Remittances Review
January, 2023
Volume: 8, No: 1, pp. 255-270
ISSN: 2059-6588 (Print) | ISSN 2059-6596 (Online)

Received: 11 November 2022 Accepted: 02 February, 2023
DOI: https://doi.org/10.33182/rr.v8i1.17

Feasibility Study of Future Digital Currency Based on Blockchain Technology

Mingshan Sun[1]*

Abstract

The feasibility study for blockchain digital currency is the basis for the future development of digital economy. In this paper, through the study of blockchain cryptography and consensus mechanism, we propose a blockchain-based future digital currency scheme, using associated ring signature to ensure the privacy of both sides of the transaction, introducing a third-party agent authorized by the payer to retrieve the transaction, and conducting performance analysis on the time and space overhead of digital currency transactions through simulation experiments, and studying the security against block interception attacks. The blockchain-based future digital currency has 37.79% less time overhead in the setup phase and 33.88% less in the payment phase than the lightning network under the condition that the number of transactions is 1000. In terms of space overhead, this solution is 29.12%, 27.07%, and 25.99% of Bitcoin at transaction counts of 500, 1000, and 1500, respectively. In the face of block interception attacks between mining pools, the fixed-value strategy and WSFS strategy perform the best. The future digital currency based on blockchain can effectively realize large-scale payments, make user data more difficult to be tampered with, provide more reliable identity authentication, and guarantee the security of digital currency.

Keywords: *blockchain technology, digital currency, consensus mechanism, performance analysis, security*

Introduction

In essence, blockchain belongs to a decentralized distributed database. The characteristics of blockchain technology are mainly reflected in common maintenance, traceability, and immutability, which make it play an important value in many fields of applications, such as decentralized software systems, Internet of Things, post-quantum cryptocurrencies, and federated malware detection in mobile devices (Li, Jiang, Chen, Luo, & Wen, 2020; Liu, Xie, Chen, Ma, & Gong, 2021). Bitcoin belongs to the first digital currency application based on blockchain technology, and it is the most typical and successful application of blockchain technology(Andrychowicz, Dziembowski, Malinowski, & Mazurek, 2016; Böhme, Christin, Edelman, & Moore, 2015; Göbel, Keeler, Krzesinski, & Taylor, 2016; Vranken, 2017). Subsequently though more digital currencies have emerged one after another, all of which originated from Bitcoin (Juhász, Stéger, Kondor, & Vattay, 2018).

[1] International College, National Institute of Development Administration, Bangkok, 10240, Thailand.
Corresponding author: Mingshan Sun (cliff13697@163.com)

In digital currencies, the individual nodes in the blockchain system are not completely anonymous. Each node in the blockchain has an address identifier, and although it is not directly associated with the real identity of the user, the transaction data stored on the blockchain is completely public, and the transaction records of any node can be viewed and even traced back to the source (Filippi D, 2015; Hur Y, 2015). With the rapid development of data analysis technology, if attackers analyze the transaction data of certain nodes, they can obtain the correlation information between transaction addresses and other private information of users, such as transaction characteristics and transaction patterns, and further infer the real identity information of users, thus seriously threatening their privacy. Therefore, it is of great importance to analyze the feasibility of blockchain digital currency (Wüst, Kostiainen, Capkun, & Capkun, 2018).

The study of digital currency feasibility involves knowledge of various aspects, including mathematics, cryptography, arithmetic, etc. The literature (Hansen & Delak, 2022) analyzes the security of existing cases of central bank digital currencies of various institutions and proposes improvement methods for some of the shortcomings. The literature (Delak & Hansen, 2022) argues that anonymity-based central bank digital currency inevitably poses certain risks to users and suggests that central banks can mitigate the risks of central bank digital currency by limiting the balance or modifying the liability rules. The literature (Rennie & Steele, 2021) investigates the social and economic policy choices involved in the design of central bank digital currencies and analyzes the impact of these policy choices on privacy, proposing that the loss of central bank digital currencies is reflected in the loss of anonymity, freedom, personal control, and regulatory control.

The literature (Guo S P, 2019), on the other hand, examines the Chinese digital RMB project from the perspective of digital currency payments, pointing out that the key to digital currency is how it can be linked to a broad ecosystem of economies to ensure the circulation of money and cash flows. The literature (Wu, Fan, Wang, & Zou, 2019) proposes a digital currency protocol for anonymous payments that can be supervised by an auditor and incorporates proof-of-work techniques to establish a regulatory system. The literature (L., 2020) analyzes the current challenges and opportunities for central banks to face the emerging digital currencies by examining private digital currencies. The literature (Yanagawa & Yamaoka, 2019) explores whether central banks should issue digital currencies, pointing out that the possible impact of payment efficiency, bank and fund intermediation, liquidity crises, and the transmission mechanism of monetary policy are all key issues in the development of digital currencies.

