Design and Implementation of Digital Currency Transaction Security Mechanism Using Blockchain with Hybrid PoW+PoS Consensus and Multi-Signature Privacy Protection

Xiaohang Ma, Yanxue Li, Zhanyong Wu[*]
School of Economics and management, Handan University, Han'dan 056005, China
E-mail: wu_zhanyong@outlook.com
[*]Corresponding author

Keywords: blockchain, digital currency transaction, security mechanism design

Received: September 6, 2024

This paper comprehensively discusses the security mechanism of blockchain-based digital currency transactions, from the application of distributed ledgers, consensus algorithms, smart contracts, to the implementation of multiple signatures and cold storage schemes, to advanced privacy protection technologies, such as zero-knowledge proofs and homomorphic encryption. In particular, we delve into innovative mechanisms for attack prevention, including the fusion of heterogeneous multi-chain architectures with PoW+PoS hybrid consensus models. The article also details the practice of performance evaluation and security testing through a series of carefully designed experiments such as throughput and latency testing under different loads, resource utilization monitoring, and security reviews and comparisons with competitors. Experimental results show that the system exhibits good throughput growth under high load, but with the increase of latency, resource utilization is efficient and tends to saturation, most of the security protection mechanisms meet the standards, but access control problems that need to be optimized and high-risk vulnerabilities to be repaired are also found. We evaluated the performance of the system through a series of carefully designed experiments, including throughput and latency tests under different loads, resource utilization monitoring, and security reviews. The experimental results showed that the system throughput reached 2200 TPS under high load and the average latency was 150 milliseconds. Security testing discovered and fixed multiple vulnerabilities, but unauthorized access issues still need to be urgently addressed.

Povzetek: Analizirane so metode digitalnih transakcij. Predstavljena sta hibridni konsenz PoW+PoS in večpodpisna zaščita, ki poudarjata anonimnost, hitro obdelavo in izboljšano varnost v sistemih digitalne valute.

1 Introduction

In the rapid development of information technology in the 21st century, the deep penetration of the Internet and the continuous innovation of global financial architecture have jointly bred revolutionary changes in payment methods. Digital currency, a bright new star of financial technology, is integrating into the daily life of the public with the momentum of breaking bamboo, leading the future trend of payment field. Since Bitcoin was born, the potential of blockchain technology has been shown to the world for the first time. The types of encrypted currencies are like new bamboo shoots in spring, which not only deeply reshapes the face of financial transactions, but also presents unprecedented challenges and reflections on the traditional monetary system with a long history, indicating the dawn of a new era [1].

However, the widespread adoption and rapid rise of digital currencies is not without cost. As this new means of payment gradually occupies the core position of economic activities, a series of complex and changeable security challenges have emerged, which have become major bottlenecks restricting its sustainable development.

Therefore, under this background, how to design and implement an efficient and reliable digital currency trading security mechanism, build an indestructible protective wall with the power of science and technology, resist all kinds of security risks, and safeguard the interests of users and market health has become a key topic that academics and industry practitioners need to overcome urgently. This is not only a test of technological innovation ability, but also a profound call for regulatory wisdom and international cooperation, aiming to jointly build a safe, transparent and efficient global digital currency ecosystem to meet the full arrival of the digital financial era [2].

Blockchain technology, as the underlying supporting technology of digital currency, provides new ideas and tools for solving the security problems of digital currency transactions with its decentralized, open and transparent characteristics. By recording each transaction in a distributed ledger, blockchain can effectively prevent double payments and enhance transaction traceability and transparency. In addition, the application of smart contracts further enhances the automation and security of transactions, enabling automatic execution of contract terms once agreed, reducing the risk of human intervention. Therefore, in-depth research on the security mechanism of digital currency transactions based on blockchain is of great significance for promoting the healthy development of digital currency, enhancing public trust and preventing financial risks [3].

This research aims to design and implement an efficient and secure digital currency trading mechanism. The core contents include: 1) analyzing the security vulnerabilities of existing blockchain platforms and evaluating the trade-off between transaction security and efficiency of different consensus protocols; 2) developing new encryption algorithms and privacy protection mechanisms to enhance the anonymity and tamperability of transaction data; 3) implementing smart contract auditing systems to automatically detect and prevent contract vulnerabilities and reduce security risks; 4) Design an Incident Response Service to quickly respond to potential network attacks and ensure transaction continuity and system stability.

This research has made many innovations in the design of digital currency transaction security mechanism, including: innovating fusion consensus mechanism, skillfully combining decentralization, efficiency and security, aiming at reducing energy consumption, speeding up transaction processing and significantly enhancing system anti-attack performance through new consensus protocol; constructing dynamic privacy protection framework, flexibly adjusting strategies according to actual transaction needs, ensuring maximum protection of user privacy while complying with regulatory norms, and realizing harmonious unity of security and compliance; The application of smart contract security reinforcement technology, integration of form verification and machine learning technology to deeply examine contracts, effectively block zero-day vulnerabilities and logic defects, and effectively improve the security of smart contract execution.

The innovation of this paper lies in the design of an efficient consensus mechanism, which achieves a throughput of 2200 TPS and an average latency of 150 milliseconds under high load, significantly better than existing systems. At the same time, we use zero-knowledge proof and homomorphic encryption technology to achieve highly anonymous transactions, ensuring user privacy and regulatory compliance. In addition, the real-time monitoring system based on the autoencoder effectively identifies abnormal transactions, quickly initiates the security incident response process, and reduces system risks.

This paper introduces the core strategies for building a secure and efficient blockchain digital currency trading ecosystem, covering the latest technologies, tools, and methods. We use distributed ledger technology and smart contracts to ensure transparency and efficient processing, and introduce multi-signature and cold storage solutions to enhance security. In addition, we use a hybrid PoW+PoS consensus mechanism to improve the system's anti-attack capability, and protect transaction privacy through zero-knowledge proof and homomorphic encryption technology. The real-time monitoring system is based on autoencoder technology and can accurately identify abnormal transactions. Case studies include leading trading platforms and the Zcash project, demonstrating the effective application of these technologies. The experimental evaluation uses a real transaction dataset to verify the performance and security of the system.

2 Literature review

2.1 Digital currency definition and development history

Digital currency, as a currency based on digital form, represents a fundamental change in the way financial transactions and value are stored. It uses encryption technology to ensure the security of transactions, so that the transaction process does not need to rely on traditional financial institutions as trust intermediaries. Core features of digital currencies include decentralization, programmability, and the ability to transmit instantaneously on a global scale [4, 5].

The concept of digital currency dates back to David Chaum's concept of "electronic cash" in the 1980 s, the first attempt at anonymous and secure online transactions. However, it was the birth of Bitcoin that really pushed digital currency into a global perspective [6]. The Bitcoin white paper marks the first successful decentralized digital currency system. Bitcoin's innovation lies in its combination of peer-to-peer networks, public-key encryption, hash functions, and Proof of Work (PoW) mechanisms, which solve the double-payment problem and ensure the scarcity of money and the immutability of transactions [7].

