Blockchain Security: A Technical Report Based on Patent Analysis

Abstract (Summary)

This report analyzes a collection of patents focused on enhancing blockchain security. The inventions address various challenges, including smart contract vulnerabilities, consensus mechanism weaknesses, data integrity issues, access control limitations, and the need for privacy. The solutions leverage techniques such as abstract syntax tree analysis for smart contract hardening, multiple proof-of-work problems for enhanced decentralization, blockchain-based data hashing for tamper-proof logging, smart contracts for access rule enforcement, and trusted execution environments (TEEs) for data privacy. The overall goal is to improve the security, reliability, and efficiency of blockchain networks and applications.

Background and Existing Technologies/Challenges

Blockchain technology, while inherently secure due to its cryptographic foundations and distributed nature, faces several security challenges. Smart contracts, which automate agreements on the blockchain, are susceptible to vulnerabilities that can be exploited. Traditional consensus mechanisms can be vulnerable to attacks and centralization. Data stored on the blockchain needs protection against unauthorized access and tampering. Furthermore, the increasing demand for scalability and privacy introduces new complexities. Existing technologies often struggle to balance these competing requirements, leading to the need for innovative solutions.

Technical Fields of Invention

The inventions discussed in this report span several technological areas related to blockchain security:

- **Smart Contract Security:** Techniques for vulnerability detection, patching, and formal verification of smart contracts (WO 2022078632, EP 4550714, WO 2024074875).

- **Consensus Mechanisms:** Novel consensus algorithms designed to improve security, decentralization, and efficiency (EP 4057567, WO 2023025394, WO 2024059068, WO 2022188831).
- **Data Integrity:** Methods for ensuring the integrity and authenticity of data stored on the blockchain (WO 2021085701, WO 2021034274, EP 4231167).
- **Access Control:** Mechanisms for managing access to data and assets on the blockchain, including consent-based systems and permissioning schemes (WO 2022046524, WO 2024032994, WO 2021042818).
- **Privacy-Enhancing Technologies:** Techniques for protecting sensitive data on the blockchain, such as zero-knowledge proofs and trusted execution environments (WO 2024236572).
- **Decentralized Computing:** Platforms for secure and incentivized resource sharing in decentralized environments (WO 2022103900).
- **Blockchain Architecture:** Layered network architectures for efficient smart contract state management (WO 2021165754).
- **Random Number Generation:** Methods for generating unpredictable random numbers on the blockchain (WO 2023185051).

Inventions Related to Blockchain Security

Smart Contract Hardening and Vulnerability Detection

- **WO 2022078632:** This invention focuses on hardening smart contracts by automatically detecting and patching vulnerabilities. It translates smart contract source code into an abstract syntax tree, generates a code property graph, enriches it with inferable information, and then checks for predetermined vulnerability patterns. Patches are applied to the code property graph to fix the found vulnerabilities. This approach improves smart contract security by proactively addressing potential weaknesses. The novelty lies in the automated process of vulnerability detection and patching using code property graphs. (Relevant)
- **EP 4550714:** This invention introduces a modular apparatus for generating resilient smart contracts, particularly for B2B applications. It uses a Modular Asset Lifecycle Descriptor (ALD) and a feedback loop to generate and iteratively improve smart contracts. The objective is to reduce the cost and complexity of smart contract security measures. (Relevant)

- **WO 2024074875:** This invention presents a method for monitoring and classifying smart contract behavior using machine learning. It addresses the problem of detecting malicious activity in smart contracts by classifying the type of behavior based on data representative of events resulting from its execution. This allows for the identification of anomalous or suspicious behavior without modifying existing blockchain infrastructure. (Relevant)

