Received October 18, 2020, accepted October 29, 2020, date of publication November 5, 2020, date of current version November 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3036004

Security Assessment of Blockchain in Chinese Classified Protection of Cybersecurity

DI WANG[1], YAN ZHU[1], (Member, IEEE), YI ZHANG[1,2], AND GUOWEI LIU[3]

[1] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
[2] Institute of Software Chinese Academy of Sciences, Beijing 100190, China
[3] Beijing Municipal Bureau of Economy and Information Technology, Beijing 101101, China

Corresponding author: Yan Zhu (zhuyan@ustb.edu.cn)

This work was supported in part by the National Key Technologies Research and Development Programs of China under Grant 2018YFB1402702, in part by the National Natural Science Foundation of China under Grant 61972032, and in part by the Beijing Municipal Bureau of Economy and Information Technology under Grant HTBH_20200901_573.

ABSTRACT Classified protection is one of primary security policies of information system in many countries. With the increasing popularity of blockchain in various fields of applications, it is extremely necessary to promote classified protection for blockchain's risk assessment in order to push forward the sustainable development of blockchain. Taking the Level 3 in Chinese classified protection 2.0 as an example, this paper proposes the common evaluation rules on blockchain to ensure that blockchain can meet the needs of countries to build it as critical infrastructure. Both assessment requirements and enforcement proposals are presented and analyzed from the standpoint of blockchain's core technologies, e.g., peer-to-peer network, distributed ledger, contract's scripting system, and consensus mechanism. Moreover, the assessment results on three main platforms, Bitcoin, Ethereum, and Hyperledger, are summarized and analyzed in compliance with the control points specified in the level 3. Our investigation indicates that the current blockchain is able to satisfy the requirements of evaluation items in many aspects, such as software fault tolerance, resource control, backup and recovery, but further improvements are still needed for some aspects, including security audit, access control, identification and authentication, data integrity, etc., in order to satisfy the requirements of important fields on national security, economic development and human life.

INDEX TERMS Blockchain, classified protection of cybersecurity, peer-to-peer network, consensus mechanism, assessment and analysis.

I. INTRODUCTION

Blockchain is a cryptographic decentralized ledger and network transaction accounting system that can provide secure electronic transaction services without relying on trusted third parties [1]. As technology's rapid advancement continues, blockchain has gradually become a hot spot in the development of information technology. Due to its cryptographic structure, P2P network, consensus mechanism, smart contract and other mechanisms, blockchain has the characteristics of decentralization, tamper resistance and traceability, which make blockchain suitable for public sector organizations. In particular, the permissioned blockchain is a better choice for governments because all parties provide a degree of trust to central authorities, allowing the choice of consensus mechanisms that are more efficient and less expensive than permissionless blockchain [2].

The application of blockchain has been extended to many fields including medical care [3], copyright [4], law [5], asset management [6], etc. Many governments around the world are investing heavily in blockchain technology and its industrial applications, including Russia, the United Kingdom, China, the United States and Canada. In the United States, government agencies are deploying blockchain to various areas such as supply chains, medical records, and financial services, while several federal agencies, including the General Services Agency (GSA), the Department of Homeland Security (DHS) and the Department of Health and Human Services (HHS), have announced blockchain initiatives. In the United Arab Emirates, the government is exploring a variety of use cases, including business registration, trade, and central banking. In China, blockchain technology

The associate editor coordinating the review of this manuscript and approving it for publication was Zhaojun Li.

has made great progress in finance market, insurance technology, cross-border payment and central bank digital currencies. It can be seen that blockchain has brought a lot of innovation and breakthrough, but various potential security risks are also causing widespread concern, e.g., using components with vulnerabilities, insecure deserialization, sensitive data exposure and security misconfiguration.

In order to avoid the potential risks of blockchain, the most effective way is to conduct strict security assessment on it and particularly blockchain used by some government departments is set up as national infrastructure, which needs to meet higher security requirements. The protection of national critical infrastructure is based on the classified protection assessment system in many countries around the world, which can effectively improve the security protection capability of the information system and reduce the risk of various attacks once the system is modified.

Blockchain has passed into an maturity stage of development, and its assessment must be advanced synchronously. According to the ideas of classified protection, the evaluation criteria should be formulated for specific technologies in terms of general security requirements, e.g., assessment specifications have been gradually produced in cloud computing, mobile internet, internet of things, industrial control, big data and other areas. As for blockchain technology, some organizations and groups has initiated the development of blockchain assessment specifications, e.g., the Chinese Blockchain Evaluation Alliance (CBEA) has introduced the ''Grading Evaluation Specification for Blockchain and Distributed Ledger Information System''. However, the above-mentioned works does not apply the classified protection criteria to the formulation of blockchain assessment specifications.

The implementation purpose of classified protection [7], [8] is to guide the security management of various industries, regulate the supervision and evaluation institutions, and promote the significance of the cybersecurity. Therefore, the security classified protection is imposed by some countries, e.g., the *Cyber Security Law of China* (CSLC) [1] stipulate that the state implements a cybersecurity classified protection scheme and give priority protection to important industries and fields such as public communications, information services and energy, as well as other critical information infrastructure on the basis of it. Hence, it is necessary to carry out the research of blockchain-oriented classified protection and evaluation methods according to current standards.

The purpose of this paper is to address the current situation of rare researches on blockchain evaluation under classified protection for proposing the common evaluation rules on several popular blockchain platforms. Our research will take the chinese *Classified Protection of Cybersecurity* (CPC) 2.0 as an example, and the level 3 of Critical National Information Infrastructure (CNII) in CPC 2.0 (called CPC-2.0-L3) will be set as our target considering that the security protection strength of blockchain is at least level 3 as national network infrastructure according to the CSLC. In this paper, the focus of our research is to present and analyze assessment requirements and enforcement proposals on blockchain's core technologies, e.g., peer-to-peer network, distributed ledger, contract's scripting system, and consensus mechanism. Moreover, the assessment results on three main platforms, Bitcoin, Ethereum, and Hyperledger, are summarized and analyzed in compliance with the control points specified in the CPC-2.0-L3.

Our investigation indicates that the current blockchain is able to satisfy the requirements of evaluation items in many aspects, such as software fault tolerance, resource control, backup and recovery, but further improvements are still needed for some aspects, including security audit, access control, identification and authentication, data integrity, etc., in order to satisfy the requirements of important fields on national security, economic development and human life. Our result and exploration on Chinese CPC 2.0 will benefit the other countries as well.

II. PAPER ORGANIZATION

The rest of the paper is organized as follows. In section III, the classified protection is outlined. Section IV summarizes the blockchain's architecture. In sections V to VII, the assessment requirements are respectively proposed to peer-to-peer (P2P) network, consensus mechanism and distributed ledger in the blockchain. Section VIII summarizes the smart contract and the security audit mechanism based on log workflow in the blockchain system. Finally, we conclude the paper in Section IX.

III. CLASSIFIED PROTECTION OUTLINE

Classified protection is one of fundamental policies of information security, which basic idea is to classify different objects of protection so as to manage and supervise them according to standards. Classified protection work has already been carried out in many countries: the U.S. Department of Defense (DoD) established the National Computer Security Center (NCSC) in the 1980s, and the Trusted Computer System Evaluation Criteria/Orange Book (TCSEC) stimulated international security assessment work published in the 1990s. Subsequently, the confidentiality, integrity and availability (CIA) of information security have been proposed for the first time in the Information Technology Security Evaluation Criteria/ European White Paper (ITSEC), which marks the international information security research reach a higher stage of development. In 1996, the USA, Canada, and European Community (EC) absorbed advanced experience from countries including the White Paper, the Canadian trusted computer product evaluation criteria (CTCPEC), and the ISO: SC27WG3 security assessment standards, then published the Common Criteria (CC) for Information Technology

[1] Cybersecurity Law of the People's Republic of China, 2016, [Online]. Available: http://www.lawinfochina.com/display.aspx?id=a9bc8a6c2ad2ad03bdfb&lib=law

TABLE 1. The relation between grading elements and safety level.

Level Object Degree	Citizen Corporations	Social Order, Public Interest	National Security
General Damage	Level 1	Level 2	Level 3
Significant Damage	Level 2	Level 3	Level 4
Especially Significant Damage	Level 3 *	Level 4	Level 5

* Level 2 in classified protection 1.0.

security Evaluation. On the basis of CC standards, each country has set up a national classified protection strategy that suits its own national conditions.