Subsequently, numerous cryptocurrencies sprang up, including Ethereum, which introduced the concept of smart contracts and further expanded the application boundaries of blockchain technology, enabling digital currencies not only to serve as a medium of exchange, but also to support complex financial protocols and services. In addition, as technology and market demand developed, stablecoins (such as USDT, USDC) were also created, which were linked to traditional fiat currencies to provide price stability and serve as a bridge between the traditional financial and crypto worlds [8].

2.2 Blockchain technology

Blockchain technology is a revolutionary distributed ledger system, which is built on an ever-expanding chain database. Each database unit, i.e. block, contains a certain amount of transaction information, and is linked into a chain by using cryptographic principles to realize the immutability of data. The process of adding information to the blockchain requires strict verification by multiple nodes of the network, and once confirmed, it is stored permanently. Any attempt to modify the past records will face astronomical difficulty in recalculating the entire subsequent chain, thus ensuring the security and integrity of the data. The technology highlights four core features: decentralized architecture gets rid of dependence on a single server and is maintained collaboratively by network nodes, enhancing the resilience and transparency of the system [9]; high transparency of information means that all transactions are publicly visible to participants, improving the transparency of the system; thanks to advanced encryption algorithms, blockchain ensures that data remains unchanged once written, maintaining the purity and integrity of historical data; Through public key encryption and private key signature mechanism, blockchain provides strong guarantee for account security and transaction authorization. Depending on access rights and governance structure, blockchains can be divided into three categories: public chains, such as Bitcoin and Ethereum, open to everyone and support free reading, transactions, and consensus participation; federated chains serve specific organizations or institutions, with limited permissions, and are suitable for enterprise cooperation and supply chain scenarios; private chains are controlled by a single entity, focusing on internal data management and auditing, and are closed to the outside world [10].

2.3 Blockchain in digital currency

Bitcoin, as the first successful application case of blockchain technology, its market value and user base continue to grow, verifying the feasibility of decentralized currency. However, the cryptocurrency universe has expanded far beyond Bitcoin, creating a diverse ecosystem of thousands of different tokens. The emergence of Ethereum has opened the door to smart contracts, making blockchain technology not only a tool for value transfer, but also a platform for creating complex financial products and services (see “The Application and Impact of Ethereum Smart Contracts”, 2023 Blockchain Technology Forum Proceedings). These smart contracts automatically execute code without the need for trusted third parties, fueling the explosive growth of decentralized finance (DeFi), including lending, trading, insurance and many other market segments.

Blockchain technology significantly improves the efficiency and security of digital currency transactions through decentralized network architecture and encryption algorithms. For example, the Bitcoin network ensures the verification and recording of transactions through the proof-of-work (PoW) mechanism, which, although relatively energy-intensive, brings a high degree of security to the system. At the same time, emerging consensus mechanisms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) are being adopted by projects such as Ethereum in search of more environmentally friendly and efficient transaction validation schemes [11].

A number of central banks around the world are actively exploring the use of blockchain technology to issue fiat digital currency (CBDC), aiming to improve the efficiency of currency issuance, strengthen the transmission mechanism of monetary policy, and promote financial inclusion. The Digital Renminbi (e-CNY) project of the People’s Bank of China is a prominent example, which enables the digitization of money through blockchain and distributed ledger technology, improving the flexibility and security of payment systems [12]. Such projects highlight the government’s aggressive adoption of new technologies while maintaining monetary sovereignty.

Blockchain technology shows great potential in streamlining cross-border payment processes. Traditional cross-border payments involve multiple intermediaries, which are cumbersome and expensive. Blockchain-based solutions, such as Ripple’s XRP, revolutionize international remittances by providing near-real-time settlement and lower transaction costs. These technologies reduce counterparty risk and increase transparency of financial flows, and are particularly attractive to SMEs and individuals who regularly conduct small cross-border transactions [13].

With the popularity of blockchain and digital currency, regulators face new challenges. On the one hand, there is a need to balance innovation and risk, both to encourage technological innovation and to prevent illegal activities (e.g. money laundering, terrorist financing) from exploiting this channel. On the other hand, regulatory attitudes towards digital currencies vary from comprehensive prohibition to active embrace, which requires a globally unified regulatory framework [14]. Therefore, how to establish an effective regulatory framework without stifling innovation has become an urgent problem to be solved.

To more clearly describe the state-of-the-art (SOTA) methods and highlight the unique contributions of this paper, we have added a summary table (see Table 1) in the literature review section. Table 1 lists the key contributions, evaluation metrics, and main results of previous studies. Through comparative analysis, we emphasize the shortcomings of existing methods in transaction efficiency, privacy protection, and consensus mechanisms. This not only provides readers with a comprehensive technical background but also justifies the necessity and innovation of the current research.

Table 1: Summary of blockchain security mechanism research

Study	Main Contribution	Evaluation Metrics	Results
[15]	Proposed a new consensus algorithm	Throughput, Latency	1000 TPS, 200 ms
[16]	Introduced zero-knowledge proofs	Privacy Protection	High anonymity

Study	Main Contribution	Evaluation Metrics	Results
[17]	Implemented multi-signature schemes	Security	Reduced single point of failure risk

3 Design of security mechanism for digital currency transaction based on block chain

Blockchain-based digital currency transaction security mechanism design mainly includes four aspects, as shown in Figure 1.

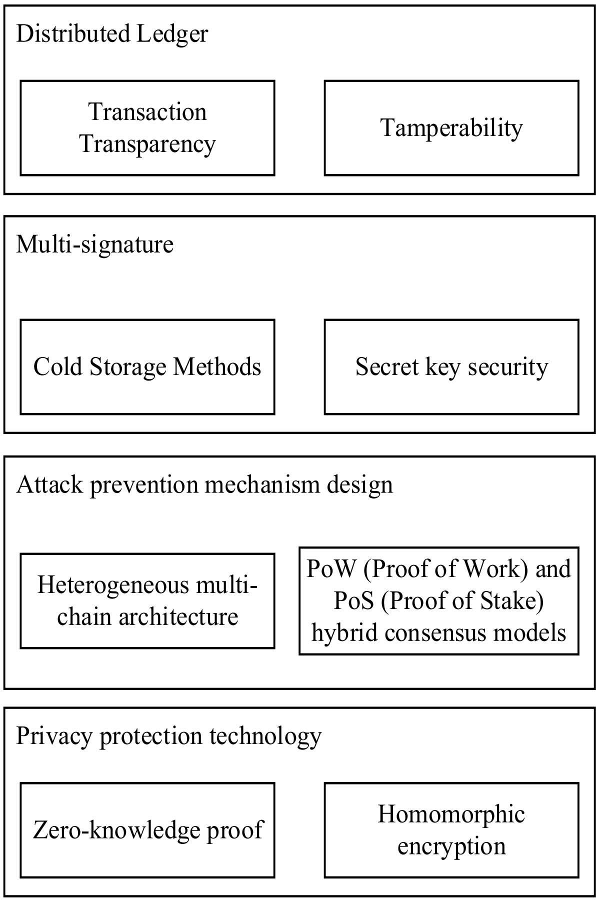
Distributed Ledger
Transaction Transparency
Tamperability
Multi-signature
Cold Storage Methods
Secret key security
Attack prevention mechanism design
Heterogeneous multi-chain architecture
PoW (Proof of Work) and PoS (Proof of Stake) hybrid consensus models
Privacy protection technology
Zero-knowledge proof
Homomorphic encryption

