Enterprise-Grade Security in Public Blockchain Networks

Amar Čolaković[1] and Angela Popa[1]

[1]LogosLabs [logoslabs.io]

Release History

Version	Date	Changes
0.1.0	June, 30 2024	Initial draft of the paper, including the introduction and case study analysis

Abstract

This research paper examines enterprise-grade security in public blockchain networks. The study aims to address critical security and privacy challenges in blockchain-based environments, particularly where robust security measures are paramount. Through a comprehensive analysis of current security protocols, models, and solutions, this research provides insights into effective strategies for safeguarding public blockchain networks. The findings highlight the necessity of integrating these security principles to develop solutions that enhance the overall resilience and reliability of public blockchain networks.

Contents

1 Introduction

The focus of this research is to analyze how security is managed in public blockchain networks, with an emphasis on techniques that enable high-level security and privacy. The findings provides implementation possibilities, demonstrating practical methods and strategies for integrating security and privacy techniques into existing and new blockchain infrastructures. Each blockchain network typically employs a unique security model, generally comprising various critical components, including *cryptographic mechanisms*, *consensus algorithms*, *network security protocols*, *identity and access management*, *verification and auditing processes*, *privacy measures*, *isolated execution environments*, *monitoring and response systems*, and *regulatory compliance strategies*.

In this research paper, we conduct a detailed examination of previously mentioned aspects to develop a complete solution that enables private and hybrid blockchain networks to be operated securely and "entirely" trustless by the public participants. The objective is to formulate robust strategies and implementation methodologies that ensure the security and integrity of public blockchain networks. This includes maintaining transparency and trustlessness, even when these networks are publicly provisioned, thereby enhancing their overall reliability and adoption.

The research itself focuses on general aspects of security in public blockchain networks. However, the proposed solution (findings section) and the subsequent implementation of recommended practices will be integrated into the Substrate framework. This will enable a security model that can be specifically implemented for Substrate-based chains. While the security model can, in general terms, be applicable across various frameworks, our primary focus will be on its implementation within Substrate. The decision to use Substrate for the implementation is driven by its modular architecture and its capability for forkless updates. These features allow the system to integrate new functionalities over time and simplify updates of the network. Forkless updates are essential in blockchain systems because they allow quick mitigation's of vulnerabilities, ensuring the system remains secure without requiring disruptive hard forks.

A security system that does not implement principles of *zero-trust*, *zero-knowledge*, and *zero-tolerance* cannot provide complete security. Each of these principles plays a crucial role in ensuring robust security measures: zero-trust assumes no implicit trust in any network component, zero-knowledge ensures privacy through cryptographic proofs without revealing data, and zero-tolerance mandates strict enforcement of security policies. Our approach is to "fully" integrate these principles, thereby achieving a comprehensive and robust security model. [16]

An enterprise-grade security model aims to ensure the highest security standards to effectively counteract threats. Key differentiators of an enterprise-grade solution include scalability to handle large volumes of data, advanced threat detection and mitigation, compliance with legal and regulatory requirements, ensuring data integrity and availability. Enterprise blockchains generally considered, theoretically do not fully align with the Web3 approach, as their implementations often rely on private validators and centralized control. This contradicts the principles of decentralization that characterize Web3. Implementing an enterprise-grade security *trustless solution* can make public governed blockchains more robust, trustworthy, and resilient against threats, which is crucial for the general long-term adoption and use of blockchain technology.

1.1 Motivation

Security in blockchain networks is one of the most crucial factors for the broader adoption of blockchain solutions. Most public blockchain platforms are rarely used for real enterprise solutions because private blockchain platforms (such as IBM Blockchain Platform, R3 Corda Enterprise, Kaleido, Azure Workbench, etc.) are generally perceived as more secure and are utilized for many applications in enterprise sector. One of the key differentiating factors is the enterprise-grade security and privacy. While public blockchain platforms offer a certain level of security and privacy, they are often not suitable for many use cases that require a higher degree of protection. Enterprise blockchain platforms typically come with higher costs, making migration unaffordable for many Web2 services. Public blockchain platforms are more cost-effective but are often viewed as not equally secure.

The possibility of providing a fully community-operated blockchain infrastructure, where completely private services with high-security requirements can be run, would present a viable path for migrating from Web2 to Web3. This approach can enable for example services from various sectors such as public transportation, communal services, educational institutions, and cultural institutions to be operated and governed by the community, advancing the migration to Web3. The implementation of private elements in a public blockchain network aims to balance transparency and data

privacy, ensuring that data can be handled securely and privately even in a publicly provisioned infrastructure.