The U.S. government has issued a number of presidential executive orders to protect classified information and to promote its economic and technological interests. The Executive Order 12829 [9] establishes a National Industrial Security Program to safeguard Federal Government classified information, Executive Order 13526 [10] Executive Order 13549 [11] 13556 [12] 13587 [13] respectively provides additional protection methods for other classes of information, named for the ''Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities'', ''Controlled Unclassified Information'' and ''Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information''. The promulgation and implementation of executive orders gives the U.S. a clearer guideline for its conduct in cybersecurity.

The U.K. policy papers on classified protection are published by the Cabinet Office. The *Government Protective Marking Scheme* (GPMS) [14] was used before 2014, which used five levels to classify information: unclassified, protect, restricted, confidential, secret and top secret. In 2014, the *Government Security Classifications Policy* (GSCP) [15] replaced the old scheme to be the current classification system, which divides data into official, secret and top secret based on the ability and motivation of the potential attacker, and each of their classes sets a baseline of security controls and provides appropriate protection against typical threats.

Although the classification system varies from country to country, most have levels (from highest to lowest) corresponding to the following British definitions. European institutions have four levels: EU top secret, EU secret, EU confidential, EU restricted based on the degree of damage to the basic interests of the European Union or one or more member states caused by the unauthorized disclosure of the information and materials. Russia has classified documents from high to low: OB (Particularly important), CC (completely secret,), C (secret), limited access, and set official identities with corresponding powers over the corresponding levels of documents.

China has established the computer information security classified protection system [16] based on the construction and management of information systems, and formulated security assessment standards. The national standard *Information security technology — Baseline for classified protection of cybersecurity* (GB/T 22239-2019) [17] has played a significant role in the process of carrying out information security classified protection. In order to improve the applicability, timeliness and manipulability of classified protection, the domain-oriented classified protection standards has been formulated according to the revised ideas and methods of GB/T 22239-2019 in five new network technologies: mobile interconnection, cloud computing [18], big data [19], internet of things [20] and industrial control system. With the advent of classified protection 2.0 era [21], the *Classified Protection of Information System Security* (CPISS) has been officially renamed to CPC [22].

A. COMPARISON AND EVALUATION

B. GRADING STANDARD OF CLASSIFIED PROTECTION

The grading classification of assessment objects is determined by many factors such as the importance of information system in national security, economic construction, society, as well as the degree of damage to national security, social order, public interest, and the legitimate rights of citizens, legal persons, and other organizations. Table 1 shows the relation between grading elements and security level.

C. APPLICATION LAYER CONTROL POINTS COMPARISON IN CPC 2.0 AND 1.0

The CPC 2.0 standard was re-established and developed on the basis of CPC 1.0. As shown in Table 2, the application security, data security and backup recovery of the CPC 1.0 are merged into application and data security at CPC 2.0; the integrity and confidentiality of communication are included in the network and communication security layer. In addition, residual information protection and personal information protection are added on the basis of CPC 1.0.

IV. BLOCKCHAIN ARCHITECTURE

At present, there are many blockchain systems, each of which has its own advantages and specialized research directions. However, Bitcoin [1], Ethereum [23] and Hyperledger [24] are the most commonly used and most systematic systems in the market today. Their codes are completely open source and have a huge influence on the construction of other systems. Therefore, the research on the assessment standard of classified protection based on the above three blockchain

TABLE 2. Comparison of application layer control points in classified protection 1.0 and 2.0 at level 3.

Version	Category	Control Points
Classified Protection 1.0	Application Security	Identity Authentication, Access Control, Security Audit, Communication Integrity, Communication Confidentiality, Software Fault Tolerance, Resource Control
	Data Security and Backup Recovery	Data Integrity, Data Confidentiality, Backup and Recovery
Classified Protection 2.0	Application and Data Security	Identity Authentication, Access Control, Security Audit, Software Fault Tolerance, Resource Control, Data Integrity, Data Confidentiality, Data Backup and Recovery, Residual Information Protection, Personal Information Protection

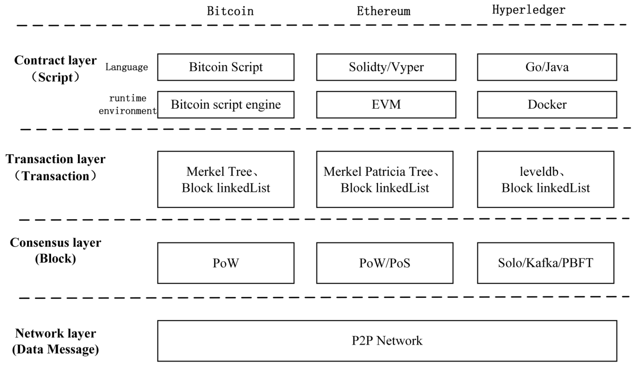


FIGURE 1. Blockchain framework.

systems will be more beneficial to relevant researchers. Their respective advantages are listed as follows:

1) **Bitcoin**: Bitcoin is the earliest decentralized blockchain system, in which nodes obtain the accounting right through the consensus mechanism of proof-of-work (PoW). Bitcoin can only handle simple scripts without Turing Complete smart contract's executive capabilities.
2) **Ethereum**: Ethereum is a programmable blockchain that allows users to create complicated operations, and have Turing Complete smart contract functions, which brings blockchain into the era of smart contracts [25].
3) **Hyperledger Fabric**: Hyperledger Fabric is a pluggable, extensible, modular blockchain platform that is highly centralized and supports general programming languages to write smart contracts rather than a domain-specific language (DSL).

The different characteristics of the above-mentioned blockchain increase the difficulty of blockchain assessment, but all kinds of blockchain can be divided into Contract layer, Transaction layer, Consensus layer and Network layer shown in Figure 1. To find specific evaluation requirements and implementation methods for blockchain, this paper separately evaluate the core parts of the blockchain that mainly include P2P network (Network layer), consensus mechanism (Consensus layer),distributed ledger (Transaction layer), and smart contract (Contract layer) in later sections.

V. DISTRIBUTED P2P NETWORK ASSESSMENT

A distributed peer-to-peer (P2P) network is a computer network that only contains nodes with equivalent control and operational capabilities. The underlying topology of the blockchain information system is a distributed P2P network, in which each node carries out data communication to support the upper functions. The five-layer model of the TCP/IP network can be divided into physical layer, data link layer, network layer, transport layer, and application layer. The P2P network of the blockchain model [26] is a logical overlay network based on the TCP/IP protocol at the application layer. The characteristics of P2P network mainly include decentralization, scalability and load balancing [27], which provide a strong guarantee for the efficient and stable operation of the blockchain system.

The Bitcoin system maintains a list of peer nodes that can be connected at startup [28]. When a new node accesses an existing network, it first obtains a list of peer nodes IP through ''seeds''. Then nodes usually use TCP to establish connections with each other through port. When a connection is established, the communication process of authentication ''handshake'' is used to determine the P2P protocol version, software version, node IP, block height, and so on. Finally, the new node exchanges the list of connected IP addresses with the connected nodes in order to be discovered by more nodes.

TABLE 3 introduces the evaluation scheme and results of distributed P2P networks of the blockchain. The first column of table lists the evaluation requirements in five categories: identification, software fault tolerance, resource control, data integrity, and security audit; the second column describes the evaluation items for each categories; in the last four columns, the evaluation result is summarized according to the following subsections. The evaluation items include:

1) **Node access control**: It should support access to blockchain nodes by authenticating users and nodes.
2) **Self-protection and adaptation**: It should adapt to network jitter.
3) **Concurrent connection restriction**: It should limit the maximum number of concurrent connections for a single node.
4) **Connection timeout limit**: The session is automatically terminated when one party has not responded for a long time.

TABLE 3. Distributed peer-to-peer network assessment.