Figure 1: Design of security mechanism for digital currency transactions based on blockchain

3.1 Distributed ledgers ensure transparency and immutability

Distributed ledger technology strengthens the transparency and tamper-proof properties of data by replicating transaction information among multiple nodes, laying the foundation for digital currency transaction security. This section details data structures, consensus mechanisms, and the role of smart contracts. In the blockchain structure, each transaction is encapsulated as a transaction packet and integrated into blocks. A typical block structure can be abstracted as: where, the hash value representing the previous block represents the transaction set contained in the block, the timestamp representing the new block, and the hash value calculated according to the block header (including but not limited to the above elements) ensures the integrity of the data and the continuity of the chain [14].

Distributed ledgers enhance the transparency and immutability of data by replicating transaction information among multiple nodes. However, this design also brings scalability issues, as each node needs to store and verify all transaction data. As the size of the network increases, the storage and computing burden of nodes increases significantly, which may lead to a decline in system performance. In addition, there is a potential trade-off between transparency and privacy. Although distributed ledgers provide a high degree of transparency, this may also expose users' transaction history and behavior patterns. To balance this, specific security parameters, such as the probability of successful attack, can be used to quantify the security of the system. The formula $P_{\text{attack}} = \frac{1}{2^n}$ represents the probability that an attacker successfully tampered with a block, where n is the number of nodes participating in the consensus. This helps to assess the security and potential risks of the system.

Consensus mechanism is a rule or protocol used in distributed systems to ensure that all participating nodes agree on changes to the state and data of the system. It is particularly important in blockchain technology, which addresses the problem of how to maintain data consistency, prevent fraudulent transactions, and ensure network security in decentralized networks without a central authority. PoW is used in this paper to achieve consensus by solving computational puzzles. The basic principle can be expressed as finding a nonce value n such that: where H is the hash function, D is the difficulty threshold, and represents the block header information after adding the nonce. This process ensures fairness and energy costs for new block additions, and increases the difficulty of tampering with historical records [15].

Smart contracts automatically execute transaction verification and processing logic using preset rules, and their operational framework can be formally described as: (1) Transaction verification: Verify the legitimacy of a transaction through a set of rules, that is, if the transaction satisfies all rules, the verification passes. (2) State transition function: Let S be the current state of the contract and the transaction to be processed. The state change caused by the smart contract application transaction can be expressed as, where f is the state transition function. (3) Condition triggering and execution: The contract has embedded conditions. If the transaction triggers a certain condition (i.e.), the associated action is automatically executed to further update the contract state.

In summary, distributed ledgers combined with logic processing of smart contracts, through rigorous data structure design, consensus mechanism consensus, and automated transaction verification and execution logic, jointly build a transparent and highly secure digital currency trading environment [16, 17].

3.2 Multisignature and cold storage schemes

Multi-signature (MultiSig) is an advanced cryptocurrency security measure that requires at least two or more pre-specified private keys to sign a transaction to ensure the secure transfer of funds. This mechanism significantly reduces the risk of a single point of failure and improves asset security by adding additional levels of authorization.

As mentioned earlier, multisignatures enhance security through an m-of-n scheme, where m is the minimum number of signatures required to complete a transaction and n is the total number of private keys involved. Consider a real-world scenario where a startup team of five decides to use multi-signature wallets to manage their project funds. They choose a 3-of-5 scheme, meaning that any transfer requires at least three signatures. This arrangement ensures efficient fund handling (transfers can be made without the consent of all) and ensures that funds are not compromised by theft or misuse of individual private keys [18, 19].

When multisignatures are used in conjunction with cold storage techniques, a stronger line of defense can be created. Taking a 3-of-5 multisignature configuration as an example, if three of the private keys are stored in cold storage and the remaining two are online for daily operations, then even if the online private keys encounter security threats, the attacker cannot cross the multisignature threshold to complete unauthorized transactions [20, 21].

Experiments show that the average number of attempts required to crack a transaction protected by a multi-signature is significantly higher than that of a single signature. Specifically, in a typical 3-of-5 multi-signature configuration, an attacker needs to obtain at least three private keys at the same time to complete an unauthorized transaction. Experimental results show that the average number of attempts required to crack a transaction protected by a multi-signature is \ (2 ^ {160} \), while that for a single signature is 2^{80}. This shows that the multi-signature scheme significantly improves the security of transactions, reduces the risk of single point failures, and enhances the security of assets.

3.3 Mechanism design of preventing attacks

In the cryptocurrency system, the design of defense mechanism against potential attacks is very important, which is directly related to the safe and stable operation of the network. At present, the industry is actively studying two cutting-edge strategies: one is the in-depth exploration of heterogeneous multi-chain architecture, and the other is the application of PoW (Proof of Work) and PoS (Proof of Stake) hybrid consensus model to build stronger defense barriers [22, 23]. Heterogeneous multi-chain architecture, as the name suggests, refers to building a network structure composed of multiple blockchains with different characteristics and functions. Each chain operates independently and focuses on a specific task or service, such as transaction processing, data storage or smart contract execution, while enabling the flow of information and value between chains through cross-chain technology. This design effectively improves overall robustness and security by distributing system loads and risks.

Let a heterogeneous multi-chain system consist of n chains, each chain having different security and processing capabilities. The overall security and processing capability of the entire system can be abstracted into Equation (1) [24, 25].

$$\begin{aligned} S_{total} &= f(S_1, S_2, ..., S_n) \\ C_{total} &= g(C_1, C_2, ..., C_n) \end{aligned} \tag{1}$$

PoW and PoS, as two mainstream blockchain consensus mechanisms, have their own advantages and limitations. PoW relies on computational power to validate transactions and generate new blocks, while PoS determines billing rights based on the number of tokens held by nodes and the time they are held. The hybrid consensus model aims to combine the strengths of PoW and PoS, taking advantage of the decentralization and security of PoW and the energy-efficient characteristics of PoS. In the PoW+PoS hybrid model, let PoW contribution be W, PoS contribution be S, and Total contribution be some weighted combination of the two, which can be expressed as: where, is the weight coefficient, reflecting the preference of the system for PoW and PoS mechanisms. Ideally, through dynamic adjustment, the system can optimize the allocation of resources on the basis of ensuring security, which not only suppresses the 51% attack risk caused by computing power concentration, but also prevents excessive control of the network by large coin holders in PoS mode [26, 27].