The primary reason for this research is the provision of the *Logos network* [8] and its resulting *sub0layer* [3]. The approach is to provide a community enterprise grade computation and storage solution (DePin - Decentralized Physical Infrastructure Network) for the general Web3 core infrastructure, this means that a blockchain network (*Logo Chain* in our case) must contain private elements but can still be operated securely by the community. The security and privacy requirements that such a network entails will be further discussed in Chapter 2, Case Study, where the specific requirements will be addressed in detail.

Our primary driving factor is to enable the provision of resources and infrastructure for Web3 through a community-driven, secure, and trustless model by implementing new security principles. This approach adheres to the true ethos of Web3, ensuring that no private parties (e.g., private validators) centralize the network or undermine its trustless nature.

1.2 Document Structure

The research paper is structured for staged release to facilitate a thorough and focused investigation of security in blockchain networks by segmenting it into distinct fields. This approach allows each field to be independently researched in depth, ensuring comprehensive analysis and valuable solution proposals for specific subjects. The research, findings, and solution proposals for the individual research fields will be documented and released incrementally in this paper. Once all aspects are defined and specified, a final version 1.0 will be published.

By addressing individual topics separately, the findings and forthcoming implementations can be provided independently. Similar to the Substrate ecosystem, where functionalities are delivered through specific modules known as pallets, this approach allows for a high level of agility. This means that research and development in fields such as identity, access control, and key management can occur initially and independently, while other areas like consensus mechanisms or network security can be addressed subsequently or concurrently.

It is important to emphasize that this separation is feasible because the core requirements or rules are clearly defined, and each implementation area must adhere to these primary requirements.

The paper is divided into six main chapters. The first chapter (Introduction) provides an overview of the topics covered and the motivations driving this research. In the second chapter (Case Study), we define the primary requirements of a secure public blockchain network that demands full zero-trust principles. In this section, we also divide the security into separate security fields according to the specific areas they address.

Chapters 3, 4, and 5 are subdivided according to the defined security sections in Chapter 2. The third chapter (Theoretical Foundations) examines current solutions and implementations for each defined section of the security. In Chapter 4 (Findings), we present the results and potential implementations and propose a security model. Chapter 5 (Discussion) explains the significance of the achieved results and how they should be interpreted in relation to existing solutions.

The final chapter (Conclusion) summarizes the key findings of the study and emphasizes the main contributions of the research to the field. Additionally, it discusses potential practical applications of the research findings. The paper concludes with a bibliography and a glossary of key terms related to the research.

2 Case Study

The study fundamentally adheres to the requirements for providing a publicly provisioned blockchain infrastructure that delivers security, privacy, and efficiency at an enterprise-grade level. The Logos Blockchain (primary reason for the research) is designed specifically for certain use cases rather than being a general-purpose blockchain. However, the security model that will be implemented in the Logos chain, and presented in detail in this study, especially in section 4 (Findings), can possibly be applicable to other blockchain frameworks. The findings primarily present the core principles and methodologies that can be adapted to enhance the security and performance of blockchain systems generally, before presenting the possible substrate-based solution.

In this section (case study), the description of the case is outlined. First we define the general security aspects of a Blockchain network. In Section 2.2 (Requirements), the general security requirements for an enterprise-grade blockchain infrastructure are presented. This leads to Section 2.3 (Specifications), where this requirements are clearly specified and defined to create a comprehensive picture of what an enterprise-grade security model demands in terms of security and privacy.

2.1 Definition

This research primarily focuses on the security and privacy aspects of a blockchain network[2], it does not delve into aspects such as scalability, network performance, upgrade and maintenance capability, etc. These aspects will be addressed in a separate research project, focusing on achieving optimal efficiency in a distributed system like blockchain.

We define here the "general security" in a blockchain network. For practical purposes, we designate it here as a *general security model* and categorize it into four distinct sections. As elaborated in Chapter 1.2, this segmentation also streamlines the research of individual sections and the development of solution approaches independently, but they will must adhere to predefined fundamental network rules as they pertain to the entire system. It is important to note that although the segmentation of security provides a certain structure, it must be acknowledged that these sections intersect. Generally, we define the security characteristics (general security model) of a blockchain network as follows.