Categories	Items	Implementation	Expected Effectiveness	Description of actual evaluation results	Y/N
Identification	Node access control	Check if the connection to the blockchain requires authentication.	When nodes are connected, the system authenticates them to restrict node access.	The identity is not authenticated when the node is connected.	N
Software fault tolerance	Self-protection and self-adaptation	Inspect information transmission when the network is unstable.	Network jitter does not have much impact on transmission. Blockchain runs stably.	Bitcoin system runs stably when network jitter occurs.	Y
Resource control	Concurrent connection restriction	View the maximum number of connections on nodes	Limit maximum concurrent connections to prevent system resource exhaustion	Node connections do not exceed 117 input connections and 8 output connections.	Y
	Connection timeout limit	View related network configurations	Automatically end long-term unanswered sessions to prevent system resource usage.	If there is no communication for more than 30 minutes, a heartbeat message is sent. End the session if there is no communication for 90 minutes.	Y
Data integrity	Anti-tampering of unicast	Check whether data transmission is encrypted and tamper-proof	Data is not tampered with in the process of point-to-point communication.	The integrity of data in unicast communication cannot be guaranteed.	N
	Multicast communication tamper-proof	Check whether the system can provide communication multicast, broadcast function and tamper-proof data in the process of communication	Data is not tampered with during broadcast communication	The Bitcoin system does not guarantee the integrity of data in the broadcast communication process	N
	Forwarding communication tamper-proof	Data Tampering Prevention in Forwarding Communication	Data is not tampered with when forwarded by a node.	The integrity of data in the process of forwarding communication cannot be guaranteed	N
security audit	Network status get update	Check whether the log records node status information.	Ability to provide trusted node data for stable operation of the system	There is a status update record for a single node. However, update records are not exchanged in the whole network, the whole network status cannot be obtained.	N
	Network node dynamic monitoring	Statistics on the number of online nodes	Ability to recognize nodes dynamically increasing and decreasing	The Bitcoin system does not have the real-time statistical ability of the number of nodes in the whole network	Y

5) **Anti-tampering of unicast**: It should provide peer-to-peer tamper-proof communication.
6) **Multicast communication tamper-proof**: It should provide tamper-proof broadcasting function.
7) **Forwarding communication tamper-proof**: It should provide forwarding function and prevent information from being tampered with during transmission.
8) **Network status acquisition and updating**: It should record the network nodes operation status and update relevant information.
9) **Dynamic monitoring of network nodes**: It can supervise nodes dynamically joining and exiting.

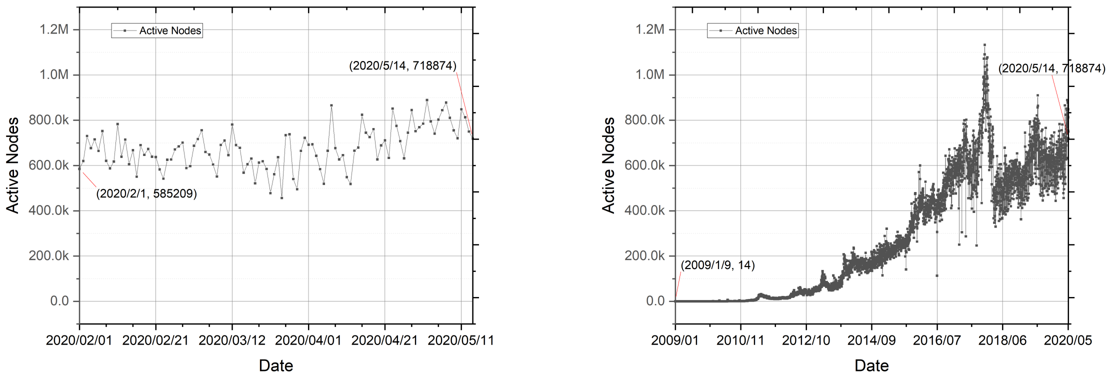
It is worth noting that the nodes which have established the connection will periodically send information to maintain the connection. If a node has no communication for 90 minutes, the session ends. Bitcoin node connection does not exceed 117 input connections, initiate 8 output connections to other nodes, and the excess number of IP addresses will be ignored.

Bitcoin adopts a P2P network where each node has 8 adjacent edges. As shown in Figure 2(a), we measured the variation of bitcoin network size in recent three months. The results shows that the current scale of the network could reach 600,000 nodes, in which 7-10 forwarding is needed to realize the whole network broadcast of transactions. As can be seen from Figure 2(b), the network scale has been increasing since 2009, which makes the requirements on P2P network strict gradually.

We collect and analyze the network stability in terms of network scale, node geographical distribution, node interrupt availability, relevant transmission information, transmission time and other data, and summarize the actual use of blockchain P2P network for the assessment work. Table 3 summarizes the implementation methods and expected results for each item, as well as the assessment results of the Bitcoin. It can be seen that, except for the passing of items **2), 3), 4)** and **9)**, the other five items did not meet the CPC-2.0-L3 requirements of classified protection.

VI. CONSENSUS MECHANISM ASSESSMENT

The consensus mechanism [29], [30] is a way for the member nodes of blockchain system to agree on the operation of blockchain (e.g., building blocks, transaction verification). Since the blockchain is a decentralized, distributed system, there is no centralized accounting node to ensure



(a) (b)

FIGURE 2. The scale change of Bitcoin P2P network.

TABLE 4. Consensus mechanism assessment.

Categories	Items	Implementation	Expected Effectiveness	Description of actual evaluation results	Y/N
Resource control	Consensus Resource Control	Check the use of resources in the computer.	Consensus mechanisms should minimize the consumption of computer resources.	PoW consumes a lot of computing resources, but the system resources are controllable.	Y
Backup and Recovery	Real-time backup	Check whether the node has synchronized the new consensus block.	All network nodes have the same data replica.	Real-time backup of transaction data generated in Bitcoin system by nodes.	Y
	system hot redundancy	View system availability after node paralysis.	Business continuity not interrupted.	Nodes are redundant to each other, and single or few node failures do not affect the stability and availability of the system.	Y
Consensus effect	Consensus fault tolerance	Set exception nodes and view consensus.	There is a consensus threshold, so that the node exceeding the threshold reaches the consensus, which means that the consensus of the whole network is completed.	The system can accommodate 5% node consensus errors. More than 95% of the nodes are successful.	Y
	Consensus effectiveness	Initiate an illegal transaction to see if the consensus failed	Illegal transaction consensus failed. By verifying the correctness and logic of the transaction, the cost of malicious fraudulent transactions is expensive and avoids malicious consensus	Illegal transactions cannot be passed by consensus.	Y
	Consensus Consistency	Initiate a legal transaction and see if the consensus result is consistent	Loyal participant consensus results are consistent	After agreeing on the legal transaction of Bitcoin system, it is written into the blockchain.	Y

that the records of all transactions are consistent on each node, so the role of consensus mechanism is to implement the data consistency and operational synchronization between nodes of blockchain, which is one of the key technologies of blockchain system.

The existing mainstream consensus technologies [31] mainly include proof of workload (PoW) [32], [33], Byzantine Fault Tolerance Consensus (PBFT) [34], [35], proof of equity (PoS) [36], proof of authorized rights (DPoS) [37] and so on. The Bitcoin system uses the PoW protocol, which is suitable for large networks and is the most mature consensus protocol by far. In contrast, PBFT is more suitable for small, fully connected networks. Blockchain can select the appropriate consensus algorithm according to requirements and the actual situation (e.g., the number of nodes, fault tolerance, performance efficiency and other indicators). This section will evaluate the PoW protocol of the Bitcoin system.

The assessment of consensus mechanism is based on its resource consumption and the effect achieved by the consensus. Table 4 lists the categories of consensus mechanism to be evaluated with their corresponding evaluation items, and summarizes the evaluation result according to the following subsections. The evaluation categories mainly include three aspects: consensus resource control, backup and recovery, and consensus effect, and the evaluation items are as follows:

1) **Consensus resource control**: The computer resources (e.g., CPU, network, and storage) that are consumed by consensus can be controlled.

2) **Real-time backup**: It should use the P2P network to back up generated transaction data to local and remote nodes in real time.
3) **System hot redundancy**: When the blockchain node is abnormal, other nodes will automatically clear it and complete normal data processing.
4) **Consensus fault tolerance**: Even if there are some abnormal nodes, the consensus is still unaffected.
5) **Consensus effectiveness**: The submitted transaction should be verified for correctness and logic.
6) **Consensus consistency**: Normal nodes are consistent with the results of same request.