Enhanced Consensus Mechanisms

- **EP 4057567:** This invention addresses the vulnerability to attacks and centralization in blockchains that depend on a single proof-of-work problem. The technical solution involves a blockchain dependent on a plurality of proof-of-work problems, improving the security and decentralization of blockchain networks. (Relevant)
- **WO 2023025394:** This invention describes a blockchain consensus method that ensures high security and authentication of transactions while avoiding high energy consumption and the "nothing-at-stake" problem. It involves an administrative node, an elected node, and regular nodes, each with a virtual machine and checker service, along with provider nodes providing transactions. (Relevant)
- **WO 2024059068:** This invention focuses on analyzing blockchain validation networks and consensus reward emissions. It addresses the challenge of accurately analyzing operations within a proof-of-stake blockchain network by determining staking balances for validator nodes and calculating an average staking return rate based on consensus and execution layer emissions. (Relevant)
- **WO 2022188831:** This invention aims to reduce block chaining time and improve blockchain throughput by executing transaction data in a proposal block using a smart contract to obtain a target contract execution result, caching the block hash value and the result in a temporary list, performing two rounds of consensus voting in parallel, and storing the proposal block and execution result in the blockchain if consensus is reached. (Relevant)

Data Integrity and Security Event Processing

- **WO 2021085701:** This invention focuses on processing security events using blockchain and smart contracts to reliably verify that existing data

has not been hacked. It stores security event information, transaction hash values, and merged hash values in both a blockchain and a security event database, as well as in a smart contract. A security event inquiry unit verifies the consistency of these values to detect integrity issues. The improvement lies in the automated recovery of integrity when security events occur. (Relevant)

- **WO 2021034274:** This invention improves data security in industrial control systems (ICS) by creating tamper-proof data logs for forensic analysis. It uses a blockchain network to store hashes of operational data files, enabling validation of data integrity. Each storage node records operational data, generates a hash of the file, and registers the hash by sending a transaction to the blockchain network, where a smart contract generates metadata and records the hash and metadata in a node of the blockchain. (Relevant)

Access Control and Data Ownership

- **WO 2022046524:** This invention addresses the problem of securing data and managing data ownership in cloud-based systems. It uses owner consent contracts stored in a blockchain to define and enforce access rules for digital assets, providing an auditable trail of data access. The core of the invention is a blockchain access method that includes adding to a blockchain a consent block storing an owner consent contract containing one or more access rules that determine access, for an entity other than an owner of the owner consent contract, to a portion of an asset that is stored in another block of the blockchain and owned by the owner. (Relevant)
- **WO 2024032994:** This invention aims to solve the technical problem of permission control and user authorization in databases by using a blockchain-implemented database overlay and indexing mechanism. The technical solution involves mapping records in a traditional database to transactions on a blockchain, leveraging the blockchain's consensus mechanism for permissioning and access control. (Relevant)
- **WO 2021042818:** This invention enables data isolation for asset distribution transactions issued to the blockchain by different investment managers, ensuring that only authorized users can query specific asset release transactions. It guarantees data security by decrypting smart contract code and asset release transactions within a trusted execution environment (TEE). (Relevant)

Privacy-Enhancing Technologies

- **WO 2024236572:** This invention addresses the blockchain trilemma (scalability, security, and decentralization) and data privacy by isolating operators from accessing selected user data and transactions. The technical solution involves hosting Zero-Knowledge (ZK) rollups within a Trusted Execution Environment (TEE), encrypting and processing data sent to the blockchain Node, Prover, and Sequencer components within the TEE. (Relevant)

Unique Components, Devices, Apparatus, Methods, or Systems

- **Code Property Graph:** Used in WO 2022078632 for representing smart contract code and facilitating vulnerability detection and patching. (Relevant)
- **Modular Asset Lifecycle Descriptor (ALD):** Used in EP 4550714 for generating and iteratively improving resilient smart contracts. (Relevant)
- **Trusted Execution Environment (TEE):** Used in WO 2021042818 and WO 2024236572 for decrypting smart contract code and processing sensitive data in a secure environment. (Relevant)
- **Smart Contracts for Access Control:** Used in WO 2022046524 and WO 2024032994 for defining and enforcing access rules for digital assets. (Relevant)
- **Blockchain-based Data Hashing:** Used in WO 2021034274 for creating tamper-proof data logs in industrial control systems. (Relevant)