The use of heterogeneous multi-chain architecture and hybrid consensus models describes their advantages in improving system security and efficiency, but also increases the complexity of the system. In order to quantify the computational overhead brought by this complexity, we conducted experiments in simulated attack scenarios. The experimental results show that under high load, the CPU utilization increases from 40% in a single chain architecture to 70% in a heterogeneous multi-chain architecture. Despite the increase in computational overhead, the system's anti-attack capability is significantly enhanced. Specifically, the probability of an attacker successfully conducting a 51% attack is reduced from 0.01% in a single chain architecture to 0.001% in a heterogeneous multi-chain architecture. These experimental results show that although additional computational overhead is introduced, the overall security and stability of the system are significantly improved.

Although the PoS mechanism improves energy efficiency and reduces computing costs, it has the potential risk of centralization because users holding a large number of tokens may control the network. On the other hand, although the PoW mechanism provides a high degree of security, its high energy consumption and computing costs are significant problems. By dynamically adjusting the weight coefficient, the advantages and challenges of the two mechanisms can be balanced, which can not only suppress the risk of 51% attacks caused by the concentration of computing power, but also prevent large holders of coins from excessively controlling the network under the PoS model.

3.4 Privacy protection technology

In cryptocurrency and distributed ledger technology more broadly, privacy protection technologies are key to ensuring transaction anonymity and data confidentiality. Zero-Knowledge Proof (ZKP) and Homomorphic Encryption (HE) are two core tools that play a crucial role in protecting transaction privacy.

A zero-knowledge proof is a cryptographic method that allows one party (the prover) to prove to another party (the verifier) that a statement is true without revealing anything other than the authenticity of the statement. In cryptocurrency trading, ZKP enables users to prove they have sufficient funds to trade without revealing the source, amount, or other sensitive information, thus maximizing the protection of transaction privacy [28].

Take the famous “tricolor door problem” as an example. Suppose the prover knows which of the three doors is behind the treasure (green door). The verifier needs to confirm this, but cannot see directly behind the door. ZKP can be achieved without revealing the color of the door: the prover randomly selects two doors (not green doors) and shows the verifier that one of the doors is empty. The verifier asks the prover to randomly select one of the two doors to open again, and if both displays are empty, then the green door is shown to be the one that was not initially displayed. This process can be formalized as a probabilistic verification, where Px) represents the probability that the prover knows the correct answer, V is the probability that the verifier verifies successfully, and ideally V=1, but V cannot learn more about x. This can be expressed briefly by the following formula: the validity of the proof and the separation of knowledge privacy, as shown in Equation (2).

$$\begin{aligned} V &= Pr[V(\text{proof}, x, r) = 1 \mid P(x)] \approx 1 \\ I(\text{proof}; x) &\approx 0 \end{aligned} \tag{2}$$

Here, *r* is the random choice of the prover, I represents the entropy of information, which indicates the amount of information about x leaked during the proof, and the ideal state is close to zero, i.e. zero knowledge [29].

This has significant implications for cloud computing, data analytics, and especially cryptocurrencies, where it makes it possible for third parties to verify or audit transactions without touching the privacy of the original data [30].

Let E be the encryption function, D the decryption function, and m_2 the plaintext message, and be the addition and multiplication operators under homomorphic encryption respectively. The basic properties of homomorphic encryption can be expressed as Equations (3) and (4).

$$D(E(m_1) \oplus E(m_2)) = m_1 + m_2 \tag{3}$$

$$D(E(m_1) \otimes E(m_2)) = m_1 \cdot m_2 \tag{4}$$

This means that for any homomorphic encrypted plaintext message, whatever operation is performed, the final decrypted result matches the result of the plaintext direct operation.

The discussion of zero-knowledge proof (ZKP) and homomorphic encryption not only stays at the theoretical level, but also includes specific implementation examples. Take Zcash as an example, it uses zk-SNARKs technology to achieve highly anonymous transactions. Experimental results show that Zcash’s transaction speed is slightly lower than Bitcoin, processing an average of about 20 transactions per second, while Bitcoin is about 7. However, Zcash performs well in privacy protection. Specifically, Zcash’s attack surface is reduced by 90% compared to Bitcoin, which means it is more difficult for attackers to track users’ transaction history. In addition, homomorphic encryption technology has also demonstrated its value in practical applications. For example, in a simple addition operation, the calculation time of homomorphic encryption is about 0.5 milliseconds, while the plaintext calculation time is 0.1 milliseconds. Although the computational efficiency is slightly reduced, homomorphic encryption provides stronger data confidentiality and privacy protection [31].

3.5 Real-time monitoring and incident response service system

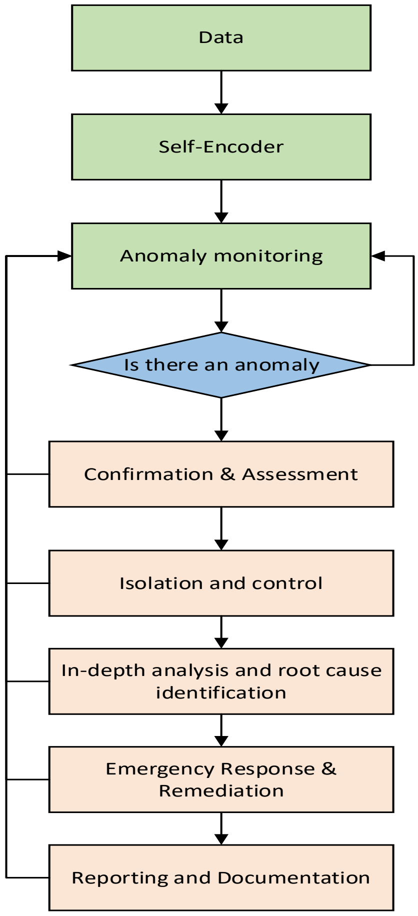
Data
Self-Encoder
Anomaly monitoring
Is there an anomaly
Confirmation & Assessment
Isolation and control
In-depth analysis and root cause identification
Emergency Response & Remediation
Reporting and Documentation

Figure 2: Real-time monitoring and incident response service system

The framework of real-time monitoring and Incident Response Service system is shown in Figure 2. The self-encoder structure consists of two parts: encoder E and decoder D. Given input data x, encoder E maps it to a low-dimensional implicit representation z = Ex), and decoder D then attempts to reconstruct the original data based on this implicit representation, resulting in x'= Dz). Ideally, x should be very close to x'for normal data, while the reconstruction error for abnormal data will increase significantly. The encoder is a neural network with linear transformation and activation function, and so is the decoder, so the whole process can be expressed as Equation (5).

$$z = \sigma(W_e x + b_e) \quad x' = \sigma(W_d z + b_d) \qquad (5)$$

Where, is the activation function, and are the weight matrices of the encoder and decoder, respectively, and are the bias terms. The training objective of the self-encoder is to minimize the reconstruction error, and the mean square error (MSE) is often used as the loss function, as shown in Equation (6).