The consensus process of Bitcoin is shown in Figure 3, the goal of which is that all nodes jointly build new blocks containing recent transactions. The consensus can be divided into several stages: transaction collection, candidate block creation, workload certification (mining [38]), broadcasting block, block loading to chains and transaction recovery, which are implemented by common nodes (transaction nodes) and miner nodes(abbreviated as miners). The following evaluation content is evaluated based on this consensus process.

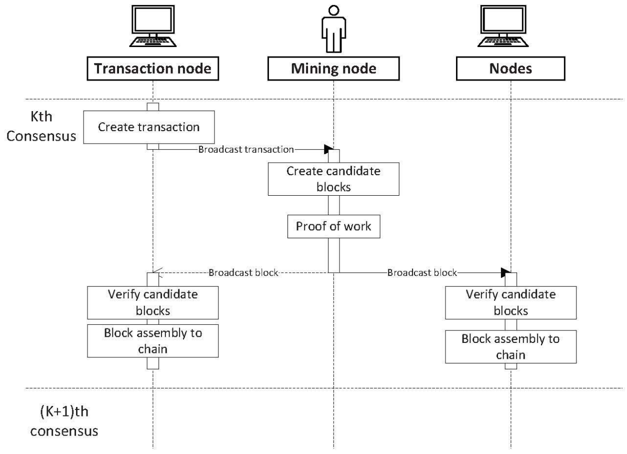


FIGURE 3. Consensus timing diagram.

A. CONSENSUS RESOURCE CONTROL

In the blockchain consensus mechanism, the miner continually modifies value of the random number N_n in the $BlockHeader_n$ and calculates hash value $SHA256^2$ of the blockhead until the blockhead hash is less than the difficulty value D_n. The above relationship can be expressed by the following formula: $SHA256^2(BlockHeader_n) < D_n$. The miners consume a lot of computing resources in a short period of time to obtain random numbers that meet the requirements, and then compete for accounting rights. If the mining is successful, N_n will serve as proof of the miner's workload. The proof is difficult to generate (the average mining calculation complexity under the birthday attack is $O(\sqrt{\frac{2^{256}}{D}})$), but any node can easily verify whether the miner is a winner by the above formula. After the system has been in operation for more than ten years, the difficulty of mining has become greater and greater, resulting in a large amount of resource consumption (electricity). This means that the system operating cost increases and the consensus period extends, which seriously affects the stability of system. Therefore, the average computing power of entire network and the distribution time of block generation should be used as the evaluation indicators of resource control **(item 1)**. The following uses Bitcoin as an example for evaluation and analysis.

1) AVERAGE COMPUTING POWER OF THE WHOLE NETWORK

Computing power is a measure of the total power that generates new blocks under a certain network consumption. The entire network computing power, that is, the integration of computing power used by all mining machines participating in the network, the entire network computing power of Bitcoin is the sum of computing power of all participating Bitcoin mining machines. As shown in Figure 4, we collected the average computing power of entire network from 2009 to present (May 2020) and draw a distribution trend graph. It can be seen that with the increase in number of Bitcoin online active addresses and the rapid development of computing power, the entire computing power of Bitcoin network has also been greatly improved.

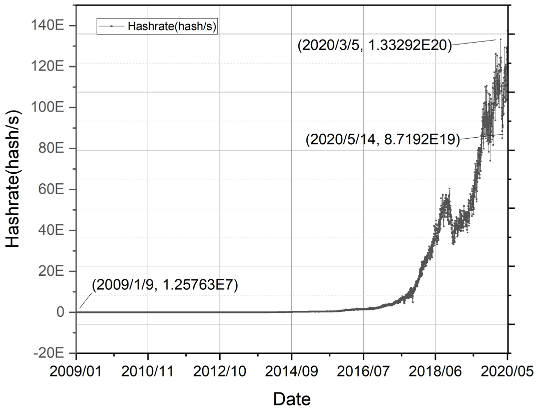


FIGURE 4. Bitcoin Hashrate historical chart.

2) TIME DISTRIBUTION OF BLOCK GENERATIONS

Consider a node in blockchain with address A and balance $bal(A)$ [39]. During the mining process, the node continuously modifies the value of random number (usually gradually adding 1), so that the calculated result is less than the target threshold to build an effective block. The target value when building a new block is denoted as θ, and the mining difficulty is D, thus all valid blocks in the blockchain need to meet a condition $U \leq \theta \leq 1$. In the formula, $U \in [0, 1]$ is a uniformly distributed random variable generated after hashing blockHeader data and normalizing the obtained value. Due to the characteristics of hash functions, many consensus technologies are special cases of this formula, for example:

- In the case of PoW, $\theta = 1/D$;
- In the case of PoS, $\theta = bal(A)/D$.

To generate a block, the user needs to find the data that makes U satisfy $U \leq \theta \leq 1$, that is, constantly changing the random number, and calculate the U by hashing blockHeader which contains it, so that U satisfies $U \leq \theta \leq 1$. Let N be the number of data combinations that the user needs to calculate before finding a valid block. Since the workload proves that PoW interval is very large, the user can only iterate r combinations per second, where r is determined by the user's mining equipment. In the case of PoS, the search space is small, so we can assume $r = 1$. The time T required by the user to find a valid block is related to N: $T = N/r$. Considering the cumulative probability distribution:

$$\begin{aligned} Pr\{T \leq t\} &= Pr\{N \leq rt\} = 1 - Pr\{N \geq re\} \\ &= 1 - (1-\theta)^{rt} = 1 - exp(log(1-\theta)^{rt}) \end{aligned}$$

When $\theta \ll 1$, $log(1-\theta) \approx -\theta$,

$$P\{T \leq t\} \approx 1 - exp(-\theta rt)$$

Therefore, the time T required is exponentially distributed at a rate θr. In the case of PoW, this rate is equal to r/D. In the case of PoS, $r = 1$, so it is equal to $bal(A)/D$. The probability of generating a valid block is equal to the ratio of user's balance of funds to the total amount of currency in circulation, and the block generation time of the entire network is distributed exponentially with rate $\sum_a bal(a)/D$. As shown in Figure 5, we collected the difficulty values of bitcoin blocks in recent years and plotted the difficulty change curve. It can be seen that it is a more obvious exponential distribution curve with a fitting equation of $y = -1.44623E9 \times (1 - e^{-0.00228x})$. ($E$ is the simplification of scientific notation means, $E9 = 10^9$.)

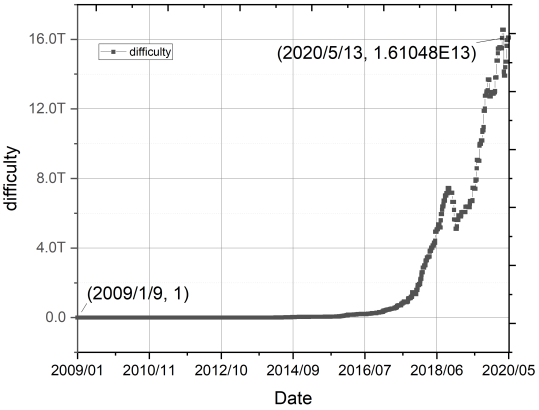


FIGURE 5. Consensus difficulty change trend diagram Bitcoin.

The attack against PoW is to make adversary [40] become the winner of mining with a big advantage, thereby using the billing right to change or falsify transactions. In order to achieve successful mining, the main attacks taken by current adversaries include: 1) Attacks against consensus include the 51% attack [41], brute force attack [42], private mining [43] and so on. Take 51% attack as an example, it does not mean that you have more than 51% of the total network's computing power to successfully attack, but when power exceeds the threshold of 51%, the opponent will calculate a correct hash faster than other miners in the whole network, and the attack success rate will be greatly increased. 2)The block broadcasting process can be affected by factors such as eclipse attacks [44] and sybil attacks [45]. Among them, the eclipse attack is the way in which adversaries influence the consensus by blocking communication of the normal nodes; in the sybil attack, the adversaries will pretend to be a blockchain node of different roles to monitor and interfere with the normal network.