To address the problem that the feasibility study of future digital currency is not comprehensive enough, this paper first analyzes the similarities and differences of different blockchains in terms of identity identification and read/write authority, establishes a complete blockchain cryptographic chain based on RSA public key cipher, digital signature and hash function, and explores the principle of PoW consensus mechanism. Then, through the study of the origin and development of digital currencies, a blockchain-based future digital currency scheme is proposed, which gives three pairs of public-private key pairs each to the transaction initiator and the transaction receiver, while the initiator authorizes a third-party agent to retrieve them to ensure the anonymity of both parties to the transaction. At the same time, the transaction is guaranteed to be public by constructing an associated ring signature. Finally, the future digital currency scheme is simulated to simulate transactions, analyze its performance in terms of time overhead and space overhead, and use block interception to attack digital currency transactions and select the best management strategy based on the performance score.

Blockchain key Technologies

Classification of blockchain

Satoshi Nakamoto published a white paper on Bitcoin in 2008, in which the core technology of Bitcoin is introduced, and the blockchain technology is only a tamper-proof chain data structure used to record the history of Bitcoin transactions. The basic property of blockchain is a distributed ledger, and this ledger consists of multiple blocks strung together, allowing only the constant addition of data, with each block containing multiple transaction information (Dai, Zhang, Wang, & Jin, 2018; M., 2017). In order to adapt to various application scenarios and needs, blockchain technology is constantly expanding and evolving, and is no longer limited to data recording, but can also be used to perform more complex operations, and is generally classified into three categories: public, private, and federated chains. Table 1 compares the three types of blockchains from various aspects.

Table 1: Comparison of the three types of blockchains

Category	Identity	Performance	Access Rights	Consensus Mechanism	Scenarios
Public blockchain	Anonymity	Slow	Open read/write	POW/POS	Bitcoin, Ethereum
Private chain	Known identity	Fast	Restricted read/write	Raft/PBFT	Linux Foundation
Consortium chain	Known identity	Fast	Restricted read/write	Raft/PBFT	Fabric, Corda

The public chain is open to the whole network, and any node can freely choose to join or leave the blockchain network without getting authorization. The public chain is completely decentralized, and all nodes on the public chain have access to the full ledger record, initiate transactions, and compete for bookkeeping rights.

Private chains, in contrast to public chains, do not disclose their ledger information and have a limited range of participating nodes, with only authorized nodes having access to read operations. Private chains are generally used in enterprises or databases for management or auditing work, etc.

A federated chain is a blockchain that is maintained by a number of organized groups that have reached an agreement to work together. Only authorized nodes can join the federated chain and have read and write access. The data on the blockchain can be public or internal, and can be considered partially decentralized.

Blockchain Security

A large number of cryptographic techniques are cleverly used in blockchain systems and the use of these techniques brings various excellent properties to the blockchain. Hash functions are used to ensure data integrity, public-key cryptography and digital signatures help protect user privacy, and techniques such as zero-knowledge proofs and ring signatures are used in various newly proposed systems. Cryptography is the cornerstone of blockchain.

Public Key Cryptography

Public-key ciphers are also known as asymmetric ciphers. Public key ciphers use different keys for encryption and decryption, which are generally referred to as public and private keys. The public and private keys correspond to each other and are called key pairs. The public key is generated by the private key calculation, and the content encrypted by the public key needs the corresponding private key to be decrypted. The key holder sends the public key to others and keeps the private key properly for himself, avoiding the impact of key dissemination on the security of the system. Common public key cryptosystems are RSA, ElGamal and ECC.

The security of the RSA public key cryptographic algorithm comes from the difficulty of the prime factorization problem for large integers, but there is no theoretical proof that the factorization problem is necessarily intractable:

(1) Choose two large prime numbers p and q at random.

(2) Let $n = pq$, and then take:

$$\phi(n) = (p-1)(q-1) \quad (1)$$

Where n public, $\phi(n)$ confidential.

(3) Randomly select a positive integer $1 < e < \phi(n)$ that satisfies:

$$\gcd(e, \phi(n)) = 1 \quad (2)$$

e is the public key.

(4) Compute the private key d that satisfies:

$$de \equiv 1(\bmod \phi(n)) \quad (3)$$

(5) Encryption process: set the plaintext to $m \in Z_n$ and get the ciphertext:

$$c = m^e \bmod n \quad (4)$$

(6) Decryption process: the ciphertext is $c \in Z_n$, and the plaintext is obtained:

$$m = c^d \bmod n \quad (5)$$

Digital signatures

Digital signatures are mainly used to prevent tampering or forgery of data, and can also be used to identify both parties to a communication. Digital signatures are non-forgeable, non-reproducible, non-changeable and non-repudiation, making them an important safeguard against information fraud. A public key cryptography satisfying Equation (6) can be designed as a digital signature scheme:

$$E_{k_e}(D_{k_d}(x)) = x \quad (6)$$

Where E_{k_e} is the encryption transform, k_e is the encryption key, D_{k_d} is the decryption transform, and k_d is the decryption key. The message is generally hash transformed before digital signature, and the transformed message is signed, which on the one hand reduces the length of the required signature information and can speed up the signing process, and on the other hand prevents attacks against defects in the signature scheme. The process of digital signature is shown in Figure 1. When the digest obtained by user B after digest operation is the same as the digest obtained by reduction, it is proved that the message has not been tampered.

