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, 29 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. [11]

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* [6] 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. Generally, we define the security characteristics (general security model) of a blockchain network as follows.

(1) **Identities, Access Control and Key Management:**[1][7][10][4] 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.

(2) **Cryptographic Mechanisms and Data Privacy:**[9][12] 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".

(3) **Consensus Mechanisms and Network Security:**[8][13] 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.

(4) **Auditing, Policies and Regulations:**[5][10] 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

2.3 Specifications

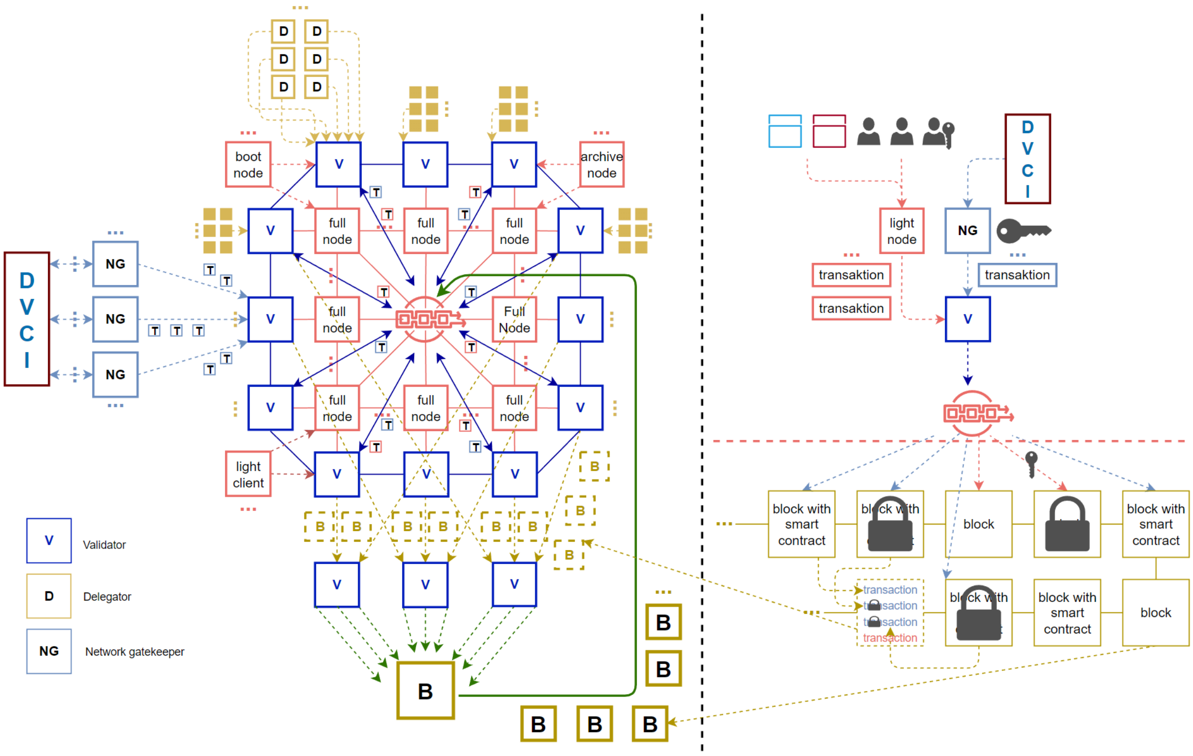

Figure 1:

3 Theoretical Foundations

3.1 Identities, Access Control and Key Management

3.2 Cryptographic Mechanisms and Data Privacy

3.3 Consensus Mechanisms and Network Security

3.4 Auditing, Policies and Regulations

4 Findings

4.1 Identities, Access Control and Key Management

4.2 Cryptographic Mechanisms and Data Privacy

4.3 Consensus Mechanisms and Network Security

4.4 Auditing, Policies and Regulations

4.5 Security Model Proposal

5 Discussion

5.1 Identities, Access Control and Key Management

5.2 Cryptographic Mechanisms and Data Privacy

5.3 Consensus Mechanisms and Network Security

5.4 Auditing, Policies and Regulations

5.5 Justification of the Proposal

6 Conclusion

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] 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).

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

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

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

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

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

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

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

[12] 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).

[13] Dr. Gavin Wood. *Polkadot: Vision for a heterogeneous multi-chain framework.* URL: `https://assets.polkadot.network/Polkadot-whitepaper.pdf`. (published: 2024).

Glossary

Name	Acronym	Description	Definition

Table 1: Glossary for the Research