DEVELOPMENT OF THE MODEL AND ARCHITECTURE OF A BLOCKCHAIN-BASED DATA PROTECTION SYSTEM

Abdullayev Xushnud Raxmatulla ogli
Axmatov Bekzod Nurali ogli
Kutlimurotov Abrorbek Hamid ogli
Narzikulova Sevinch Aktam kizi
Students of the Muhammad al-Khwarizmi Technical University

Annotation

This study presents the development of a model and architecture for a blockchain-based data protection system. The research focuses on addressing the limitations of traditional centralized systems, such as single points of failure, lack of transparency, and vulnerability to cyberattacks. A multi-layer architecture is proposed, integrating blockchain technology, cryptographic mechanisms, distributed storage, and access control services. The system ensures data confidentiality, integrity, availability, traceability, and accountability throughout its lifecycle. Key components include user roles, application services, smart contracts, and hybrid storage solutions combining on-chain and off-chain mechanisms. The findings demonstrate that the proposed architecture significantly enhances security, scalability, and reliability in modern information systems.

Keywords

blockchain architecture, data protection, cybersecurity, decentralized systems, smart contracts, cryptography, access control, distributed storage, IPFS, hybrid storage

The rapid digital transformation of modern society has significantly increased the amount of sensitive information processed, transmitted, and stored within information systems. Government institutions, financial organizations, healthcare providers, educational institutions, and private enterprises continuously generate large volumes of digital data that require secure storage and protection against unauthorized access, modification, and destruction. Traditional centralized data management architectures often suffer from several limitations, including single points of failure, limited transparency, vulnerability to insider attacks, and challenges related to data integrity verification. Consequently, the development of secure and decentralized data protection systems has become one of the most important research directions in modern cybersecurity.

Blockchain technology has emerged as a promising solution for addressing many of these challenges. Unlike conventional centralized systems, blockchain

provides a distributed ledger architecture in which data records are replicated across multiple network nodes and protected through cryptographic mechanisms. The decentralized nature of blockchain significantly improves reliability, transparency, and resistance against cyberattacks. Furthermore, the use of consensus mechanisms, smart contracts, and cryptographic hashing allows organizations to establish trusted environments without relying on a single central authority.

The primary objective of the proposed blockchain-based data protection system is to ensure confidentiality, integrity, availability, traceability, and accountability of information throughout its entire lifecycle. To achieve these objectives, a multi-layer architecture is designed that integrates blockchain technology, cryptographic protection mechanisms, distributed storage systems, and access control services into a unified framework.

General Architecture of the Proposed System. Figure 2.1 illustrates the overall architecture of the proposed blockchain-based data protection system. The proposed blockchain-based data protection architecture consists of four main layers: the User Layer, Application Layer, Blockchain Layer, and Storage Layer. In addition, several cross-cutting security and management mechanisms operate throughout the entire system. The architecture is designed to ensure secure data processing, decentralized storage, integrity verification, and reliable access control within modern information systems.

The User Layer represents the highest level of interaction between users and the blockchain ecosystem. This layer serves as the entry point through which various categories of users access system resources and services.

The architecture supports multiple user roles, including:

- Administrators
- Operators
- Auditors
- External Services
- Mobile Application Users

Administrators are responsible for system configuration, user management, policy enforcement, and overall infrastructure supervision. Operators perform routine data processing tasks, including uploading, updating, and managing protected information. Auditors are granted read-only access to transaction histories and security logs for compliance verification and security assessment purposes. External services interact with the blockchain platform through APIs and integration interfaces, while mobile users access the system remotely using dedicated applications.

To ensure secure communication between users and the system, industry-standard protocols such as HTTPS, WebSocket, and gRPC are employed. These protocols provide encrypted communication channels that protect data against interception, eavesdropping, and man-in-the-middle attacks.

The separation of user roles according to the principle of least privilege enhances security by ensuring that users receive only the permissions required to perform their specific tasks.

The Application Layer acts as an intermediary between end users and the blockchain infrastructure. It is responsible for handling business logic, request processing, user authentication, and communication with blockchain services. The main components of this layer include:

API Gateway and Load Balancer. The API Gateway serves as a centralized entry point for all incoming requests. It performs request routing, traffic management, protocol translation, and security filtering. The Load Balancer distributes requests across multiple application instances to ensure system scalability and fault tolerance.

Authentication Service. Authentication is a critical component of any data protection system. The Authentication Service verifies user identities using modern authentication technologies such as:

- JSON Web Tokens (JWT)
- OAuth 2.0
- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)

These mechanisms ensure that only authorized users can access protected resources.

Data Processing Service. Before data is recorded in the blockchain network, it undergoes preprocessing operations, including:

- Data validation
- Data normalization
- Encryption
- Hash generation
- Metadata extraction

This service guarantees that only verified and properly formatted information enters the blockchain ecosystem.