- **Identities, Access Control and Key Management:**[1][9][13][6] In blockchain systems, identity management, access controls, and key management are central security aspects. Generally an *identity* is represented by an *account*, secured by a key pair consisting of a *public and a private key*. The private key signs transactions, while the public key serves for identification within the network. Managing these keys includes secure creation, storage, and recovery. In addition to regular user accounts, there are also *technical or service accounts* used for specific tasks or *privileged operations*, such as smart contracts or oracles. These accounts often have special rights and access levels and are frequently protected by Hardware Security Modules (HSMs). An important concept are *session keys* (substrate term), which are temporary key pairs employed by validators. These keys are rotated regularly to enhance security and minimize the risk of long-term key compromises. Session keys enable validators to efficiently handle various critical tasks such as signing blocks and secure network communication. *Access controls* ensure that only authorized entities can access specific functions and data. Most modern frameworks typically offer the flexibility to implement customized *role-based or attribute-based access control mechanisms*, although these mechanisms are not necessarily provided natively.

- **Cryptographic Mechanisms and Data Privacy:**[11][17] In blockchain systems generally, cryptographic mechanisms and data privacy are fundamental elements that ensure the security and confidentiality of data. Cryptographic algorithms such as *SHA-256, Blake2b, and elliptic curve cryptography (ECC) (e.g. sr25519; ed25519)* are utilized to ensure data integrity and authenticity. Hash functions like SHA-256 generate unique, immutable checksums for data, making any manipulation immediately detectable. ECC is used to create secure key pairs and digital signatures that authenticate transactions and protect against unauthorized modifications. In blockchains, these cryptographic mechanisms are closely tied to account management. As each *account is secured by a key pair* consisting of a public and a private key. In addition to fundamental cryptographic mechanisms, there is increasing work on advanced techniques such as *Zero-Knowledge Proofs (ZKPs)*. ZKPs allow the verification of the validity of information without revealing the information itself, significantly enhancing user privacy. *Encryption* also plays a central role in *data privacy*. Data stored on the blockchain can be protected using encryption techniques to ensure that only authorized parties have access to sensitive information. Various encryption methods can be applied to secure both data in "transit" and data at "rest".

- **Consensus Mechanisms and Network Security:**[10][20] In blockchain systems, consensus mechanisms and network security are crucial for ensuring the integrity and availability of the network. Consensus mechanisms determine how transactions are validated and new blocks are added to the blockchain. Frameworks typically support various consensus algorithms such as *Proof of Stake (PoS), Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT)*, etc. There is also a interesting specific variant of PoS called *Nominated Proof of Stake (NPoS)*. NPoS is based on the principle that validators are elected by nominators who stake their tokens. This promotes decentralization and ensures that only trusted validators can create blocks. A critical security risk in blockchain systems is the *51% attack*. In a 51% attack, a single entity or a coalition controls the majority of the network's hashrate (in Proof of Work) or staked tokens (in Proof of Stake). This allows them to manipulate transactions, perform double-spending, and censor or rewrite new blocks. This risk is mitigated by NPoS, where the selection and monitoring of validators are carried out by a broad community of nominators, making it difficult and costly to gain control over the network due to the involvement of multiple

stakeholders. Proof of Authority (PoA), for example, relies on a limited number of trusted validators who are authorized based on their identity and reputation. While PoA enables high speed and efficiency, it is less relevant for a public blockchains as it relies on trust in private parties. From the aforementioned example (NPos), the importance of consensus mechanisms in a blockchain network becomes clearly evident. In addition to consensus mechanisms, network security plays a central role. Network security measures include protection against *Distributed Denial of Service (DDoS) attacks, Sybil attacks*, and other malicious activities. Networks implements mechanisms such as peer authentication, network segmentation, and the use of secure communication protocols like *Transport Layer Security (TLS)* to ensure the integrity and confidentiality of data transmission.