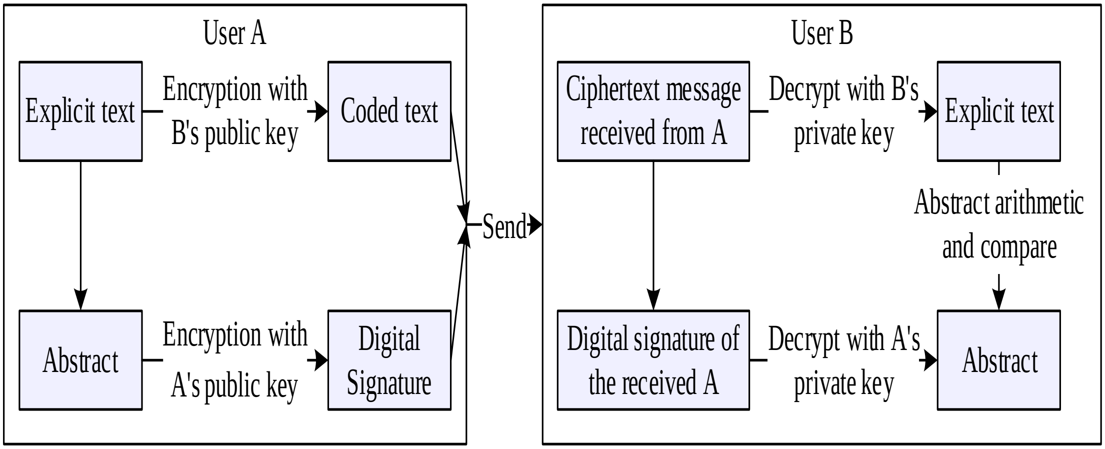
User A
Explicit text
Encryption with B's public key
Coded text
Abstract
Encryption with A's public key
Digital Signature
Send
User B
Ciphertext message received from A
Decrypt with B's private key
Explicit text
Abstract arithmetic and compare
Digital signature of the received A
Decrypt with A's private key
Abstract

Figure 1 Digital signature generation and verification process

Hash functions

The role of the hash function is to compress a string of any length into a fixed-length binary string, the output is called a summary, also known as a hash or hash value. The security of the hash function is reflected in the "anti-collision", because the hash function is a many-to-one mapping, when using the same hash function to calculate two different data, to get the same summary of the case is called a collision. According to the strength of security performance, there are weak collision-free and strong collision-free. Integrity, confidentiality and non-repudiation are the three basic attributes of information security, of which integrity verification is often done with the help of the anti-collision property of the hash function. When it is computationally infeasible for an attacker to get the original message based on the digest, the hash function is one-way also known as original image irreversible. Commitment schemes are a basic class of models in the field of cryptography, where the commitment is confidential and binding, and the commitment has to be able to hide the specific message, but when opened anyone can verify the correctness of the committed message, which includes two algorithms:

(1) Known message m, take the random value r, calculate the commitment value c:

$$c = \text{commit}(m, r) \tag{7}$$

(2) Determine whether the promise is true or not:

$$c == \text{verify}(c, m, r) \tag{8}$$

If the equation holds then the promise is true, if it does not then the promise is false.

Using hash function definition:

$$\text{commit}(m, r) = H(r \| m) \tag{9}$$

Collision resistance and unidirectionality guarantee promised confidentiality and binding, and these properties of hash functions are exploited in the non-interactive zero-knowledge proofs used in Zcash.The Bitcoin system applies two hash functions, SHA256 and RIPEMD160. SHA256 functions are used in the Merkle tree of block headers and block bodies to ensure data integrity. The Secure Hash Algorithm (SHA) is a family of hash functions published by the National Institute of Standards and Technology. SHA256 inputs a string of length less than 2^{64} bits and outputs a digest of length 256 bits. SHA256 calculates the message digest in two steps: the message is padded and expanded and divided into n blocks of 512 bits. Then the data blocks are compressed by the function respectively, the specific process is shown in Figure 2.