Audit Service. The Audit Service continuously collects system logs, transaction records, user activities, and security events. These logs support compliance verification, forensic investigations, and incident response activities.

Communication between the Application Layer and Blockchain Layer is performed through REST APIs, gRPC protocols, and blockchain Software Development Kits (SDKs), such as Hyperledger Fabric SDK.

The Blockchain Layer forms the core security component of the proposed architecture. This layer is responsible for maintaining immutable transaction records, enforcing access policies, and ensuring trust among distributed participants. The blockchain network consists of multiple peer nodes and ordering nodes organized according to a consortium blockchain model.

Smart Contracts. Smart contracts automate system operations and enforce predefined security policies without human intervention. The proposed architecture includes three primary smart contracts:

1. Data Registry Contract. This contract manages the registration of digital assets and metadata. It records cryptographic hash values, ownership information, timestamps, and storage references.
2. Access Control Contract. This contract manages user permissions and access rights. It verifies whether users possess sufficient authorization before granting access to protected information.
3. Audit Log Contract. This contract maintains immutable records of all system events and transactions. Since blockchain data cannot be modified after confirmation, audit logs remain trustworthy and tamper-resistant.

Peer Nodes. Peer nodes validate transactions, execute smart contracts, and maintain synchronized copies of the distributed ledger. Multiple peer nodes improve redundancy and eliminate single points of failure.

Ordering Service. The ordering service is responsible for transaction sequencing and block creation. In the proposed architecture, the Raft consensus algorithm is utilized due to its simplicity, efficiency, and fault-tolerant characteristics.

Consensus Mechanism. Consensus mechanisms ensure agreement among distributed participants regarding the validity of transactions. The use of Raft consensus enables the system to maintain consistency while minimizing computational overhead compared to Proof-of-Work-based systems.