- **Auditing, Policies and Regulations:**[7][13] In blockchain systems, auditing, policies, and regulations are crucial components to ensure transparency, compliance, and trust. Auditing involves the systematic review and analysis of blockchain transactions and activities to detect and prevent fraud, ensure data integrity, and verify compliance with relevant standards and regulations. Blockchain frameworks, including Substrate, provide tools and mechanisms to facilitate comprehensive auditing. These include immutable ledgers that record every transaction, cryptographic proofs that ensure the integrity of data, and smart contracts that can automate compliance checks and reporting. Auditors can leverage these features to conduct real-time audits, trace transactions, and verify the authenticity of data on the blockchain. Policies define the rules and guidelines that govern the operation and use of the blockchain network. These policies may cover various aspects such as access control, data privacy, transaction processing, and security measures. Policies can be implemented and enforced through on-chain governance mechanisms, allowing stakeholders to propose, vote on, and enact changes to the network's rules and parameters. Regulations refer to the legal and regulatory frameworks that blockchain networks must comply with. These may include data protection laws, financial regulations, anti-money laundering (AML) requirements, and other legal standards. Compliance with regulations is crucial for ensuring the legitimacy and acceptance of blockchain technology in various industries. Substrate's modular architecture allows developers to build compliance into their blockchain applications, ensuring that they meet the necessary regulatory requirements. Effective auditing, robust policies, and strict regulatory compliance are vital for maintaining the integrity, security, and trustworthiness of blockchain systems. By leveraging the these principles its possible to implement comprehensive auditing practices, establish clear policies, and ensure adherence to relevant regulations, thereby fostering a secure and transparent blockchain environment.

These are the fundamental elements that constitute security and privacy in a blockchain network. The area of isolated execution is not addressed in this research as it pertains to a specific field that requires separate consideration.

In this study, we specifically address the use case of private transactions without involving a closed consortium. Solutions that incorporate private validation parties are not considered. The aim is to define a system capable of handling private transactions without involving private parties, utilizing the highest security compliance and automation level. The next section outlines the general security and privacy requirements that such a blockchain network needs to achieve to reach the highest possible security grade.

2.2 Requirements

We have defined the "general security model" that represents the overall security of a blockchain system. Based on this general model, we go into specific areas and outline the general requirements for an enterprise-grade security system. Generally, this system must be capable of providing high levels of resilience and privacy using the principles of zero trust, zero knowledge, and zero tolerance. As an enterprise-grade system, it must be highly regulated and automated. We define the general requirements for a highly secure, community-provisioned, and governed blockchain system as follows.

- **Identities, Access Control and Key Management**[1][9][13][6]
  In an enterprise system, clearly defined identities are very important. All system accounts (*service and technical accounts*) must have a unique and verifiable identity to ensure trust within the network. Identities must be tied to specific roles within a network, such as admin, peer, client, etc., to control their access and actions. This simplifies management and ensures consistent application of access policies. The process of issuing and managing identities must

be secure to prevent unauthorized access and impersonation. The system must support the revocation of identities to ensure that compromised identities cannot be used.

Fine-grained control over access to resources is necessary to protect sensitive information and operations. This involves defining *Access Control Lists (ACLs)* that specify permissions for accessing resources. These ACLs must be capable of detailed specification, allowing policies to control access at the level of individual resources or actions. The system must allow for the creation, modification, and deletion of access control policies in real-time. This involves the ability to update ACLs, role definitions, access control rules, etc., as network needs evolve.

Keys (not public participants' keys) must be generated and stored in a secure environment to prevent unauthorized access. The system must employ *Hardware Security Modules (HSMs)* or equivalent secure storage solutions to protect private keys. Keys must be stored in a tamper-resistant environment to prevent extraction. Regularly rotating keys and revoking compromised keys is important to maintain ongoing security. This involves generating new keys, securely distributing them, and deprecating old keys without interrupting ongoing operations. These mechanisms must be in place to ensure that revoked keys cannot be used for further operations.

- **Cryptographic Mechanisms and Data Privacy**[11][17]
  Use of strong, standardized cryptographic algorithms to ensure the confidentiality, integrity, and authenticity of data is a fundamental element of security in general. The system must implement advanced cryptographic algorithms such as *AES (Advanced Encryption Standard)* for symmetric encryption, *RSA (Rivest-Shamir-Adleman)*, and *ECC (Elliptic Curve Cryptography)* for asymmetric encryption. Such algorithms are selected based on their proven security and efficiency. Standards from organizations like *ISO (International Organization for Standardization)*, *NIST (National Institute of Standards and Technology)*, and *CIS (Center for Internet Security)* must be followed to ensure compliance with industry best practices. The system must use cryptographic hash functions combined with digital signatures to verify the integrity and origin of data.