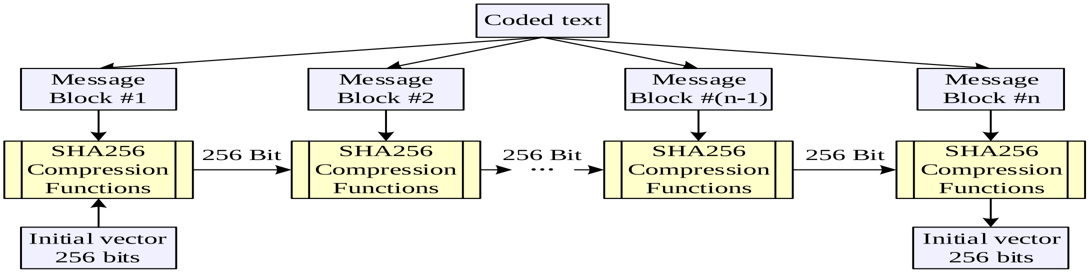

Figure 2 SHA256 work flow

The PoW mechanism in the blockchain consensus mechanism makes use of the puzzle-friendly property of the hash function. Difficulty friendly is defined as:If a hash function gets output y from n-bit input, k is a value in a high small entropy distribution. It is not possible to get x in time 2^n. In other words, it is hard to get y if some of the inputs are random. Assuming that the output range is extended to a subset Y of all possible values of the output, changing the range of Y can control the difficulty of the problem.

Blockchain consensus mechanism

Consensus mechanism is a key technology for blockchain networks to realize transactions between users who do not trust each other without central control. The result of consensus is to ensure the uniqueness of the blockchain ledger, and all nodes in the public blockchain can participate in the consensus process. The commonly used consensus mechanisms are proof-of-work (PoW), proof-of-stake (PoS), and practical Byzantine fault-tolerant algorithm (PBFT). In this paper, we focus on PoW mechanism.

When Satoshi Nakamoto proposed the Bitcoin system, he used PoW as the consensus mechanism. A common form of the PoW algorithm is:

$$H(Param \,||\, Nonce) < Target \tag{10}$$

Where $H(\cdot)$ denotes the hash function, $Param$ denotes some parameters associated with the block, $Nonce$ denotes a random number, and $Target$ denotes the target value, which is determined by the current difficulty value in the network. The first $Nonce$ node to compute the eligible block is awarded the bookkeeping right. PoW ensures that the higher the workload of a node, the higher its revenue.

An attacker who attempts to tamper with blockchain data must ensure that he has sufficient arithmetic power to support his calculation of the hash difficulty value including the block and subsequent blocks, and can achieve an attack chain that exceeds the length of the main chain. An actual attacker implementing such an attack would result in more losses than gains. However, the strong arithmetic power of PoW consensus mechanism also causes the waste of resources such as electricity, which is a major drawback of PoW.

PoW is a completely decentralized design without considering the concentration of arithmetic power, participants prove credit with workload also known as behavior, and anyone can participate with complete anonymity. Participants with more currency in PoW become big bankers in the system and gain revenue easier than other participants, thus encouraging hoarding of currency in the system and destroying the liquidity of the system. Nodes also accumulate offline coin age, and rewards weaken the promotion of node participation in consensus, making it easy to lack enough nodes to participate in consensus.

Blockchain-Based Digital Currency

Development of Digital Currency

Digital money is derived from E-Cash, an untraceable electronic payment scheme proposed by David Chaum in 1982. It is considered to be the earliest electronic money system, which used blind signatures to build an anonymous electronic money system based on the "consumer-bank-merchant" model. Since banks were involved as third-party institutions, it was clearly a centralized e-money scheme that had to rely on banks (central nodes) to complete transactions properly and did not support direct transactions between users. On this basis, various electronic cash systems have been proposed, all of which are centralized e-money schemes. A centralized digital currency transaction scheme usually consists of a withdrawal protocol, a payment protocol, and a deposit protocol, in which there are three participants: the consumer, the bank, and the merchant.

Bitcoin, on the other hand, uses blockchain technology with an open distributed ledger at its core, without any three-party institutions involved in the transaction. Bitcoin has significant advantages over centralized digital currencies, and its transaction model is shown in Figure 3. The emergence of Bitcoin has revolutionized the traditional "consumer-bank-merchant" model of digital currencies. Unlike traditional digital currencies, Bitcoin is a new type of decentralized digital currency that uses peer-to-peer transactions and does not rely on any central institution. A bitcoin transaction first needs to be sent to the bitcoin network in order to be propagated and thus verified by more nodes. When it is successfully verified by a mining node and that miner successfully performs the mining operation, the transaction can be added to a new block, and eventually the new block is added to the blockchain to indicate a successful transaction.