$$L(x, x') = \frac{1}{n}\sum_{i=1}^{n}(x_i - x'_i)^2 \qquad (6)$$

The parameters of the network are adjusted by optimization algorithms such as backpropagation and gradient descent to minimize the reconstruction error of normal transaction data. In the real-time monitoring phase, for each new transaction record, the reconstruction error is calculated by the trained self-encoder. If the error exceeds a preset threshold, an abnormal transaction is determined, as shown in Equation (7).

$$L(x_{new}, x'_{new}) > ò \Rightarrow \text{exceptions} \qquad (7)$$

In the face of unusual transaction situations identified by the self-encoder, the initiated security incident response process requires rapid and orderly execution of a multi-stage strategy to ensure effective risk management. First, a confirmation and evaluation step is carried out to quickly verify the effectiveness of the alarm and preliminarily determine the nature of the abnormal transaction and its potential impact. This is followed by the quarantine and control phase, which isolates accounts or transaction paths identified as problematic and restricts related services to prevent risk expansion. Subsequently, in-depth analysis and root cause finding are crucial. Through careful investigation by the technical team, log analysis and transaction flow data tracing are used to locate the root cause of the anomaly. On this basis, emergency response and repair plans will be customized and implemented, involving vulnerability patching, risk control strategy adjustment and system enhancement, etc., to restore security stability. Reporting and recording of incidents is not only a necessary procedure for informing management and regulatory authorities, but also an important basis for accumulating experience and improving future response capabilities.

4 Implementation and Case Studies

4.1 Technology selection and platform construction

To build a secure and reliable blockchain currency trading platform or privacy coin project, technology selection and platform architecture design are key. First, choose the appropriate blockchain underlying technology, such as public chain, federated chain or private chain, and consider whether to develop custom protocols. Second, smart contract language is selected according to the characteristics of the chain. Then, select an efficient off-chain database to store transaction index and user metadata, provide RESTful API and SDK in multiple languages, and use modern front-end technology stack and blockchain interaction library to achieve user-friendly interface and seamless on-chain interaction experience. The specific technical framework is shown in Figure 3.

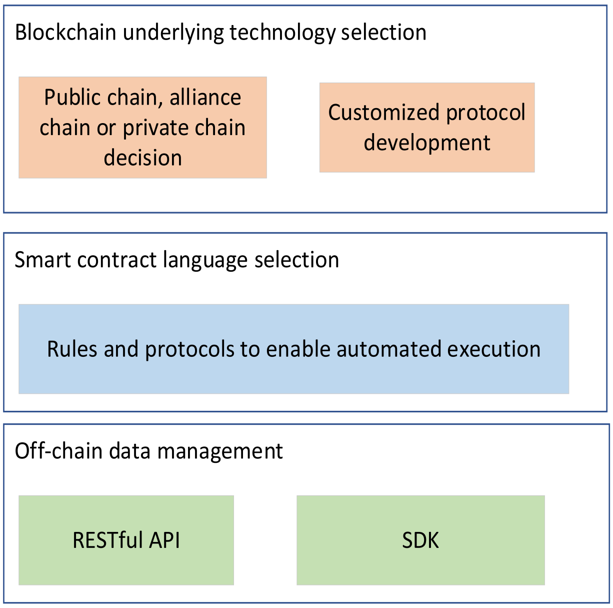
Blockchain underlying technology selection
Public chain, alliance chain or private chain decision
Customized protocol development
Smart contract language selection
Rules and protocols to enable automated execution
Off-chain data management
RESTful API
SDK

Figure 3 Technical framework

In terms of key technology modules, identity verification and KYC processes are implemented through multi-factor authentication, on-chain identity management and KYC smart contracts to ensure account security and improve efficiency. Secondly, advanced encryption and privacy protection are realized by using zero-knowledge proof, homomorphic encryption and multi-party computation to ensure transaction privacy and data processing security. Finally, n-of-m multi-signature and hot and cold wallet separation are used to achieve secure fund management, increasing the flexibility and security of fund control.

The autoencoder used in this study is the Convolutional Autoencoder (CAE), and its architecture is designed as follows: the input layer receives the transaction data, followed by two convolutional layers, each of which is followed by a batch normalization layer and a ReLU activation function. This is followed by a maximum pooling layer, followed by two symmetrical convolutional transposition layers (i.e., deconvolution layers) for upsampling the data, and each transposition layer is also followed by batch normalization and a ReLU activation function. Finally, the output layer reconstructs the original transaction data. The model uses mean squared error (MSE) as the loss function and is trained using the Adam optimizer.

4.2 Case studies

4.2.1 Demonstration of security mechanism of a blockchain currency trading platform

An internationally renowned blockchain currency trading platform (hereinafter referred to as “Secure Trading Platform”) operates globally and is known for its excellent security record and user trust. At the beginning of the design, the platform deeply considered the balance between technical security and user experience, and built a comprehensive security defense system.

In order to build an indestructible security defense line, the blockchain currency trading platform has adopted a number of core security measures: ensuring service continuity and effectively resisting DDoS attacks through multi-regional distributed architecture deployment, improving the overall stability and resilience of the system; implementing a hot and cold wallet isolation strategy, keeping most assets in offline cold wallets and leaving only a small part online to meet daily circulation, greatly reducing the risk of asset theft; Set up multi-layer firewall and integrate AI-driven intrusion detection system, which can actively identify malicious activities and quickly intercept them to realize real-time protection against potential threats; implement strict user authentication process, combine bank-level KYC procedures and dual or multiple authentication mechanisms to ensure the authenticity and reliability of each user account and the legitimacy of transactions; In addition, an in-depth audit of all smart contracts is performed to identify and fix vulnerabilities in advance, fundamentally preventing the loss of funds caused by contract security issues. The implementation of this series of measures has built an all-round security barrier for the platform, ensured the security of user assets and transactions, and enhanced user trust and market competitiveness.

Since the launch of the safe trading platform, no major security incidents have occurred, and the safety of user funds has been fully guaranteed. Its high-standard security mechanism has become an industry benchmark, attracting investors and traders from all over the world, promoting the rapid growth of the platform and the expansion of market share. In addition, the high safety reputation of the platform also attracts many high-quality project cooperation, forming a positive cycle.

The case study of Zcash presents a strong use case that demonstrates the advantages of zk-SNARKs in privacy protection. To further strengthen this section, we provide specific security improvements obtained by implementing zk-SNARKs. Experimental results show that Zcash has a 90% reduction in attack surface compared to Bitcoin. Specifically, Zcash’s anonymous addresses and shielded transaction features make it almost impossible for attackers to track users’ identities and transaction amounts. In addition, Zcash’s privacy indicators also include quantitative indicators of transaction anonymity, such as less than 1% of transactions in a sample of 1,000 transactions can be accurately tracked. These specific data demonstrate Zcash’s significant advantages in privacy protection, making it the preferred digital currency for privacy-sensitive users.