Technical Problems Solved and Improvements Provided

- **Smart Contract Vulnerabilities:** WO 2022078632, EP 4550714, and WO 2024074875 address the risk of vulnerabilities in smart contracts by providing automated vulnerability detection, patching, and behavior monitoring. (Relevant)
- **Centralization and Attack Vectors:** EP 4057567 improves decentralization and security by using multiple proof-of-work problems. (Relevant)

- **Data Tampering:** WO 2021085701 and WO 2021034274 ensure data integrity by using blockchain to store hashes of data files and security event information. (Relevant)
- **Unauthorized Access:** WO 2022046524, WO 2024032994, and WO 2021042818 provide mechanisms for managing access to data and assets on the blockchain, ensuring that only authorized users can access sensitive information. (Relevant)
- **Data Privacy:** WO 2024236572 protects sensitive data by using zero-knowledge proofs and trusted execution environments. (Relevant)

Applicability and Uses

The inventions described in these patents have a wide range of practical applications:

- **Smart Contract Security:** Can be used by blockchain developers and auditors to improve the security of smart contracts in decentralized applications (dApps), decentralized finance (DeFi), and other blockchain-based systems. (Relevant)
- **Data Integrity:** Can be used in industrial control systems, supply chain management, and other applications where data integrity is critical. (Relevant)
- **Access Control:** Can be used in healthcare, finance, and other industries where data privacy and security are paramount. (Relevant)
- **Privacy-Enhancing Technologies:** Can be used in applications that require the protection of sensitive data, such as voting systems, identity management, and confidential transactions. (Relevant)
- **Decentralized Computing:** Can be used for various computation tasks, such as video transcoding, drug design, and scientific research. (Relevant)
- **Blockchain Emission Analysis:** Can be used to monitor and improve blockchain network security, schedule blockchain transactions, and improve the efficiency of transaction processing. (Relevant)

Conclusion

The patents analyzed in this report demonstrate a range of innovative approaches to enhance blockchain security. These inventions address critical

challenges related to smart contract vulnerabilities, consensus mechanisms, data integrity, access control, and privacy. By leveraging techniques such as abstract syntax tree analysis, multiple proof-of-work problems, blockchain-based data hashing, smart contracts for access rule enforcement, and trusted execution environments, these inventions contribute to the development of more secure, reliable, and efficient blockchain networks and applications.

Citations

- WO 2022078632 (Relevant)
- EP 4057567 (Relevant)
- EP 3598879 (Relevant)
- WO 2022103900 (Relevant)
- WO 2022235854 (Relevant)
- WO 2022046524 (Relevant)
- WO 2023025394 (Relevant)
- WO 2021085701 (Relevant)
- WO 2021034274 (Relevant)
- WO 2024244339 (Relevant)
- EP 4231167 (Relevant)
- WO 2021042818 (Relevant)
- WO 2020125218 (Relevant)
- EP 3844642 (Relevant)
- WO 2024032994 (Relevant)
- WO 2021165754 (Relevant)
- WO 2020036270 (Relevant)
- WO 2024236572 (Relevant)
- WO 2023185051 (Relevant)
- WO 2024059068 (Relevant)
- EP 4550714 (Relevant)
- WO 2024074875 (Relevant)
- WO 2024242242 (Relevant)
- WO 2019092544 (Relevant)
- WO 2022188831 (Relevant)
- EP 4036765 (Relevant)