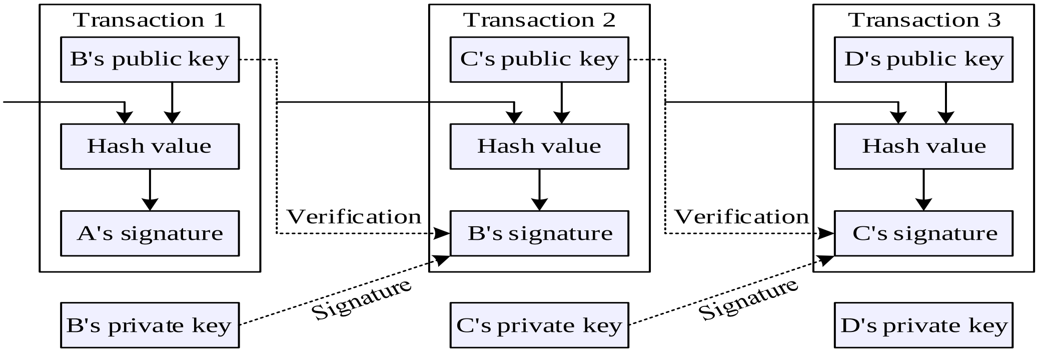

Figure 3 Bitcoin transactions

Mining is the process by which miners perform a large number of mathematical operations in order to generate new blocks, which can be understood as proof of workload. Each node in the Bitcoin network consumes arithmetic power to find the answer to a mathematical puzzle and compete for the right to book a new round of transactions. The node with the higher power output is more likely to find the solution to the mathematical problem, and the node that solves the problem first gets the bookkeeping rights, which not only rewards the node with a certain number of bitcoins for successful mining, but also takes a certain amount of transaction fees from these bitcoin transactions.

Blockchain-based digital currency transactions

Blockchain digital currency trading scheme

To ensure the anonymity of both the transaction initiator and the transaction receiver, each of the transaction initiator and the transaction receiver has three pairs of public-private key pairs, including one pair of primary public-private key pairs and two pairs of secondary public-private key pairs, as shown in Table 2. The first-level public-private key pair is used to generate the associated ring signature $\sigma(m)$, and the second-level public-private key pair has two roles: one is used to generate a virtual intermediate address, and the other is used to authorize agents to retrieve transactions on the blockchain. This scheme has three entities: Alice, the transaction initiator, Bob, the transaction recipient, and Carlo, the agent, a virtual intermediate address. The intermediate address in this scheme is similar to the hidden address in the CryptoNote protocol, but the difference is that in this scheme, each party to the transaction has three pairs of public and private keys, and an agent is introduced to help the transaction recipient retrieve the transactions on the blockchain, and the user Bob can also use his private key to check whether there is a transaction belonging to him on the blockchain.

Table 2 Public and Private Keys of the user

User	Public and Private Keys	Condition	Description
Alice	First-level public and private keys	$K_{a1} = k_{a1}P$	K_{a1} is the public key, k_{a1} is the private key.
	Second-level public and private keys	$K_{a2} = k_{a2}P$ $K_{a3} = k_{a3}P$	K_{a2} and K_{a3} is the public key, k_{a2} and k_{a3} is the private key.
Bob	First-level public and private keys	$K_{b1} = k_{b1}P$	K_{b1} is the public key, k_{b1} is the private key.
	Second-level public and private keys	$K_{b2} = k_{b2}P$ $K_{b3} = k_{b3}P$	K_{b2} and K_{b3} is the public key, k_{b2} and k_{b3} is the private key.

Blockchain Digital Currency Transaction Process

Let E be an elliptic curve defined over a finite field $GF(p)$, G be a cyclic subgroup on an elliptic curve E, P be a generating element of group G, and q be the order of generating element P. Let H be a collision-resistant Hash function:

$$H:\{0,1\}^{*} \rightarrow ¢_{P} \tag{11}$$

Alice wants to pay a sum of money to Bob, generating a transaction slip as shown in Figure 4. It contains the address of the receiver, the payment amount, the payment voucher, the timestamp, and the signature of the sender. Assumption m represents the transaction information. In fact, Alice pays this amount to the intermediate address, not to Bob's real address.

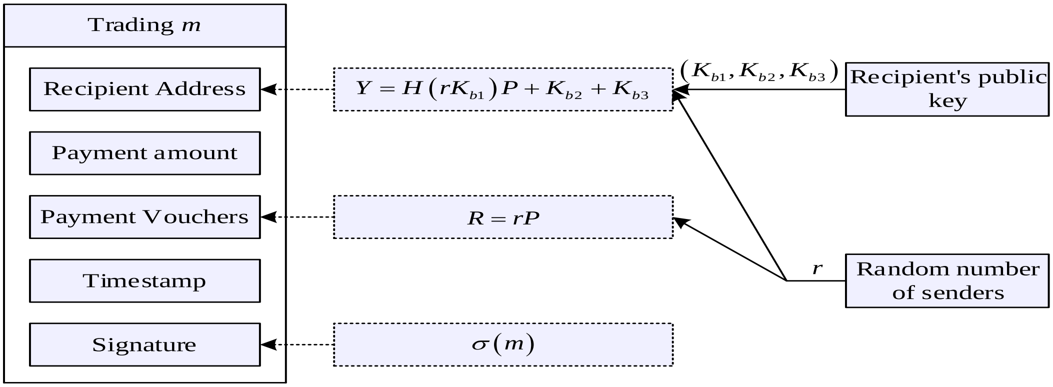

Figure 4 Payment for agreement orders

Alice generates a transaction as follows:

(1) Obtain Bob's primary public key K_{b1}, secondary public keys K_{b2} and K_{b3} from the blockchain.

