[42] J. Dennis, *Comparing privacy laws: GDPR v. CCPA & CPRA.*

[43] P.-C. Chen, T.-H. Kuo and J.-L. Wu, "A study of the applicability of ideal lattice-based fully homomorphic encryption scheme to ethereum blockchain," *IEEE Syst. J.,* vol. 15, p. 1528–1539, 2021.

[44] C. Regueiro, I. Seco, S. de Diego, O. Lage and L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," *Inf. Process. Manag.,* vol. 58, p. 102745, 2021.

[45] R. K. Raman, R. Vaculin, M. Hind, S. L. Remy, E. K. Pissadaki, N. K. Bore, R. Daneshvar, B. Srivastava and K. R. Varshney, "Trusted multi-party computation and verifiable simulations: A scalable blockchain approach," 2018.

[46] H. Zhong, Y. Sang, Y. Zhang and Z. Xi, "Secure multi-party computation on blockchain: An overview," in *Parallel Architectures, Algorithms and Programming*, Singapore, Springer Singapore, 2020, p. 452–460.

[47] J. Zhou, Y. Feng, Z. Wang and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors (Basel),* vol. 21, p. 1540, 2021.

[48] A. Mühle, A. Grüner, T. Gayvoronskaya and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.,* vol. 30, p. 80–86, 2018.

[49] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, New York, NY, USA, 2020.

[50] R. Mercer, "Privacy on the Blockchain: Unique Ring Signatures," 2016.

[51] X. Li, Y. Mei, J. Gong, F. Xiang and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access,* vol. 8, p. 76765–76772, 2020.

[52] G. Yu, "Blockchain stealth address schemes," *Cryptology ePrint Archive,* 2020.

[53] J. Fan, Z. Wang, Y. Luo, J. Bai, Y. Li and Y. Hao, "A new stealth address scheme for blockchain," in *Proceedings of the ACM Turing Celebration Conference - China*, New York, NY, USA, 2019.

[54] M. M. H. Onik, C.-S. Kim, N.-Y. Lee and J. Yang, "Privacy-aware blockchain for personal data sharing and tracking," *Open Comput. Sci.,* vol. 9, p. 80–91, 2019.

[55] E. McCallister, T. Grance and K. A. Scarfone, "Guide to protecting the confidentiality of Personally Identifiable Information (PII)," National Institute of Standards and Technology, Gaithersburg, 2010.

[56] *What personal data is considered sensitive?.*

[57] *What is valid consent?,* 2022.

[58] *Art. 7 GDPR – Conditions for consent - general data protection regulation (GDPR).*

[59] Office of the Privacy Commissioner of Canada, *Consent and privacy*, 2016.

[60] *Art. 9 GDPR – Processing of special categories of personal data - General Data Protection Regulation (GDPR).*

[61] *Children,* 2022.

[62] *Sensitive personal data.*

[63] *Art. 14 GDPR – Information to be provided where personal data have not been obtained from the data subject - General Data Protection Regulation (GDPR).*

[64] *Art. 13 GDPR – Information to be provided where personal data are collected from the data subject - General Data Protection Regulation (GDPR).*

[65] *Blockchain Explained: How does a transaction get into the blockchain?.*

[66] *Consent - General Data Protection Regulation (GDPR).*

[67] *Principle (a): Lawfulness, fairness and transparency*, 2022.

[68] *Principle (b): Purpose limitation,* 2022.

[69] *1798.135 – Opt out link,* 2020.

[70] *Guidelines 05/2020 on consent under regulation 2016/679.*

[71] *CPRA Data Retention.*

[72] *GDPR Data Retention Policy.*

[73] *Bill Text - AB-375 Privacy: personal information: businesses (1798.100.).*

[74] B. Wolford, *Art. 17 GDPR - Right to erasure ('right to be forgotten'),* 2018.

[75] *Deletion Requests – the right to be forgotten (sometimes called the right of erasure or the right to deletion),* 2020.

[76] L. Guo, H. Xie and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," *J. Vis. Commun. Image Represent.,* vol. 70, p. 102741, 2020.

[77] D. Di Francesco Maesa, P. Mori and L. Ricci, "A blockchain based approach for the definition of auditable Access Control systems," *Comput. Secur.,* vol. 84, p. 93–119, 2019.

[78] W.-S. Park, D.-Y. Hwang and K.-H. Kim, "A TOTP-based two factor authentication scheme for hyperledger fabric blockchain," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018.

[79] *Principle (c): Data minimisation,* 2022.

[80] *Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR).*

[81] K. kiener-manu, *Cybercrime module 10 key issues: Data breach notification laws.*

[82] *Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.*

[83] *Data breach response: A guide for business,* 2019.

[84] *Personal data breaches,* 2023.

[85] *Part 3: Responding to data breaches — four key steps.*

[86] *Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR).*

[87] *Art. 34 GDPR – Communication of a personal data breach to the data subject - General Data Protection Regulation (GDPR).*

[88] *Data breach notification laws by state.*

[89] *Art. 15 GDPR – Right of access by the data subject - General Data Protection Regulation (GDPR).*

[90] *California consumer privacy act (CcpA) practical guide.*

[91] A. Baig, *Data Subject Access Request (DSAR) – all you need to know,* 2022.

[92] *Data subject access requests.*

[93] *Time limits for responding to data protection rights requests,* 2020.