Contexts: WO 2022078632 :: METHOD AND SYSTEM FOR SUPPORTING SMART CONTRACTS IN A BLOCKCHAIN NETWORK\n
EP 4057567 :: IMPROVED BLOCKCHAIN RELYING ON ADVANCED CONSENSUS MECHANISM\n
EP 3598879 :: METHODS AND DEVICES FOR PROCESSING CERTIFICATES IN BLOCKCHAIN SYSTEM\n
WO 2022103900 :: EDGE COMPUTING PLATFORM SUPPORTED BY SMART CONTRACT ENABLED BLOCKCHAIN NETWORK\n
WO 2022235854 :: SECURE BLOCKCHAIN SUPPLY MANAGEMENT SYSTEM\n
WO 2022046524 :: SYSTEMS AND METHODS FOR ACCESSING DIGITAL ASSETS IN A BLOCKCHAIN USING OWNER CONSENT CONTRACTS\n
WO 2023025394 :: CONSENSUS METHOD FOR BLOCKCHAIN\n
WO 2021085701 :: DEVICE FOR PROCESSING SECURITY EVENT USING BLOCKCHAIN AND SMART CONTRACT, AND METHOD THEREFOR\n
WO 2021034274 :: BLOCKCHAIN FOR OPERATIONAL DATA SECURITY IN INDUSTRIAL CONTROL SYSTEMS\n
WO 2024244339 :: RESOURCE PROCESSING METHOD IN BLOCKCHAIN, AND BLOCKCHAIN NODE\n
EP 4231167 :: DATA STORAGE METHOD AND APPARATUS BASED ON BLOCKCHAIN NETWORK\n
WO 2021042818 :: BLOCKCHAIN-BASED ASSET QUERY METHOD AND APPARATUS, AND ELECTRONIC DEVICE\n
WO 2020125218 :: CLAIM SETTLEMENT METHOD AND APPARATUS EMPLOYING BLOCKCHAIN TECHNOLOGY\n
EP 3844642 :: DISTRIBUTED BLOCKCHAIN DATA STORAGE UNDER ACCOUNT MODEL\n
WO 2024032994 :: BLOCKCHAIN-IMPLEMENTED DATABASE OVERLAY, VERIFICATION AND INDEXING SYSTEM\n
WO 2021165754 :: SMART CONTRACTS\n
WO 2020036270 :: BLOCKCHAIN ARCHITECTURE CONFORMING TO GENERAL DATA PROTECTION REGULATION FOR MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION\n
WO 2024236572 :: A SYSTEM AND METHOD TO PROVIDE A PRIVACY-PRESERVING HARDWARE SECURE ENCLAVE ENVIRONMENT FOR GENERATING BLOCKCHAIN VERIFIABLE TRANSACTIONS AT SCALE\n
WO 2023185051 :: METHOD FOR GENERATING RANDOM NUMBER SEEDS ON BLOCKCHAIN, AND SYSTEM AND CONSENSUS NODE\n
WO 2024059068 :: PROOF-OF-STAKE BLOCKCHAIN EMISSION ANALYSIS\n
, WO 2022103900 :: EDGE COMPUTING PLATFORM SUPPORTED BY SMART CONTRACT

ENABLED BLOCKCHAIN NETWORK\n
WO 2022078632 :: METHOD AND SYSTEM FOR SUPPORTING SMART CONTRACTS IN A BLOCKCHAIN NETWORK\n
EP 4550714 :: MODULAR APPARATUS FOR CREATING RESILIENT SMART-CONTRACTS\n
WO 2021085701 :: DEVICE FOR PROCESSING SECURITY EVENT USING BLOCKCHAIN AND SMART CONTRACT, AND METHOD THEREFOR\n
WO 2024074875 :: SMART CONTRACT BEHAVIOR CLASSIFICATION\n
WO 2024242242 :: BLOCKCHAIN-BASED OFFLINE VOTING SERVICE METHOD AND SYSTEM USING SAME\n
WO 2019092544 :: SYSTEM FOR RECORDING VERIFICATION KEYS ON A BLOCKCHAIN\n
WO 2022188831 :: BLOCK CONSENSUS METHOD BASED ON BLOCKCHAIN, AND RELATED DEVICE\n
WO 2021034274 :: BLOCKCHAIN FOR OPERATIONAL DATA SECURITY IN INDUSTRIAL CONTROL SYSTEMS\n
EP 4036765 :: BLOCKCHAIN-BASED LICENSE MANAGEMENT FRAMEWORK\n