(2) Randomly select $r \in [1, q-1]$ and calculate:

$$R = rP \tag{12}$$

$$Y = H(rK_{b1})P + K_{b2} + K_{b3} \tag{13}$$

It is assumed that the address of the recipient (intermediate address), which represents the payment credentials, serves to prevent repudiation by the recipient.

(3) Send R to Bob.

(4) Construct the associated ring signature $\sigma(m)$. where μ represents the signature of the previous transaction corresponding to the current transaction, which represents the source of the funds in the current transaction, and it is public and unique on the blockchain.

(5) The timestamp is the current system time automatically generated by the blockchain.

(6) Finally, Alice broadcasts the transaction anonymously to the blockchain.

When the recipient of a transaction, Bob, has limited computing resources, he authorizes the agent Carlo to retrieve the transaction on the blockchain, and Bob sends a portion of the processed public key anonymously, without revealing his true identity. The steps for retrieving a transaction are as follows:

(1) Bob calculates:

$$R^* = k_{b1}R \tag{14}$$

$$K^* = K_{b2} + K_{b3} \tag{15}$$

The binary (R^*, K^*) is then sent to Carlo anonymously with a proxy fee.

(2) Carlo computes:

$$Y^* = H(R^*)P + K^* \tag{16}$$

Then retrieve on the blockchain whether a transaction exists that satisfies $Y^* = Y$. If it exists, it means that the transaction belongs to Bob and Carlo makes an announcement about it. Otherwise, it means that no transaction belonging to Bob has been retrieved.

(3) Once Bob learns of Carlo's announcement, he goes to the blockchain to find the transaction.

(4) To make sure the deal belongs to him, Bob once again calculates:

$$H(rK_{b1})P + K_{b2} + K_{b2} \tag{17}$$

The Feasibility of Blockchain Digital Currency

Performance analysis of digital currency transactions

For the purpose of performance analysis of blockchain-based digital currency solutions, this solution is compared with the Lightning Network. The Lightning Network (LN) is a Layer 2 protocol that acts like an overhead bridge over a highway, making multiple payments over a large network of bi-directional channels without having to record each transaction on the Bitcoin blockchain. This avoids the bitcoin transaction rate limitations and allows for faster transactions and greater capacity at a lower cost. The same transaction process is set up in the same system environment, with a setup phase, a payment phase and a settlement phase.

A comparison of the computational overhead of the blockchain transaction scheme and the lightning network transaction scheme is shown in Figure 5. When the consumers are 500, the computational overhead of blockchain in the setup phase is 2033 ms and that of the lightning network is 3271 ms, and blockchain is going to reduce the computational overhead by 37.85%. The computation overhead of the blockchain in the payment phase is 1479 ms, and the computation overhead of the lightning network is 1991 ms, which reduces the computation overhead by 25.72%. The computational overhead of the blockchain in the settlement phase is 2830 ms, and that of the lightning network is 2748 ms, which is an increase of 2.98%. When the consumers are 1000, blockchain digital currency transactions reduce the computational overhead by 37.79% in the setup phase, 33.88% in the payment phase, and only 5.79% in the calculation phase compared to the lightning network.