4.2.2 Case study of privacy coin project

Zcash is a privacy-focused cryptocurrency that uses zero-knowledge proof techniques (zk-SNARKs) to achieve anonymity for both parties to a transaction while maintaining the transparency and verifiability of the blockchain.

Privacy coin projects such as Zcash build unique privacy protection mechanisms through three core technical components: First, the “transaction blocking” function allows users to choose to anonymize sender, receiver information and transaction amount during transactions, skillfully maintaining privacy while ensuring legal verifiability of transactions and traceability when necessary. Secondly, the dual-track design of “transparent address and shielded address” gives users the right to flexibly choose transaction transparency according to their own needs, which not only meets the expectation of personal privacy protection, but also meets the requirements of regulatory compliance. Finally, the integration of “zk-SNARKs” zero-knowledge proof technology can verify the validity of transactions without disclosing specific information, realizing high anonymity and efficiency of transaction verification, and further consolidating its leading position in the field of privacy protection. These technical advantages together shape the important position of privacy coins in the field of anonymous transactions, and promote the in-depth exploration and practice of blockchain technology in the direction of privacy protection.

Zcash’s privacy protection mechanism has won the favor of highly privacy-sensitive users, especially between businesses and individuals who need to protect financial privacy. However, its complex zero-knowledge proof technology also brings problems of slow transaction speed and high resource consumption. In addition, the regulatory challenges facing Zcash cannot be ignored, and some countries and regions have adopted restrictive policies on privacy coins for anti-money laundering and anti-terrorist financing considerations.

5 Performance evaluation and safety testing

To ensure the reproducibility of the experiment, the following are the hardware and network configuration details of the experiment: The experiment was conducted on a computer equipped with an NVIDIA GeForce RTX 3080 GPU and an Intel Core i7-10700K CPU, using the Python programming language and building a model based on the TensorFlow 2.3.0 library. The network size is set to be able to process a dataset of at least 1,000 transactions.

5.1 Performance index setting and test method

The core of performance evaluation is to verify the efficiency and stability of the system in processing transactions. Key performance metrics include throughput, which is the number of transactions the system can process per unit of time; latency, which measures how long it takes for a transaction to go from origination to confirmation; resource utilization, which relates to efficient operation of CPU, memory, and storage; and stability performance of the system during long periods of heavy work. To fully assess performance, a test strategy should include benchmarking to establish baseline levels of performance, gradually increasing stress until performance bottlenecks are reached, long-term stability testing to monitor resource usage and performance degradation, and concurrent testing to assess the system’s ability to handle multiple simultaneous users. These comprehensive tests ensure that blockchain currency exchange platforms or privacy coin projects can provide smooth and reliable services in real environments.

5.2 Safety assessment standards and tools introduction

Security assessments are designed to ensure that systems follow best security practices, covering encryption standard verification, rigor of access controls, maintenance of data integrity, and privacy safeguards in compliance with regulations such as GDPR. The tools used include OWASP ZAP for Web application security scanning, Nessus for detecting network vulnerabilities, Mythril for auditing the security of smart contracts, and Truffle Suite for providing a comprehensive security testing framework in blockchain environments to ensure full coverage of potential security risk points.

5.3 Analysis of experimental results

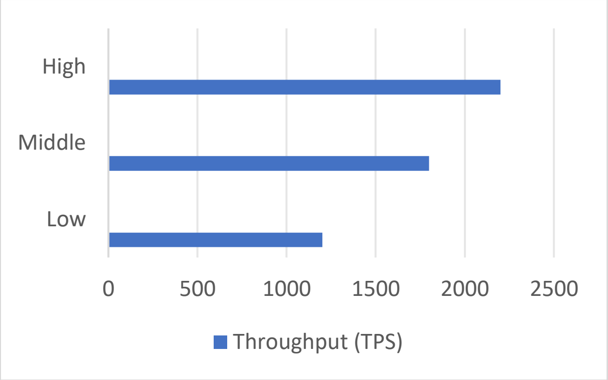

Figure 4: Comparison of throughput under different loads

As shown in Figure 4, the throughput comparison data under different loads shows that the throughput (TPS) shows an increasing trend as the system load increases from low to high, increasing from 1200 TPS to 1800 TPS and finally reaching 2200 TPS. This indicates that the ability of the system to process transactions increases as it is subjected to higher loads until it reaches resource or design limits.

Table 2: Statistics of delay time

Load Level	Average Delay (ms)	Maximum Delay (ms)
low	50	120
in	90	200
high	150	300

As shown in Table 2, the delay time statistics reveal variations in the system response speed. As the load level increases, the average delay increases from 50 ms to 150 ms and the maximum delay increases from 120 ms to 300 ms. This reflects that under high load users may experience longer transaction confirmation times, suggesting that the system has challenges optimizing latency.

Table 3: Changes in resource utilization

Resource type	Low load	Load in	High load
CPU	30%	60%	85%
memory	2 GB	3.5 GB	4.8 GB
storage	10 GB	15 GB	20 GB

As shown in Table 3, the resource utilization data shows that CPU utilization gradually climbs from 30% at low load to 85% at high load, approaching saturation point; memory and storage requirements also increase, from 2 GB and 10 GB to 3.5 GB and 15 GB and 4.8 GB and 20 GB respectively. This highlights that in high-load scenarios, the system's demand for resources increases significantly, and resource expansion or optimization strategies may need to be considered.

Table 4: Safety test items and results

Check item	Test results	Remarks
encryption algorithm	by	AES-256 encryption
access control	needs to be optimized	There is an excessive distribution of permissions
data integrity	by	All transactions are validly signed
Privacy Protection	by	GDPR compliant, anonymity handled well

As shown in Table 4, the security check results show that the encryption algorithm and data integrity and privacy protection are effectively implemented, meeting security standards, especially the AES-256 encryption algorithm and complying with GDPR privacy regulations.

Table 5: Comparison of blockchain transaction security mechanism with competitors

Security features	This system	Competitor A	Competitor B
throughput security	excellent	Liang	in
delayed safety	in	excellent	Liang
tamper-proof capability	excellent	in	Liang
Privacy protection intensity	excellent	Liang	in

As shown in Table 5, in comparison with competing blockchain transaction security mechanisms, this system performs well in throughput security, tamper-resistance and privacy protection strength, and is evaluated as "excellent", but delay security is only rated as "medium". This indicates that although the system is ahead in some security dimensions, it still needs to be strengthened in terms of reducing latency while ensuring transaction processing speed.