  The system should incorporate *Zero-Knowledge Proofs (ZKPs)* to allow one party to prove to another that a statement is true without revealing any additional information. Techniques such as *zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)* and *zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)* can be used. ZKPs are essential for scenarios where transaction details need to remain confidential while still ensuring the transaction's validity—in other words, the ability to perform private transactions with zero knowledge.

  Sensitive data stored on the blockchain must be encrypted. Encryption should be applied at rest and in transit to ensure that data remains confidential. Only authorized parties should have access to decryption keys, ensuring that sensitive data is protected even if the storage medium is compromised. *TLS* must be used to encrypt data in transit, ensuring that data exchanged between nodes is protected from eavesdropping and tampering. *Mutual TLS (mTLS)* can be implemented to authenticate both the client and server, enhancing security in communication. Techniques such as *pseudonymization* and *anonymization* must be employed to obscure *personally identifiable information (PII)*. This involves replacing sensitive data with pseudonyms or removing identifiable elements to protect user privacy while allowing data analysis and processing.

- **Consensus Mechanisms and Network Security**[10][20]
  The system must continue operating correctly despite node failures or malicious actions. Enterprise blockchain systems require robust fault tolerance mechanisms to maintain network reliability. *Byzantine Fault Tolerance (BFT)* mechanism implementations are commonly used to handle scenarios where some nodes may act maliciously or fail. BFT generally ensures that consensus can be reached as long as a majority of nodes are honest. Fault tolerance also involves *crash fault tolerance (CFT)*, where the system can recover from node crashes without losing data integrity or network functionality.

  The Blockchain System must maintain a decentralized network structure to prevent central points of failure or control. Decentralization is achieved by distributing the consensus process among multiple independent nodes. This prevents any single entity from having control over the entire network Consensus mechanisms must be designed to mitigate risks such as Sybil attacks, where an attacker creates multiple fake identities to gain influence over the network.

Using mechanisms like PoW or PoS, which require significant resource investment to participate, helps protect against such attacks. Additionally, mechanisms must ensure transaction finality and prevent double-spending by ensuring that once a transaction is confirmed, it cannot be reversed or duplicated. Blockchain systems generally aim for energy-efficient consensus mechanisms to reduce operational costs and environmental impact. Alternatives to energy-intensive *Proof of Work (PoW)*, such as *Proof of Stake (PoS)* and its variants, offer significant energy savings. These mechanisms maintain security by relying on economic incentives rather than computational power.

Implementing systems like *intrusion detection systems (IDS)* and *intrusion prevention systems (IPS)* is essential. These systems monitor network traffic, identify suspicious activities, and automatically respond to potential threats. Continuous monitoring and anomaly detection help in early detection and mitigation of security breaches. Only Authenticate and authorize nodes are legitimate participants and can access the network. Its fundamental to establish a robust plan for responding to security incidents and network failures.

- **Auditing, Policies and Regulations**[7][13]
  One of the most important elements of a system is determining whether it functions as intended and adheres to all applicable guidelines and regulations. Enterprise blockchain systems must record all transactions and changes in an immutable ledger. This ensures transparency and accountability. Each transaction is timestamped and linked to the preceding transaction, creating a clear and unalterable history. This audit trail is crucial for regulatory compliance, internal audits, and general investigations.

  The blockchain system must adhere to relevant guidelines and standards set by organizations such as NIST, ISO, and other industry-specific regulatory bodies. This includes complying with data protection regulations like *GDPR(General Data Protection Regulation)*[15] and implementing security controls and practices recommended by these standards to ensure compliance and avoid legal penalties.

  Mechanisms must be implemented to protect data stored on the blockchain. This includes data minimization, encryption, and providing users with control over their data (e.g., consent management, data access requests). Regular audits and assessments should be conducted to ensure ongoing compliance. Different industries have unique regulatory requirements. For instance, financial services must comply with regulations like the *Sarbanes-Oxley Act (SOX)*, while healthcare systems must adhere to *HIPAA*. Ensuring compliance with these regulations involves implementing specific controls, conducting regular compliance audits, and maintaining detailed records of all regulatory interactions. Through the implementation of various regulations via a policy-based system, it is possible to use one system across different sectors while adhering to all regulatory requirements. This approach provides a security model with a certain level of generality.