[94] *A DSAR Comparison Between GDPR and CCPA- Timing for Compliance?.*

[95] *Access exceptions.*

[96] *Are there any exceptions?,* 2022.

[97] Professor United States Congress and United States House of Representatives and Committee on Transportat Infrastructure, What will it cost?: Protecting the taxpayer from an unachievable coast guard acquisition program, North, Charleston: Createspace Independent Publishing Platform, 2017.

[98] *PHIA Fee Fact Sheet.*

[99] D. Dimitrova, "The rise of the personal data quality principle. Is it legal and does it have an impact on the right to rectification?," *SSRN Electron. J.,* 2021.

[100] *Art. 16 GDPR – right to rectification - general data protection regulation (GDPR).*

[101] D. Song and M. Yuan, "An improved method for data storage based on blockchain smart contract," in *Machine Learning for Cyber Security*, Cham, Springer International Publishing, 2020, p. 447–460.

[102] J. Eberhardt and S. Tai, "On or off the blockchain? Insights on off-chaining computation and data," in *Service-Oriented and Cloud Computing*, Springer International Publishing, 2017, pp. 3-15.

[103] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration," *it - Information Technology,* vol. 60, no. 5-6, pp. 283-291, 2018.

[104] H. Huang, X. Chen and J. Wang, "Blockchain-based multiple groups data sharing with anonymity and traceability," *Science China Information Sciences,* vol. 63, no. 3, 2020.

[105] Q. An, Y. Zhang, C. Guo, X. Liu, J. Huang, W. Zhang, S. Zhang, C. Zhan and Y. Cai, "Anonymous traceability protocol based on group signature for blockchain," *Security and communication networks,* vol. 2022, pp. 1-10, 2022.

[106] *Data rectification requests.*

[107] *Exercise Your Rights – Article 16 GDPR – Correct inaccurate data!.*

[108] *knowyourprivacyrights.*

[109] B. Trojanowski, *Limitation of the right to request the erasure of personal data in the context of sacramental matters and canonical status in the Catholic Church in Poland,* 2022.

[110] G. A. Brown, *Consumers' ``right to delete'' under US state privacy laws,* 2021.

[111] H.-H. Herrnfeld, "Article 61 Right to rectification or erasure of operational personal data and restriction of data processing," in *European Public Prosecutor's Office*, Nomos Verlagsgesellschaft mbH & Co. KG, 2021, p. 499–504.

[112] M. Florian, S. Henningsen, S. Beaucamp and B. Scheuermann, "Erasing data from blockchain nodes," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2019.

[113] B. Wolford, *Art. 18 GDPR - Right to restriction of processing,* 2018.

[114] *What data can we process and under which conditions?.*

[115] *Art. 20 GDPR – Right to data portability - General Data Protection Regulation (GDPR).*

[116] M. Yuan, "Research on the right of data portability based on regional type and its impact on the credit reporting industry," *BCP Business & Management,* vol. 26, p. 1203–1209, 2022.

[117] *Art. 28 GDPR – processor - general data protection Regulation (GDPR).*

[118] *What are `controllers' and `processors'?,* 2022.

[119] *What responsibilities and liabilities do controllers have when using a processor?,* 2022.

[120] D. Gabel and T. Hickman, *Chapter 11: Obligations of processors – unlocking the EU general data protection regulation,* White & Case.

[121] *Contracts between data controllers and data processors.*

[122] B. Wolford, *Data Protection Impact Assessment (DPIA),* 2018.

[123] N. Jones, "The who, what, why and when of data protection impact assessments," *Comput. Fraud Secur.,* vol. 2022, 2022.

[124] S. A. Sultan, *The ultimate guide to privacy impact assessments for CPRA,* 2022.

[125] B. Wolford, *Recital 91 - Necessity of a data protection impact assessment,* 2018.

[126] *Comparing the data protection assessment requirements across the next generation of U.s. state privacy laws.*

[127] *Art. 35 GDPR – Data protection impact assessment - General Data Protection Regulation (GDPR).*

[128] *How do we do a DPIA?,* 2022.

[129] *Procedure for conducting Data Protection Impact Assessments.*

[130] C. Woollven, *7 key stages of the data protection impact assessment (DPIA),* IT Governance, 2021.

[131] A. Mladinić, L. Puljak and Z. Koporc, "Corrigendum to: Post-GDPR survey of data protection officers in research and non-research institutions in Croatia: a cross-sectional study," *Biochem. Med. (Zagreb),* vol. 32, p. 021201, 2022.

[132] *Art. 37 GDPR – Designation of the data protection officer - General Data Protection Regulation (GDPR).*

[133] *Fines / penalties - General Data Protection Regulation (GDPR).*

[134] A. Baig, *Fines & penalties for non-compliance with the CCPA,* 2022.

[135] *Chapter 7: Civil penalties — serious or repeated interference with privacy and other penalty provisions.*

[136] *Art. 77 GDPR – Right to lodge a complaint with a supervisory authority - General Data Protection Regulation (GDPR).*

[137] *Chapter 1: Privacy complaint handling process.*

[138] *Protocol for handling privacy complaints.*

[139] *Chapter 1: Privacy complaint handling process.*

[140] "When to Update Your Privacy Policy," [Online]. Available: https://www.contractscounsel.com/b/when-to-update-your-privacy-policy.

[141] T. Peterson, *When and how to update your company's privacy policy,* Legalzoom.com, 2019.

[142] B. Wolford, *Writing a GDPR-compliant privacy notice (template included),* 2018.