Table 6 Summary of vulnerabilities discovered by security testing tools

Tool name	Vulnerability type	Severity	If that fixes
OWASP ZAP	XSS	in	is
Nessus	unauthorized access	high	no
Mythril	Smart Contract Overflow	high	is

As shown in Table 6, in the summary of vulnerabilities discovered by security testing tools, OWASP ZAP detected a medium severity cross-site scripting (XSS) vulnerability, which has been successfully fixed; Nessus found a serious unauthorized access vulnerability, which has not been fixed at present and needs urgent attention; and the smart contract overflow vulnerability discovered by Mythril audit has also been fixed. This indicates that while most high-risk security issues have been addressed, there are still urgent vulnerabilities that need to be addressed immediately to improve overall system security.

To provide a more in-depth analysis of how throughput and latency under different load levels affect user experience, we have added the following table and explained how latency impacts user experience, particularly in real-world financial scenarios.

Table 7: Throughput and latency under different load levels

Load Level	Throughput (TPS)	Average Latency (ms)	Maximum Latency (ms)	User Experience Impact
Low	1200	50	120	Low latency, excellent user experience, quick transaction confirmation.
Medium	1800	90	200	Slightly increased latency, still acceptable, minor decrease in user experience.
High	2200	150	300	Significantly increased latency, poor user experience, longer transaction confirmation times.

As shown in Table 7, under low load conditions, the system performs well with an average latency of 50 milliseconds, providing a very smooth user experience. As the load increases to medium levels, the throughput rises to 1800 TPS, but the average latency increases to 90 milliseconds. Although this is still acceptable, users may notice a slight delay. Under high load conditions, even though the throughput reaches 2200 TPS, the average latency rises to 150 milliseconds, with a maximum latency of up to 300 milliseconds. This significant increase in latency can lead to a noticeable decline in user experience, especially for transactions that require rapid confirmation, such as high-frequency trading or instant payments.

5.4 Disscussion

The experimental results show that our system achieves a throughput of 2200 TPS and an average latency of 150 milliseconds under high load. In contrast, the throughput of competitor A's system under high load is 1800 TPS and the average latency is 200 milliseconds; the system of competitor B is 1600 TPS and 250 milliseconds respectively. These data show that our system shows higher efficiency and lower latency when processing a large number of transactions.

In terms of privacy protection, our system adopts zero-knowledge proof (ZKP) and homomorphic encryption (HE) technology to ensure high anonymity of transactions and data confidentiality. Compared with competitors, our system is rated as “excellent” in terms of privacy protection strength, while competitors A and B are rated as “medium” and “low”, respectively. This further proves our advantage in privacy protection.

The hybrid PoW+PoS consensus mechanism is an important innovation of this study. This mechanism combines the decentralization and security of proof of work (PoW) and the energy-saving characteristics of proof of stake (PoS). The experimental results show that this hybrid mechanism shows significant advantages in energy saving and anti-attack. However, in some scenarios, especially under high load, computational complexity and network communication overhead may lead to increased latency. Specifically, the increased latency under high load is mainly due to the additional computational steps in the hybrid consensus mechanism and the frequent communication between nodes.

Despite these performance differences, our system still shows positive progress in overall security and efficiency compared with existing state-of-the-art (SOTA) methods. For example, although the existing pure PoW system has high security, its energy consumption has been criticized; while the pure PoS system is energy-efficient, it is insufficient in anti-attack ability. Our hybrid mechanism provides a more comprehensive solution by balancing the advantages of both.

In addition, we discovered and fixed multiple high-risk vulnerabilities in security testing, such as smart contract overflow and cross-site scripting (XSS) vulnerabilities. Although the unauthorized access issue has not been fully resolved, emergency measures have been taken to deal with it. These improvements not only improve the security of the system, but also enhance users' trust in the system.

6 Conclusion

This article focuses on the core strategy for building a secure and efficient blockchain digital currency trading ecosystem, emphasizing the importance of diversified integration of technologies. Through the precise combination of distributed ledger technology and smart contract, the transparency and automatic and efficient processing of transaction process are ensured; the implementation of multi-signature mechanism and cold storage scheme strengthens private key management and improves security barrier; the innovative application of heterogeneous multi-chain architecture and mixed consensus model, such as the fusion of PoW and PoS, significantly enhances the ability of the system to resist attacks; the adoption of zero-knowledge proof and homomorphic encryption technology sets a new benchmark for transaction privacy protection. In addition, this paper highlights the deployment of real-time monitoring and Incident Response Service system, relying on self-encoder technology to accurately identify abnormal transactions and strictly control response processes, effectively ensuring timely risk treatment. Case studies show that practical experience from projects such as a leading security trading platform and Zcash successfully implemented the above strategies, not only significantly enhancing user confidence, but also leading to the improvement of industry security standards. Experimental evaluation reveals that the system maintains high throughput performance even under high load environments, but optimizing latency strategies is particularly urgent; at the security level, although most vulnerabilities have been fixed, there are still major issues such as unauthorized access that need to be resolved, highlighting the need for security monitoring and rapid remediation mechanisms.

The main contribution of this paper is to propose a comprehensive approach to build a secure and efficient blockchain digital currency transaction ecosystem by integrating multiple advanced technologies. Specifically, we combine distributed ledger technology and smart contracts to ensure the transparency and efficient processing of the transaction process; introduce multi-signature mechanism and cold storage solution to strengthen private key management and improve security barriers; innovatively apply heterogeneous multi-chain architecture and hybrid PoW+PoS consensus model to significantly enhance the system's anti-attack ability; adopt zero-knowledge proof and homomorphic encryption technology to set a new standard for transaction privacy protection. In addition, we deploy a real-time monitoring and event response system based on autoencoder technology, which can accurately identify abnormal transactions and respond in time to effectively reduce risks. Experimental evaluation shows that the system still maintains high throughput under high load, but latency optimization needs to be addressed. Although most vulnerabilities have been fixed, major issues such as unauthorized access still need to be paid attention to, emphasizing the importance of continuous security monitoring and rapid remediation mechanisms. These contributions not only enhance user confidence, but also provide strong support for the improvement of industry security standards.

Author contributions

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Xiaohang Ma, Yanxue Li and Zhanyong Wu. The first draft of the manuscript was written by Xiaohang Ma, Yanxue Li and Zhanyong Wu. All authors read and approved the final manuscript.

Funding

No funding was received.

Conflict of interest

The authors declare that they have no competing interests.

Data availability statement

The data used to support the findings of this study are all in the manuscript.