As with the "general security model," this representation also depicts a general version of enterprise-grade security. As can be inferred from this, handling security in an enterprise environment is much more structured and controlled. It must comply with widely accepted security regulations, leading to the perception of such a system as both credible and highly secure. Most currently available enterprise systems do not fully adhere to all zero trust principles, while many public enterprise blockchain systems face challenges with implementing high privacy measures and the introduction of regulations and standardizations. There is a necessity to provide a security system that meets enterprise requirements but is implemented within a public network. Public platforms like *Ethereum*, *Solana*, and *Cardano* offer a certain degree of enterprise-grade security, yet there are areas where they currently have limitations. These platforms encounter challenges such as *regulatory compliance*, *implementation complexity*, and the *implementation of security standards*. Enterprises must carefully consider these factors and potentially implement additional security measures to meet their specific requirements and ensure full compliance with security standards.

The objective of this study is to integrate both aspects (enterprise and public) and provide a highly secure, standardized, and trustless security system for public blockchain networks (in our case, substrate-based). In the next section, we will specify the requirements that an enterprise security system demands as clearly as possible at this stage and set these as the general goals of the research, which will then be presented as solution proposals in Section 4 (Findings).

2.3 Specifications

The following enterprise security requirement specifications are derived from our ongoing research and establish the foundational principles for a highly secure system. These principles will guide further detailed analysis and comprehensive reporting on specific security areas, aiming to present potential implementations of the requirements outlined. As this is the initial draft, future versions may introduce new requirements or remove some, based on new insights from ongoing research, with the goal of developing a concrete solution.

First, we outline the foundational standards for an enterprise-based system. Establishing standards is essential for creating a stable and secure system. Renowned standardization organizations, such as *ISO/IEC(International Organization for Standardization/International Electrotechnical Commission)[18][4], NIST(National Institute of Standards and Technology)[19], IETF(Internet Engineering Task Force)[12], CIS(Center for Internet Security)[14] and ENISA(The European Union Agency for Cybersecurity)[5]*, provide guidelines and standards that are widely accepted as secure and reliable. Consequently, this research and the resulting findings will adhere to these established norms. For each requirement, the relevant standard will be identified and clearly defined. Below, we specify the general enterprise security requirements for a blockchain system.

(1) **Identities, Access Control and Key Management**
- All system accounts must have unique and verifiable identities.
- All Identities must be associated with specific roles within the network
- The system must support secure processes for issuing and managing identities.
- Identity revocation must be supported to prevent the use of compromised identities
- Fine-grained access control mechanisms must be implemented.
- The system must support real-time creation, modification, and deletion of access control policies.
- Dynamic updates of policies, role definitions, and access control rules must be achievable.
- Keys must be generated and stored in secure and tamper-resistant environments.
- Hardware Security Modules (HSMs) or equivalent secure storage solutions must be used.
- Regular key rotation and revocation of compromised keys must be implemented.
- Mechanisms for secure key distribution and deprecation of old keys must be in place.

(2) **Cryptographic Mechanisms and Data Privacy**
- Strong, standardized cryptographic algorithms must be used
- Cryptographic hash functions combined with digital signatures must be used to verify data integrity and origin.
- Privacy-preserving technologies such as zero-knowledge proofs (ZKPs) must be implemented.
- Techniques to ensure transaction validity without revealing additional information must be used.
- Data must be encrypted at "rest" and in "transit".
- Access to decryption keys must be limited to authorized parties only.
- Mutual authentication mechanisms must secure communication between nodes.
- Pseudonymization and anonymization techniques must protect personally identifiable information (PII).

(3) **Consensus Mechanisms and Network Security**
- Robust and fault-tolerant consensus mechanisms must be implemented.
- The system must tolerate node failures and malicious actions while maintaining consensus.
- Consensus algorithms must provide security against common attacks, including Sybil attacks and double-spending.
- Transaction finality must be ensured to prevent transactions from being reversed or duplicated.
- Monitoring and intrusion detection/prevention systems must identify and respond to suspicious activities.
- Continuous monitoring and anomaly detection must be performed for early breach detection.
- Nodes must be authenticated and authorized to ensure only legitimate participants access the network.
- Rate limiting, traffic filtering, and load balancing must be used to mitigate DDoS attacks.
- Predefined procedures for responding to security incidents and network failures must be prepared.

- The incident response plan must be regularly tested and updated to ensure effectiveness.