The assessment of resource control (**item 1**) should consider the impact of above attacks on system and ensure system security by improving the difficulty of resource control. As far as the Bitcoin is concerned, as system nodes continue to join, the total network power of whole network has increased dramatically, and the system network structure has become more and more huge. So that the possibility adversaries occupy most of computing power is extremely small, and it is very difficult to control the Bitcoin network. Therefore, Bitcoin system resources can be controlled. However, for small blockchains, due to the low computing power of the entire network, the adversary can successfully attack system through resource control.

B. REAL-TIME BACKUP

The collection phase of transactions is as follows: 1) After the new transaction is generated, it will be broadcast to whole network by this node through the blockchain network in real time; 2) The miner nodes collect the transaction and verify its normativeness (e.g., whether the previous transaction belongs to unspent transactions [46]); 3)If correctness and logic of the transaction meet requirements, the miner will deposit it into ''unspent transaction pool'' of the memory. Therefore, after a transaction is formed, the created node will broadcast it to the whole network in real time through the distributed peer-to-peer network. The miner node will collect and verify its standardization and put it into the ''unconfirmed transaction pool'' to realize the data backup of local and remote nodes.

The specific process of block assembly to the chain work is: 1) verify the correctness of mining; 2) discard the block if verification fails, otherwise it is appended to the existing blockchain. The node looks for the parent block of a new one and links to the parent block to complete the assembly of block. Each node continuously writes consensus blocks into its own ledger, so as to achieve the effect of real-time nodes backup with the same data copy in whole network.

In summary, blockchain has achieved the effect of data backup of the whole network during the process of transaction, block generation and consensus, so that the evaluation **item 2** is guaranteed.

C. SYSTEM HOT REDUNDANCY AND CONSENSUS FAULT TOLERANCE

Blockchain system nodes are decentralized and contain a few malicious nodes, makes it obviously difficult to achieve 100% consensus. Therefore, the system evaluation should fully adopt the idea of small probability events in statistics: as long as the consensus degree exceeds 95%, it represents a complete consensus. Since the current Bitcoin can confirm a single transaction with 99.9999% probability in two hours, it can be considered that consensus fault tolerance **(item 4)** reaches the requirement. According to the above criteria, the nodes of blockchain are mutually redundant, and the failure of a few nodes does not affect the stability and availability of system, so system hot redundancy(**item 3**) of Bitcoin meets the requirement.

D. CONSENSUS EFFECTIVENESS

In the transaction collection stage, the miner node checks transaction data content through standardized verification, such as correctness of signature, existence of currency, and whether the currency is re-used, so as to ensure the validity of consensus transaction (**item 5**). However, the above verification process does not fully guarantee the absolute validity of transactions, for example, the malleable attack on exchange in the ''Mentou Gou (Mt. Gox) Incident'' [47], so the evaluation work should be carried out based on the latest CVE vulnerability.

The candidate block creation phase is completed by the miners, as follows: 1) Generate new candidate blocks and Coinbase transactions (including the new currency of mining rewards); 2) Extract transactions according to priority from ''unconfirmed transaction pool'' and write to the aforementioned block; 3) Calculate the block header information and fill it into the newly created candidate block. Before the first step, miners can calculate the rewards available for this mining. The rewards consist of current block reward and total transaction fees to be packaged into the block. Therefore, verifying the authenticity and validity of the rewards in Coinbase transaction can ensure the correctness of the miner's work (**item 5**).

The PoW consensus algorithm dynamically adjusts the difficulty value according to the hash rate of whole network. The current adjustment period is 2 weeks, and the adjustment value will be written to the blockheader and participate in the next stage of proof-of-work calculation, thereby establishing the continuation of difficulty value affect to ensure that the order of consensus data blocks remains unchanged.

When the height of main chain exceeds other branches by more than six blocks (a single transaction can be confirmed with a probability of 99.9% within 1 hour [48]), the branch block transaction will be further resolved, and unprocessed transactions will be re-released enter the ''Unconfirmed Transaction Pool''. The branch transaction recovery process can avoid transaction loss and ensure the validity of consensus to a certain extent.

To sum up,the consensus mechanism has adopted a certain mechanism at different stages to verify the correctness and logic of transaction data, ensuring the validity of Consensus consistency (**item 5**).

E. CONSENSUS CONSISTENCY

It can be obtained by PoW transaction collection, candidate block creation, proof of work (mining), broadcast block, block assembly to chain and transaction recovery that the security of blockchain is mainly affected by the mining nodes influences. The results of existing mining power analysis of the system security show that when the mining power of mining nodes strictly following the consensus rules exceeds (weak) majority, it can ensure that all nodes in system get same consensus, and the consensus results are consistent (**item 5**).

F. RESULT OF CONSENSUS MECHANISM

As shown in Table 5, document [49] shows the influence of different blockchain parameter selection (block interval, block size) on the blockchain network transmission. Through the above evaluation, Table 4 summarizes the achievement of PoW consensus blockchain system in each evaluation item. From the perspective of ''backup and recovery'' and ''consensus effects'', PoW consensus blockchain system can meet the requirements of evaluation (**items 1,2,3,4,5,6**).

TABLE 5. Impact of parameter selection on network transmission in different blockchains [49].

	Bitcoin	Litecoin	Dogecoin	Ethereum
Block interval	10 min	2.5 min	1 min	10-20 sec
Public nodes	6000	800	600	4000
Mining pools	16	12	12	13
Stale block rate	0.41%	0.273%	0.619%	6.8%
Block size	534.8 KB	6.11 KB	8 KB	1.5 KB

VII. DISTRIBUTED LEDGERS ASSESSMENT

The distributed ledger [50] is a decentralized data storage structure that synchronizes, serializes, tampers between members, and can provide writing and query services for various types of data generated during operation of the blockchain system. For digital currency transactions, distributed ledgers in blockchain system are designed to store transaction information in the latest time period (about 10 minutes), and to maintain the integrity and non-repudiation of transaction information through cryptographic Hash function.

The distributed ledger assessment is evaluated on the structure of storage, security mechanisms and functions of the information stored in blockchain. In Table 6, we divide the

TABLE 6. Distributed ledger assessment.

Categories	Items	Implementation	Expected Effectiveness	Description of actual evaluation results	Y/N
Software fault tolerance	Standardization of ledger	Check whether the data format in the ledger has a uniform standard	Data such as transactions and blocks are stored in data format	Blockchain system transactions, blocks, etc., have unified organizational standards.	Y
Access control	Ledger access control	Check whether there is an access policy supervision node and access control policy	Protect the data resources on the ledger against illegal access	Bitcoin as a public blockchain, there is no complete access control strategy	N
Data integrity	Storage integrity	Check if there is a hash mechanism in the data storage to ensure the integrity of the storage	Stored data is hashed and integrity is guaranteed	Bitcoin hashes transactions in the form of Merkel trees and stores them in blocks	Y
Data confidentiality	Storage confidentiality	Check if the storage of confidential data is encrypted	Data is not stored in plaintext format	Bitcoin data storage is stored in plaintext in hexadecimal form, which is convenient for query and verification	N
Ledger function	Data non-repudiation	Check if the transaction data in the ledger is signed	The transaction is signed by each participant, so that the transaction can be traceable to achieve the role of non-repudiation.	Bitcoin achieves data non-repudiation by signing transaction data	Y
	Ledger data synchronization	Check if there is a full node, store all data in the ledger	All the data in the ledger is synchronized in the full node. A complete copy of the blockchain data can be obtained from full nodes	There are full nodes in the Bitcoin system that synchronize all the data of the ledger.	Y
	Ledger data idempotence	Check if the results of retrieving the same data are consistent	Ensure data consistency by querying the same records with the same results	The data of Bitcoin deposited in the ledger has passed the consensus, and ledger data has idempotency.	Y

assessment items into five basic aspects: software fault tolerance, access control, data integrity, data confidentiality, as well as ledger functions with their evaluation items. Meanwhile, three unique functional points of non-repudiation, synchronization, and idempotency are listed as the ledger functions. Accordingly, the evaluation items include:

1) **Standardization of ledger**: There are strict data format specifications for transactions, blocks, contracts and other data deposited in ledgers.
2) **Ledger access control**: There is at least one node performing the supervision function for configuring and delivering the access control policy.
3) **Storage integrity**: The ledger should detect the destruction and loss of data blocks that are accidentally or intentionally deleted, modified, forged, out of order, replayed, inserted, etc., during the storage process.
4) **Storage confidentiality**: The ledger should guarantee the confidentiality of data on the chain.
5) **Data non-repudiation**: The ledger should guarantee that transaction data is non-repudiation and traceable.
6) **Ledger data synchronization**: The ledger should store and synchronize complete records.
7) **Ledger data idempotence**: Distributed ledger retrieval is idempotent, which means that multiple queries for a certain ledger resource should have the same result.