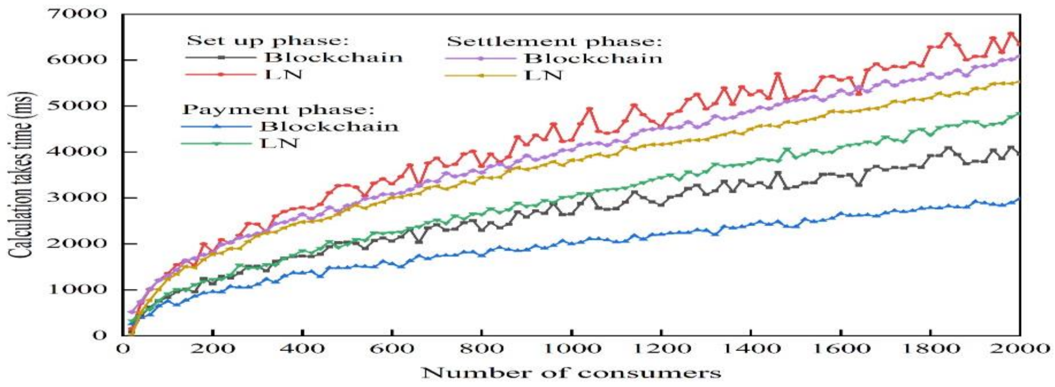

Figure 5 Computational overhead for digital currency trading schemes

In addition to the time overhead, the space overhead is also an important measure of the feasibility of digital currency transactions. A comparison of the digital currency scheme in this paper with Bitcoin in terms of space occupied per transaction is shown in Figure 6. Bitcoin in terms of occupied space varies linearly with the number of transactions. When the number of transactions is 250, Bitcoin requires 93.25 KB of space and this scheme is 29.03 KB, which is 68.87% smaller than Bitcoin. When the number of transactions rises to 500, 1000, 1500, and 2000, this solution is 70.88%, 72.93%, 74.01%, and 75.64% smaller than Bitcoin in terms of space overhead, respectively. On average, this solution requires 70.34% less space than Bitcoin for digital currency transactions.

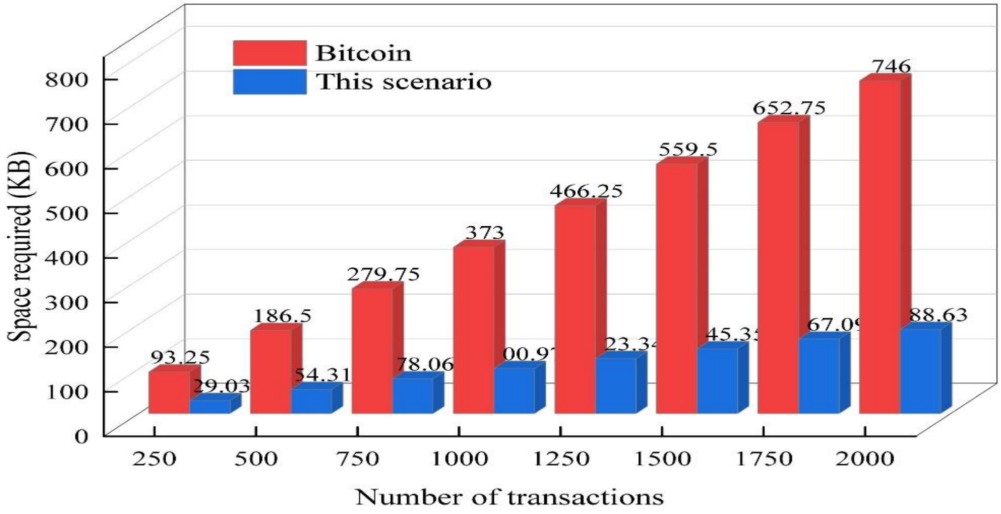

Figure 6 Digital currency trading takes up space

Security Analysis of Digital Currency

Since it is difficult for a single miner to mine new blocks with his own arithmetic power, the output of mainstream digital currencies is currently carried out in mining pools. In this paper, we conduct simulation experiments using block interception attacks among mining pools to compare the performance against attacks under different blockchain strategies, and the average score ranking is shown in Figure 7. The top three performance against attacks are fixed-value strategy, WSFS, and ALLC, with average scores of 1.38, 1.32, and 1.3, respectively. Among the traditional IPD, TFT strategy and Grim strategy perform the best. In this mining pool game model, the fixed-value and WSFS strategies perform best, and the fixed-value strategy is better than the traditional WSFS. The ALLD strategy has a score of 0.73, which is not a loss in any single game, but is a poor strategy in general. In general, bona fide strategies that choose to cooperate for the first time and are more inclined to do so perform better than greedy strategies.