(4) **Auditing, Policies and Regulations**
- Regular security audits and assessments must be conducted.
- All transactions and changes must be recorded in an immutable ledger for transparency and accountability.
- Internal and external audits must ensure compliance with security policies and standards.
- Audit trails must facilitate regulatory compliance, internal audits, and investigations.
- Adherence to relevant legal and regulatory requirements is mandatory.
- Guidelines and standards set by regulatory bodies such as NIST, ISO, and industry-specific regulators must be followed.
- Compliance with data protection regulations like GDPR must be maintained.
- Detailed records of compliance activities must be kept, and compliance measures must be regularly reviewed.
- Data minimization, encryption, and user control mechanisms must ensure data protection.
- Regular assessments must ensure ongoing compliance with data protection regulations.
- Comprehensive security policies must be developed and enforced.
- Clear policies covering data protection, incident response, and access control must be established.
- Policies must be regularly reviewed and updated to reflect changes in the threat landscape and regulatory requirements.

Our aim is to propose a stable and secure enterprise system by adhering to globally recognized standards. By following the guidelines provided by organizations such as *ISO/IEC, NIST, IETF, CIS and ENISA*, we ensure that our research aligns with best practices. Each identified requirement will be associated with a corresponding standard, clearly defined to maintain consistency and reliability.

References

[1] Elaine Barker and William C. Barker. *Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations*. URL: https://doi.org/10.6028/NIST.SP.800-57pt2r1. (published: 2019).

[2] Chainalysis blog. *The Importance of Blockchain Security*. URL: https://www.chainalysis.com/blog/blockchain-security. (accessed: 2024).

[3] LogosLabs blog. *Decoding the sub0layer: Technical Overview and Future Prospects*. URL: https://blog.logoslabs.io/year_2024/decoding_the_sub0layer. (accessed: 2024).

[4] International Electrotechnical Commission. *Cyber security*. URL: https://www.iec.ch/cyber-security. (accessed: 2024).

[5] The European Union Agency for Cybersecurity. *Standards*. URL: https://www.enisa.europa.eu/topics/standards. (accessed: 2024).

[6] Hyperledger Documentation. *DKMS (Decentralized Key Management System) Design and Architecture*. URL: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0051-dkms/dkms-v4.md. (accessed: 2024).

[7] Hyperledger Fabric Documentation. *Security Model*. URL: https://hyperledger-fabric.readthedocs.io/en/latest/security_model.html. (accessed: 2024).

[8] LogosLabs documentation. *About Logos network*. URL: https://docs.logoslabs.io/learn/logos-general/aboutLogosNetwork. (accessed: 2024).

[9] Substrare Documentation. *Accounts, addresses, and keys*. URL: https://docs.substrate.io/learn/accounts-addresses-keys. (accessed: 2024).

[10] Substrare Documentation. *Consensus*. URL: https://docs.substrate.io/learn/consensus. (accessed: 2024).

[11] Substrare Documentation. *Cryptography*. URL: https://docs.substrate.io/learn/cryptography. (accessed: 2024).

[12] Internet Engineering Task Force. *Security and privacy*. URL: https://www.ietf.org/technologies/security/. (accessed: 2024).

[13] Vincent C. Hu. *Blockchain for Access Control Systems*. URL: https://doi.org/10.6028/NIST.IR.8403. (published: 2022).

[14] Center for Internet Security. *Cybersecurity Services*. URL: https://www.cisecurity.org/services. (accessed: 2024).

[15] General Data Protection Regulation. *GDPR*. URL: https://gdpr-info.eu/. (accessed: 2024).

[16] Stu Mitchell Sean Connelly Scott Rose Oliver Borchert. *Zero Trust Architecture*. URL: https://doi.org/10.6028/NIST.SP.800-207. (published: 2020).

[17] Silvio M Micali Shafi Goldwasser and Charles Rackoff. *The knowledge complexity of interactive proof systems*. URL: https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf. (published: 1985).

[18] International Organization for Standardization. *IT and related technologies*. URL: https://www.iso.org/sectors/it-technologies. (accessed: 2024).

[19] National Institute of Standards and Technology. *COMPUTER SECURITY RESOURCE CENTER*. URL: https://csrc.nist.gov/. (accessed: 2024).

[20] Dr. Gavin Wood. *Polkadot: Vision for a heterogeneous multi-chain framework*. URL: https://assets.polkadot.network/Polkadot-whitepaper.pdf. (published: 2016).

Glossary

Name	Acronym	Description	Definition

Table 1: Glossary for the Research