Later, this chapter will evaluate these evaluation items of distributed ledger based on the specific characteristics of blockchain.

A. STANDARDIZATION OF LEDGER

The blockchain has a strict structural definition. Each block [51] is composed of a block header and a block body in which the data length of each item has a specific data format specification as shown in TABLE 7. Block header contains block version V, difficulty D, pre-block hash $PreH$, merkle tree root M, nonce N, timestamp T, etc., so it can be represented by the following formula:

$$BlockHeader_n := V_n \mid D_n \mid M_n \mid T_n \mid PreH_n \mid N_n \quad (1)$$

TABLE 7. Information and length limit of Blockchain Header.

Items	Use	Size (byte)
Version	Block version number	4
Difficulty Target	To indicate the difficulty of mining	4
Pre-block hash	Based on the 256-bit Hash value of all transactions in the block	32
Merkletree Root	The value of the transaction content 256-bit hash	32
Nonce	To adjust the current block head hash value	4
Timestamp	A UNIX timestamp	4

The block body stores the number and the list of transactions in the block. Figure 6 shows the transaction structure of the blockchain system, and most information in the structure

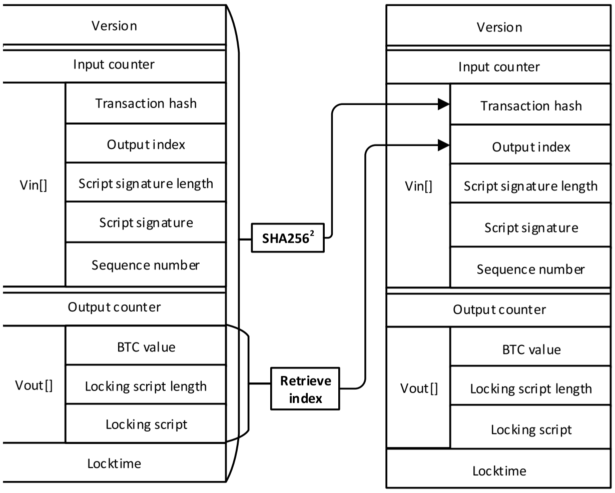


FIGURE 6. **Structure of Blockchain transaction.**

is limited by standard length. A transaction consists of a transaction's version as well as a number of input segments (Vin) and output segments (Vout). Each input segment is connected to a specific "unspent" transaction output through a hash function (*SHA*256) and a signature script, which is also called UTXO (Unspent Transaction Output).

According to the above analysis, there are strict data item requirements and data item length provisions in the block chain transactions, blocks and other structures, which can ensure the standardization and global consistency of the ledger format. So the evaluation of Standardization of ledger **(item 1)** meets the standard.

B. LEDGER ACCESS CONTROL

The openness of the Bitcoin platform enables all users to access the ledger data, and there are no nodes with supervisory functions, so the Ledger access control **(item 2)** fails to meet the standard.

C. STORAGE INTEGRITY

The blockchain has introduced a complete cryptographic data authentication and a strict, standardized data structure to ensure the non-tampering of transactions and block data, which are listed as follows:

- **Use of cryptographic hash function**: The blockchain uses the hash algorithm to reverse solve difficulties, input avalanche effects, anti-collision and other characteristics to ensure that the block data is permanently stored and cannot be tampered with.
- **Chained hash structure**: The block headers are connected by a cryptographic hash function (nested SHA256) to ensure that the data between blocks cannot be modified, inserted, or deleted on the time axis [52].
- **Tree-like hash structure**: Merkel tree structure [53], [54] is used to encapsulate a large number of transactions, and the Merkel tree root [55] is placed in the block header to ensure that the transaction content and order in this block are not allowed to be changed.

In summary, a large number of cryptographic mechanisms and data structures are used to store and protect data in the blockchain, which can ensure the integrity of the data block storage process, and the evaluation of Storage integrity **(item 3)** meets the standards.

D. STORAGE CONFIDENTIALITY

The blockchain ledger stores data in hexadecimal coding (unencrypted) mode to facilitate users query verification and traceability. Limited by the immaturity of current public key encryption technology in key negotiation, construction, distribution, update, revocation, and other technologies under large-scale dynamic groups, so it fails to meet the requirements of storage confidentiality (**item 4**).

E. DATA NON-REPUDIATION

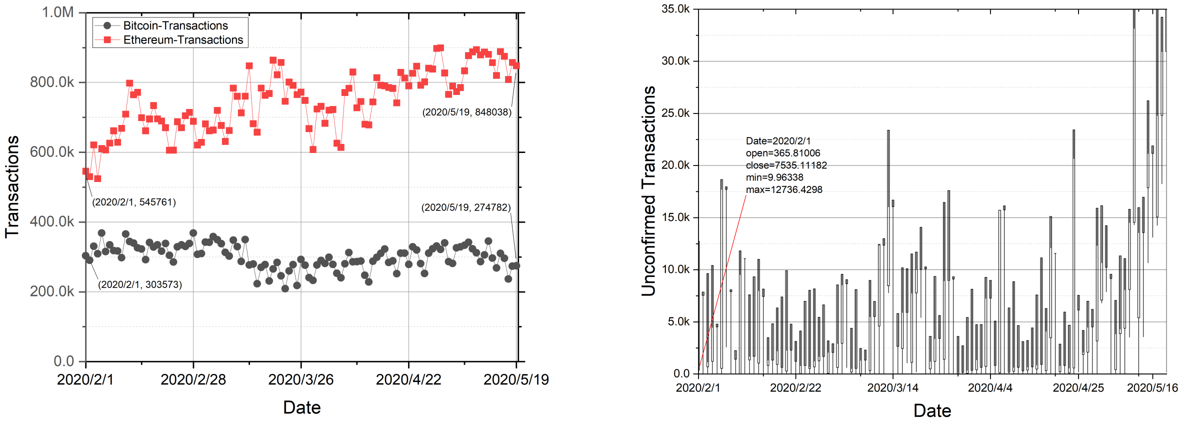
In the Bitcoin transaction structure shown in Figure 6, the "transaction output index" field included in Vin refers to the sequence number (i.e., index number) of the output segment Vout used in the previous transaction. "Script signature [56]" is the variable-length data of the unlock script, and only when the unlock script is correct can the output be consumed. The "lock script" defines the conditions required to pay for the output (such as the public key information to verify the identity of currency owner). In the transaction information, in order to verify the ownership of currency, the "lock script" of previous transaction and the "script signature" of current transaction can store "public key" and "signature" information of the currency owner, respectively, and the validity of latter signature can be verified by the unlock script. Through this process, the transaction meets evaluation data non-repudiation **(item 5)**.

F. LEDGER DATA SYNCHRONIZATION

In terms of distributed ledger management, the blockchain system relies on "full nodes" to store all the data of ledger. The newly added nodes can obtain complete backup of the blockchain data by cloning the full nodes, thus ensuring the data synchronization of the blockchain ledgers (**item 6**). In addition, the blockchain system can detect and confirm the data errors found during the synchronization process, and mark them as confirmed transactions or unconfirmed transactions. Figure 7(a) shows the changes in number of confirmed transactions of Bitcoin and Ethereum in the past three months. Figure 7(b) shows the growth of Bitcoin's unconfirmed transactions in the past three months. It can be seen that there are a large number of unconfirmed transactions (about 20%), which indicates that the blockchain can detect and distinguish malicious or invalid transactions well.

G. LEDGER DATA IDEMPOTENCE

For the query request of the ledger data, the integrity of ledger data can be verified by the cryptographic hash function.



(a) Diagram of confirmed transactions for Bitcoin and Ethereum

(b) Growth chart of unconfirmed transactions for Bitcoin

FIGURE 7. **Comparison between confirmed and unconfirmed transactions in the blockchain systems.**

The conflict avoidance feature of hash function ensures the consistency of query result in all nodes, and the retrieval idempotency **(item 7)** is realized.