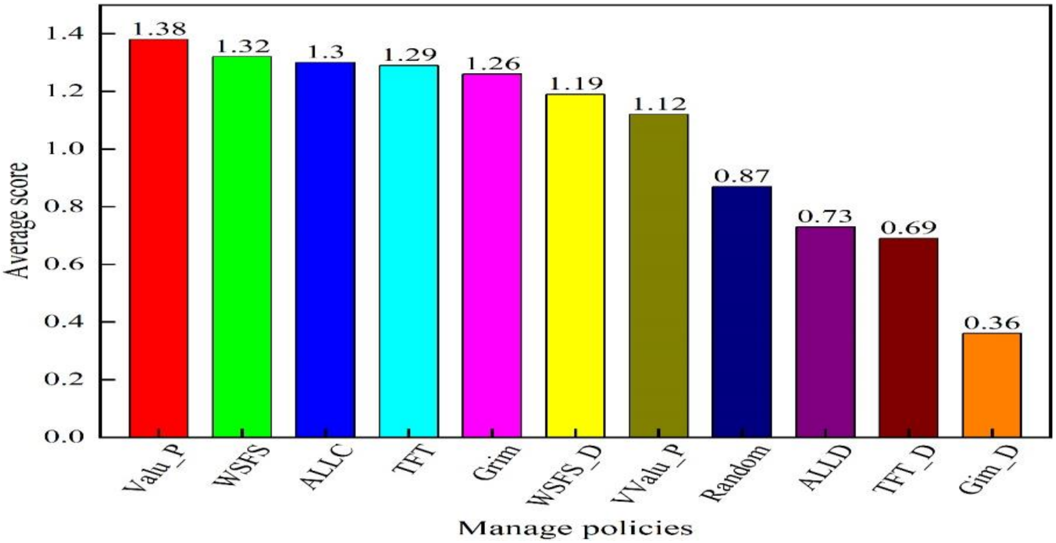

Figure 7 The performance of different strategies to respond to attacks

Based on the results, this paper suggests that mining pool managers adopt a fixed-value strategy or a WSFS strategy. This can protect their own revenue while making rival mining pools tend to cooperate, thus not only reducing the probability of block interception attacks occurring, but also effectively mitigating the losses caused by block interception attacks.

Conclusion

In this paper, we propose a future digital currency scheme based on blockchain technology and study its performance performance and security against attacks during transactions. This scheme reduces the computation time overhead by 37.79% and 33.88% in the setup phase and payment phase, respectively, compared to the lightning network. In terms of space overhead this scheme reduces 70.34% on average compared to Bitcoin.

(1) The birth of blockchain technology has provided the possibility of virtualizing physical money in society, while the value reliance of money itself has evolved, from the earliest physical value to the value of trust in science, technology and information systems today.

(2) The payment channel in the blockchain protocol can support a large number of off-chain transactions and amortize transaction costs. Linked-loop signatures, on the other hand, compress the transaction data volume from the data structure of the transaction itself, effectively reducing the transaction data.

(3) Blockchain network nodes only need to verify the final settlement transaction once to verify all the committed transactions, which greatly reduces the transaction cost.

(4) The adoption of a fixed-value strategy by mining pool managers not only effectively reduces the chance of block interception attacks with other mining pools and reduces the risk of the blockchain system being paralyzed by block interception attacks, but also enhances the performance of the blockchain system.

REMITTANCES
REVIEW

References

Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2016). Secure multiparty computations on bitcoin. *Communications of the ACM, 59*(4), 76-84.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives, 29*(2), 213-238.

Dai, M., Zhang, S., Wang, H., & Jin, S. (2018). A low storage room requirement framework for distributed ledger in blockchain. *IEEE access, 6*, 22970-22975.

Delak, K., & Hansen, T. (2022). Security Considerations for a Central Bank Digital Currency. *FEDS Notes*(2022-02), 03-01.

Filippi D, P. (2015). Handbook of Digital Currency. 463-483.

Göbel, J., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2016). Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation, 104*, 23-41.

Guo S P, Y. F. (2019). Currency Revolution: Financial Effects, Risks and Challenges of Issue of Digital Currency in China. *Journal of Shenzhen University (Humanities & Social Sciences),* .

Hansen, T., & Delak, K. (2022). Security Considerations for a Central Bank Digital Currency.

Hur Y, J. S., Yoo B. . (2015). Is Bitcoin a Viable E-Business? : Empirical Analysis of the Digital Currency's Speculative Nature.

Juhász, P. L., Stéger, J., Kondor, D., & Vattay, G. (2018). A bayesian approach to identify bitcoin users. *PloS one, 13*(12), e0207000.

L., M. J. (2020). How Did We Get Here? From Observing Private Currencies to Exploring Central Bank Digital Currency. *Payments System Research Briefing*.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems, 107*, 841-853.

Liu, J., Xie, M., Chen, S., Ma, C., & Gong, Q. (2021). An improved DPoS consensus mechanism in blockchain based on PLTS for the smart autonomous multi-robot system. *Information Sciences, 575*, 528-541.

M., G. (2017). Australia's Dial Currency Opens Avenues for Renewables Trading. *International environment reporter, 40*(18), 982-983.

Rennie, E., & Steele, S. (2021). Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency. *Law, Technology and Humans, 3*(1), 6-17.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability, 28*, 1-9.

Wu, Y., Fan, H., Wang, X., & Zou, G. (2019). A regulated digital currency. *Science China Information Sciences, 62*, 1-12.

Wüst, K., Kostiainen, K., Capkun, V., & Capkun, S. (2018). PRCash: Centrally-Issued Digital Currency with Privacy and Regulation. *IACR Cryptol. ePrint Arch., 2018*, 412.

Yanagawa, N., & Yamaoka, H. (2019). *Digital innovation, data revolution and central bank digital currency*. Retrieved from