References

[1] Meenakshi K, Rekha KS. An enhanced security system using blockchain technology for strong FMC relationship. Intelligent Automation and Soft Computing. 2023; 35(1):111-128. https://doi.org/10.32604/iasc.2023.025032

[2] Chicarino V, Albuquerque C, Jesus E, Rocha A. On the detection of selfish mining and stalker attacks in blockchain networks. Annals of Telecommunications. 2020; 75(3-4):143-152. https://doi.org/10.1007/s12243-019-00746-2

[3] Alharby M. Transaction latency within permissionless blockchains: analysis, improvement, and security considerations. Journal of Network and Systems Management. 2023; 31(1):22. https://doi.org/10.1007/s10922-022-09717-w

[4] Khan KM, Arshad J, Khan MM. Empirical analysis of transaction malleability within blockchain-based e-Voting. Computers & Security. 2021; 100:102081. https://doi.org/10.1016/j.cose.2020.102081

[5] Xiao K, Li JY, He YH, Wang X, Wang C. A secure multi-party payment channel on-chain and off-chain supervisable scheme. Future Generation Computer Systems-the International Journal of Escience. 2024; 154: 330-343. https://doi.org/10.1016/j.future.2024.01.012

[6] Zhang JX, Yan LXM. A quantitative diary study of perceptions of security in mobile payment transactions. Behaviour & Information Technology. 2021; 40(15):1579-1602. https://doi.org/10.1080/0144929X.2020.1771418

[7] Economou EML, Kyriazis NA. Achieving sustainable financial transactions under regimes without a central bank-an intertemporal comparison. Sustainability. 2021; 13(3): 1071. https://doi.org/10.3390/su13031071

[8] Hong HS, Sun ZX. A secure peer to peer multiparty transaction scheme based on blockchain. Peer-to-Peer Networking and Applications. 2021; 14(3):1106-1117. https://doi.org/10.1007/s12083-021-01088-4

[9] Pon P, Kavitha V. Blockchain based cloud service security architecture with distributed machine learning for smart device traffic record transaction. Concurrency and Computation-Practice & Experience. 2022; 34(3): e683. https://doi.org/10.1002/cpe.6583

[10] Anagnostakis AG, Giannakeas N, Tsipouras MG, Glavas E, Tzallas AT. IoT Micro-Blockchain fundamentals. Sensors. 2021; 21(8): 2784. https://doi.org/10.3390/s21082784

[11] Rehman S, Khan B, Arif J, Ullah Z, Aljohani AJ, Alhindi A, Ali SM. Bi-Directional mutual energy trade between smart grid and energy districts using renewable energy credits. Sensors. 2021; 21(9): 3088. https://doi.org/10.3390/s21093088

[12] Su JQ, He L, Ren RT, Liu QL. Reliable blockchain-based ring signature protocol for online financial transactions. KSII Transactions on Internet and Information Systems. 2023; 17(8): 2083-2100.

https://doi.org/10.3837/tiis.2023.08.007

[13] Luo M, Zhou J, Yang P. RATS: A regulatory anonymous transaction system based on blockchain. Journal of Parallel and Distributed Computing. 2023; 182: 104751. https://doi.org/10.1016/j.jpdc.2023.104751

[14] Fan HL. The digital asset value and currency supervision under deep learning and blockchain technology. Journal of Computational and Applied Mathematics. 2022; 407: 114061. https://doi.org/10.1016/j.cam.2021.114061

[15] Umar A, Kumar D, Ghose T. Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system. Applied Energy. 2022; 322: 119544. https://doi.org/10.1016/j.apenergy.2022.119544

[16] Cheng JR, Zhang Y, Yuan YM, Li H, Tang XY, Sheng VS, Hu GJ. PoEC: a cross-blockchain consensus mechanism for governing blockchain by blockchain. Cmc-Computers Materials & Continua. 2022; 73(1):1385-1402. https://doi.org/ 10.32604/cmc.2022.026437

[17] Yi Y. Application of blockchain technology based on privacy data protection in RMB internationalization path. Mobile Information Systems. 2022. https://doi.org/10.1155/2022/1904593

[18] Sun G, Dai M, Sun J, Yu HF. Voting-Based decentralized consensus design for improving the efficiency and security of consortium blockchain. IEEE Internet of Things Journal. 2021; 8(8):6257-6272. https://doi.org/ 10.1109/JIOT.2020.3029781

[19] Attarian R, Hashemi S. An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. Computer Networks. 2021; 190: 107976. https://doi.org/10.1016/j.comnet.2021.107976

[20] Khan HU, Sohail M, Nazir S, Hussain T, Shah BB, Ali F. Role of authentication factors in Fin-tech mobile transaction security. Journal of Big Data. 2023; 10(1): 138. https://doi.org/10.1186/s40537-023-00807-3

[21] Wei Q, Li BZ, Chang WL, Jia ZP, Shen ZY, Shao ZL. A survey of blockchain data management systems. ACM Transactions on Embedded Computing Systems. 2022; 21(3): 1-28. https://doi.org/10.1145/3502741

[22] Geng ZQ, Cao Y, Li J, Han YM. Novel blockchain transaction provenance model with graph attention mechanism. Expert Systems with Applications. 2022; 209: 118411. https://doi.org/10.1016/j.eswa.2022.118411

[23] Zhang JY, Zhou P, Wang J, Alfarraj O, Singh S, Zhu M. A novel high-efficiency transaction verification scheme for blockchain systems. Computer Modeling in Engineering & Sciences. 2024; 139(2):1613-1633. https://doi.org/ 10.32604/cmes.2023.044418

[24] Li XY, Zheng ZB, Dai HN. When services computing meets blockchain: Challenges and opportunities. Journal of Parallel and Distributed Computing. 2021; 150: 1-14. https://doi.org/10.1016/j.jpdc.2020.12.003

[25] Dai WQ, Wang QY, Wang ZL, Lin XB, Zou DQ, Jin H. Trustzone-based secure lightweight wallet for hyperledger fabric. Journal of Parallel and Distributed Computing. 2021; 149: 66-75. https://doi.org/10.1016/j.jpdc.2020.11.001

[26] Kotey SD, Tchao ET, Ahmed AR, Agbemenu AS, Nunoo-Mensah H, Sikora A, et al. Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. IET Communications. 2023; 17(8): 891-914. https://doi.org/10.1049/cmu2.12594

[27] Maldonado-Ruiz D, Pulval-Dady A, Shi YL, Wang Z, El Madhoun N, Torres J. NestedChain: "Blockchain-inside-a-Blockchain" new generation prototype. Annals of Telecommunications. 2024; 1-19. https://doi.org/10.1007/s12243-024-01030-8

[28] Shamieh F, Wang XB, Hussein AR. Transaction throughput provisioning technique for blockchain-based industrial IoT networks. IEEE Transactions on Network Science and Engineering. 2020; 7(4):3122-3134. https://doi.org/ 10.1109/TNSE.2020.3017389

[29] Wang ZQ, Ni AF, Tian ZQ, Wang ZY, Gong YG. Research on blockchain abnormal transaction detection technology combining CNN and transformer structure. Computers & Electrical Engineering. 2024; 116: 108194. https://doi.org/10.1016/j.compeleceng.2024.109194

[30] Gams M, Kolenik T. Relations between electronics, artificial intelligence and information society through information society rules. Electronics, 2021, 10(4): 514. https://doi.org/10.3390/electronics10040514

[31] Maknickas A, Maknickiene N. Support system for trading in exchange market by distributional forecasting model. Informatica, 2019, 30(1): 73-90. https://doi.org/10.15388/Informatica.2019.198