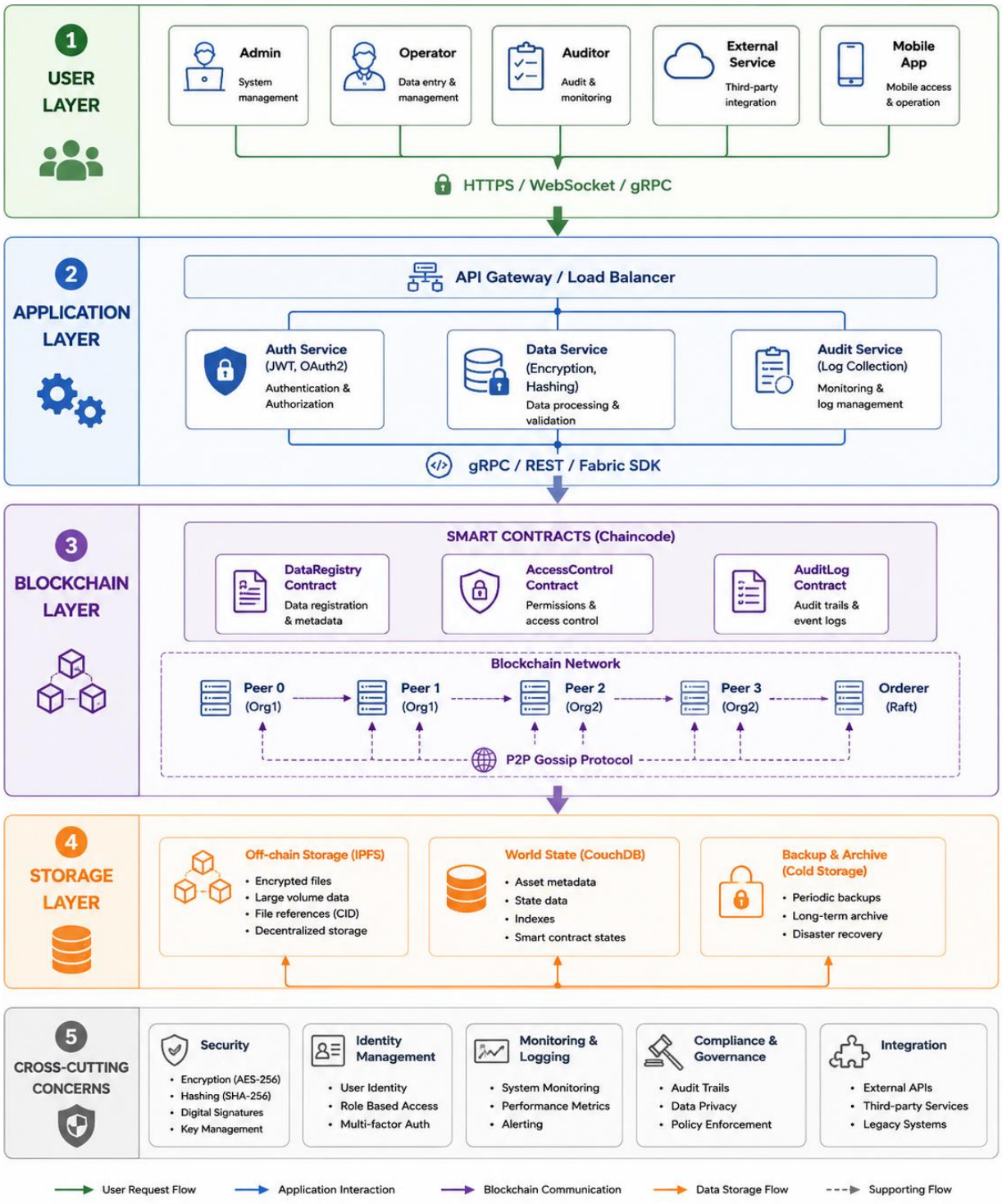

Figure 1.1. The proposed blockchain-based data protection architecture.

Storage Layer. Although blockchain provides secure storage of transaction metadata, storing large files directly on-chain is impractical due to performance and scalability limitations. Therefore, the proposed architecture employs a hybrid storage model consisting of both on-chain and off-chain storage components.

Off-Chain Storage. Large files, documents, multimedia content, and encrypted datasets are stored within the InterPlanetary File System (IPFS). IPFS offers several advantages:

- Distributed file storage
- Content-based addressing
- Reduced storage costs
- Improved scalability
- Enhanced data availability

Each file stored in IPFS generates a unique cryptographic hash that serves as its identifier.

On-Chain Storage. Only critical metadata is stored on the blockchain, including:

- File hash values
- Ownership information
- Timestamps
- Access permissions
- Transaction records

This approach significantly reduces blockchain storage requirements while preserving integrity verification capabilities.

World State Database. The architecture utilizes CouchDB as the World State Database. CouchDB stores:

- Current asset states
- Smart contract variables
- Indexes
- Queryable metadata

The database enables efficient data retrieval and high-performance query processing.

Backup and Recovery System. To ensure business continuity and disaster recovery, the architecture incorporates backup and archive mechanisms. Periodic snapshots and cold storage repositories protect critical information against accidental deletion, hardware failures, and ransomware attacks.

Security Mechanisms. Several security mechanisms operate across all architectural layers.

Cryptographic Protection. The architecture employs strong cryptographic algorithms including:

- AES-256 for encryption
- SHA-256 for hashing
- RSA and ECC for digital signatures
- TLS for secure communications

These technologies ensure confidentiality, integrity, and authenticity of information.

Identity and Access Management. Role-based access control and multi-factor authentication reduce the likelihood of unauthorized access and credential theft.

Monitoring and Incident Detection. Continuous monitoring services analyze system behavior, detect anomalies, and generate alerts whenever suspicious activities occur.

Compliance and Governance. The architecture supports auditing, regulatory compliance, and governance requirements through immutable logs and transparent transaction histories.

Advantages of the Proposed Architecture. The proposed blockchain-based architecture provides several important advantages:

- Decentralized management
- Enhanced data integrity
- Improved transparency
- Resistance to unauthorized modifications
- High availability and fault tolerance
- Secure access control
- Scalability through hybrid storage
- Support for auditing and compliance
- Reduced dependency on centralized authorities

The proposed blockchain-based data protection architecture integrates distributed ledger technology, smart contracts, cryptographic security mechanisms, and decentralized storage systems into a unified framework for secure information management. By combining on-chain and off-chain storage approaches, the architecture achieves both security and scalability while maintaining data integrity and transparency.

The proposed model can be effectively applied in healthcare systems, e-government platforms, cloud computing environments, financial institutions, supply chain management systems, and enterprise cybersecurity infrastructures where secure and trustworthy data management is essential.

Conclusion

The proposed blockchain-based data protection architecture provides a secure and scalable solution for modern information systems. By combining decentralized ledger technology, cryptographic security, and hybrid storage mechanisms, the system ensures strong protection against unauthorized access and data tampering. The use of smart contracts automates processes and enforces security policies, while distributed storage improves reliability and availability. This architecture can be effectively applied across various domains, including healthcare, finance, e-government, and cloud computing, making it a powerful tool for ensuring secure and trustworthy data management in the digital era.

REFERENCES:

1. Mastering Blockchain – Comprehensive guide to blockchain architecture and enterprise solutions.
2. Blockchain Basics – Fundamental concepts of blockchain technology.
3. Building Blockchain Projects – Practical implementation of blockchain-based systems.
4. Hyperledger Fabric in Action – Enterprise blockchain framework and architecture design.