H. RESULT OF DISTRIBUTED LEDGERS ASSESSMENT

In summary, the final results of the evaluation on the distributed ledger are shown in Table 6. Ledger access control **(item 2)** and storage confidentiality **(item 4)** failed to meet the CPC-2.0-L3 requirements, but all other evaluation items met the requirements.

VIII. CONTRACT LAYER ASSESSMENT

Smart contract is programs or scripts that run on the blockchain. Blockchain, as a carrier of data, stores the key information of events, and smart contract is the rules for operating these data in blockchain. For example, bitcoin transactions use bitcoin scripts and signature technology to limit the owners of unspent transactions; blockchain platforms (e.g., Ethereum), replace bitcoin scripts with computer programs, allowing users to make more flexible rules.

The smart contract is claimed to run on blockchain because it is not only run by one computer, but also executed and verified by other computing nodes participating in the verification. The smart contract operation process is as follows: 1) The executor initiates an operation request, runs locally and checks the feasibility; 2) The executor broadcasts operation status to the blockchain network, and the mining node executes the smart contract, passes the verification and packages it into the block. 3) The block is broadcast to all nodes, and the nodes participating in the verification complete verification by executing this contract contained in the block.

Table 8 lists the evaluation standards for smart contract layer in blockchain, and analyzes it one by one in five categories: identity authentication, security audit, malicious code prevention, data integrity, and data confidentiality according to the following subsections. The evaluation items include:

1) **Performing entity authentication**: Control the execution of blockchain smart contracts through user and node identity authentication.
2) **Behavioral event audit**: By participating in the verification of smart contract execution by mining nodes, auditing behavior events in smart contracts.
3) **Audit records**: Record the date, executor, input and output information in the smart contract.
4) **Protection from malicious code**:Through certain means, the local and blockchain programs are protected from smart contract attacks written by malicious users.
5) **Transmission integrity**: Ensure the integrity of data in transmission.
6) **Transmission confidentiality**: Ensure the confidentiality of data during transmission.

A. PERFORMING ENTITY AUTHENTICATION

Identity verification is the most basic function of smart contract. In order to achieve identity verification, Bitcoin scripts are divided into locking scripts and unlocking scripts. Through cryptographic digital signature technology, users who unlock the ''locking script'' are users who can use the transaction in accordance with regulations. The most commonly used script is shown as Figure 8:

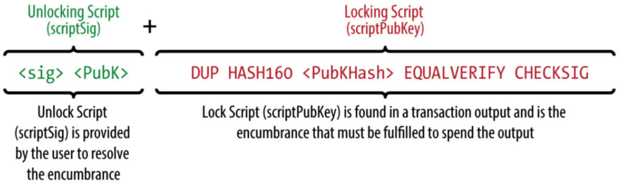

Unlocking Script
(scriptSig)
+
Locking Script
(scriptPubKey)
<sig> <PubK>
DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
Unlock Script
(scriptSig) is provided
by the user to resolve
the encumbrance
Lock Script (scriptPubKey) is found in a transaction output and is the
encumbrance that must be fulfilled to spend the output

FIGURE 8. **Common scripting mechanism.**

In Figure 8, the unlocking script takes signature and public key as input, and the correctness of signature is verified by the operation code set in lock script and stored public key hash,

TABLE 8. Blockchain contract computing layer evaluation.

Categories	Items	Implementation	Expected Effectiveness	Description of actual evaluation results	Y/N
Identification	Performing entity authentication	Check if the contract can be viewed or qualify executor's identity	The identification and authentication should be carried out for the logged-in user. The identification is required to be unique and complicated.	When publishing a transaction, the blockchain verifies the executor's identity, thus constraining the execution of contract.	Y
Security audit	Behavioral event audit	Check if to verify the execution of smart contract	The security audit function should be enabled to cover every user over significant user actions and security events.	All nodes involved in mining can verify the correctness of smart contract execution.	Y
	Audit records	Check if audit information is recorded	The audit record should include the date and time of event, the executor, the type of event, the state if the event was successful, etc. Audit records should be protected and backed up regularly to avoid unexpected deletions, modifications or overwrites.	The transactions in the block record the execution time, the executors, the input and output of the smart contract.	N
Malicious code protection	Protection from malicious code	Check if there is a mechanism to protect against malicious code	It is necessary to adopt the technical measures to avoid the attack of malicious code or the trusted verification mechanism with active immunity to identify the intrusion and virus behavior in time and block it effectively.	Local computers and blockchain systems do not be affected by restricted addressing methods, limited instruction sets, operating platforms such as Docker, or other mechanisms.	Y
Data integrity	Transmission integrity	Check if data integrity is guaranteed by CRC or cryptography	Verification technology or cryptography should be adopted to ensure the integrity of important data during transmission.	There are status updating records for individual nodes.	Y
Data confidentiality	Transmission confidentiality	Check if data confidentiality is guaranteed by cryptography.	Cryptography should be adopted to ensure the confidentiality of important data during transmission.	The blockchain system does not have the real-time statistical ability on the number of nodes in the whole network.	N

thereby identifying the user's identity, and the **item 1** meets the standard.

B. SECURITY AUDIT

Audit [57] refers to faithfully recording all acts of system in accordance with certain norms, so as to facilitate the administrator to monitor the system security in real time, detect abnormal violations in time and obtain evidence [58]. By analyzing the open source code of Bitcoin system, Table 9 lists the output errors and interface functions related to errors of six function modules of Bitcoin system, such as initialization, transaction, block, consensus, network and remote procedure call. It can be seen that the record of audit information in Bitcoin is more detailed. Each execution of smart contract will be verified by other nodes, and the behavior or events in the contract will be reviewed, so behavior event audit **(items 2)** meets the standards.

Figure 9 shows the Bitcoin log generation process. The specific process is as follows: 1) Add a timestamp of the specified format to the generated log information; 2) Check whether the parameter requires additional IP address in the output information; 3) Output the processed log to the specified location (debug.log or console). The maximum value of the log file (debug.log) is set by the system. Since the log that exceeds the capacity will be discarded, the debug.log only stores the latest audit information. It can be seen that the log information is not permanently saved and can be changed.

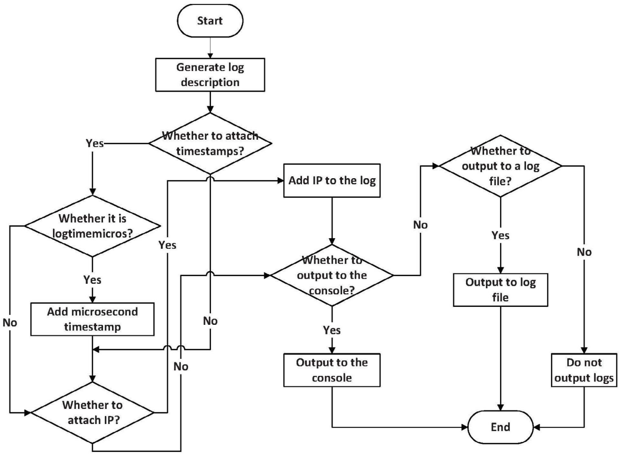


FIGURE 9. Blockchain log workflow chart.

The logs of Bitcoin are divided into three levels: debug, warning, and error. Currently, there is no fatal error. Debug log records the status information of the system during

TABLE 9. Bitcoin error audit classification.

Function	Method	Output Error
Initialization error	AppInit2Cold()	Winsock Library, Initial Integrity Detection, Wallet File Damage, etc.
Transaction error	CheckTransaction()	Errors in checking transactions, e.g., empty input and output.
	AcceptToMemoryPool()	Errors occur when validating the reasonableness of transactions and storing them in the trading pool, e.g., input being spent.
	CScriptCheck()	Script signature error
	CheckInputs()	Transaction input errors, e.g., total transaction input <total output.
	CheckSignature()	Error in checking signature
Block error	WriteBlockToDisk()	Errors in writing blocks to disk, e.g., file opening failure.
	ReadBlockFromDisk()	Error reading block from disk, e.g., failure to open block file.
	DisconnectBlock()	Error while disconnecting block links
	ConnectBlock()	Error connecting blocks, e.g., asset submission.
	CheckBlock()	Error checking blocks, e.g., Merkle root mismatch.
	ContextualCheckBlockHeader()	Check if block header information is wrong, e.g., block timestamp too early.
	LoadBlockIndex()	Error loading block index, e.g., failure to write Genesis block to disk.
Consensus error	CheckBlockHeader()	Proof-of-work error
	AcceptBlock()	Accepting blocks makes errors, e.g., failing to find proof-of-work.
Network error	RecvLine()	Socket error
	Read()	Error in peer. dat reading of connection node data file.
	Write()	Error in peer. dat writing of connection node data file
	Connect()	Connection error
	ProcessMessage()	Errors in listening for and processing different messages in the network.
Remote procedure call	JSONRPCError	Errors in remote procedure call requests, parsing, parameters, etc.

development and debugging; Warning log is used to record alarm information that may lead to errors; Error log is used to record exceptional errors during system operation. Table 9 shows the Bitcoin error audit classification.

The audit records in Bitcoin do not meet the requirements for classified protection in audit format and the recorded events are not specific enough. Bitcoin log can be outputted or not, and the output file content can be tampered with or even cleared, so the audit records **(items 3)** do not meet the requirements of CPC-2.0-L3. The improvement measures proposed for existing Bitcoin audit are as follows:

1) Establish a distributed blockchain system log network, and the logs are uploaded as transactions to the blockchain [59].
2) Refine the log entries. The audit content includes at least the date and time of event, the user, the type of event, the success of event, and other audit-related information.
3) Single-node function calls and status logs should be stored in the protected form to avoid deletion, modification or overwriting.

C. PROTECTION FROM MALICIOUS CODE

Smart contracts need to be executed by nodes involved in verification to ensure the accuracy of contract execution results. This requires the deployment and operation of smart contracts written by different users on the verification node, so it is very necessary to prevent malicious code.

The security issues of smart contracts are divided into two aspects: 1) Security issues of the smart contract program itself; 2) Security issues caused by the smart contract program to execution environment. According to the classified protection standard, this paper only discusses the second kind of security problem, that is, the problem caused by malicious smart contract code on computer, blockchain program and other smart contracts where the verification node is located.

Bitcoin's scripting system uses a stack-type operating environment, with direct addressing as the addressing rule, and the instructions are relatively simple, with no jumps or loops instructions. Therefore, it will not affect the external environment.

The Ethereum smart contract runs in the Ethereum Virtual Machine (EVM). EVM is a sandbox environment, isolated from the outside world, so malicious code will not affect the outside world. At the same time, Ethereum designs a gas mechanism to prevent malicious code from occupying too much computing resources and blockchain storage resources. Each step of the smart contract program will cost a certain amount of gas. Every time the data in blockchain is modified,

TABLE 10. Summary of evaluation results of blockchain system.

Categories		Items	✓/×		
			Bitcoin	**Ethereum**	**Hyperledger**
Distributed P2P Network Assessment	Software fault tolerance	Self-protection and self-adaptation	✓	✓	✓
	Resource control	Concurrent connection restriction	✓	✓	✓
		Connection timeout limit	✓	✓	✓
	Identification	Node link control	×	×	✓
	Data integrity	Anti-tampering of unicast	×	×	×
		Multicast communication tamper-proof	×	×	×
		Forwarding communication tamper-proof	×	×	×
	Security audit	Network status update	×	×	✓
		Network node dynamic monitoring	✓	✓	✓
Distributed Ledgers Assessment	Software fault tolerance	Standardization of ledger	✓	✓	✓
	Access control	Ledger access control	×	×	✓
	Data integrity	Storage integrity	✓	✓	✓
	Data confidentiality	Storage confidentiality	×	×	×
	Ledger function	Data non-repudiation	✓	✓	✓
		Ledger data synchronization	✓	✓	✓
		Ledger data idempotence	✓	✓	✓
Consensus Mechanism Assessment	Resource control	Consensus Resource Control	✓	✓	✓
	Backup and Recovery	Real-time backup	✓	✓	✓
		system hot redundancy	✓	✓	✓
	Consensus effect	Consensus fault tolerance	✓	✓	✓
		Consensus effectiveness	✓	✓	✓
		Consensus Consistency	✓	✓	✓
Contract Computing Layer Assessment	Identification	Performing entity authentication	✓	✓	✓
	Security audit	Behavioral event audit	✓	✓	✓
		Audit records	×	×	×
	Malicious code protection	Protection from malicious code	✓	✓	✓
	Data integrity	Transmission integrity	✓	✓	✓
	Data confidentiality	Data confidentiality	×	×	×
Statistics	Number of qualified items		19	19	22

it will also spend a certain amount of gas according to its size.

D. RESULT OF CONSENSUS MECHANISM

Through the above evaluation, Table 8 summarizes the achievement of smart contract computing layer in each evaluation item: the blockchain can meet the **(items 1,2,4)**, but the **(item 3)** fails to meet the standard. Because the consensus layer can achieve consistency in results, the contract layer above the consensus layer can verify the integrity of data (evaluation **(item 5)**). However, the data is not encrypted by cryptography in blockchain, so data confidentiality cannot be guaranteed (the evaluation **(item 6)** did not meet the standard).

IX. SUMMARY AND CONCLUSION

This paper proposes the general requirement under classified protection on blockchain evaluation by taking the chinese CPC 2.0 as an example. In order to ensure that the evaluation scheme meets the needs of countries to set up CNII based on blockchain, the scheme is proposed with the target to meet the requirements of CPC-2.0-L3 by proposing assessment requirements and enforcement proposals for the blockchain's P2P networks, consensus mechanisms, distributed ledgers and contract layer. Considering the specificity of the blockchain, this paper adds three evaluation items specially to the evaluation of distributed ledgers, such as data non-repudiation, ledger data synchronization, and ledger data idempotence. In the evaluation of consensus mechanism, consensus tolerance and consensus validity are proposed. Three main blockchain system (Bitcoin, Ethereum, Hyperledger) was evaluated from totally 28 evaluation items, as shown in Table 10.

As an assessment example of the Table 10, the evaluation results of Bitcoin system are summarized as follows: 1) The qualified points that meet the CPC-2.0-L3 requirements: software fault tolerance, backup and recovery, malicious code protection, and resource control; 2) The control points that do not reach the CPC-2.0-L3 requirements: identity authentication, access control, data integrity, data confidentiality, and security audit.

In the Table 10, it is easy to see from the evaluation results that either Bitcoin or Ethereum has reached 19 qualified points, and Hyperledger has 22. Exactly, Hyperledger is better than two others in the three evaluated fields: Node link control, Network status update, and Ledger access control. Hence, in order to meet the CPC-2.0-L3 evaluation standard of classified protection, the blockchain technology still needs to be improved.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[2] G. Mark, "Blockchain and suitability for government applications," *Public-Private Analytic Exchange Program*, 2018.

[3] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[4] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, Jun. 2018.

[5] H. Tian, J. He, and L. Fu, "A privacy preserving fair contract signing protocol based on public block chains," *J. Cryptologic Res.*, vol. 4, no. 2, pp. 187–198, 2017.

[6] D. A. Wijaya, "Extending asset management system functionality in bitcoin platform," in *Proc. Int. Conf. Comput., Control, Informat. Appl. (IC INA)*, Oct. 2016, pp. 97–101.

[7] Z. Tian, B. Wang, Z. Ye, and H. Zhang, "The survey of information system security classified protection," in *Electrical Engineering and Control*. Springer, 2011, pp. 975–980.

[8] Y. Zhu, Y. Zhang, D. Wang, B. Qin, Q. Guo, R. Feng, and Z. Zhao, "Research on blockchain evaluation methods under the classified protection of cybersecurity," *Chin. J. Eng.*, vol. 42, nos. 0007–191217, pp. 1267–1285, 2020.

[9] G. Bush, "Executive order 12829: National industrial security program," Office Federal Register, New York, NY, USA, Tech. Rep., 1993. [Online]. Available: https://www.archives.gov/isoo/policy-documents/eo-12829-with-eo-13691-amendments.pdf

[10] B. Obama, "Executive order 13526: Classified national security information," Office Federal Register, New York, NY, USA, Tech. Rep., 2009. [Online]. Available: https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

[11] B. Obama, "Executive order 13549: Classified national security information program for state, local, tribal, and private sector entities," Office Federal Register, New York, NY, USA, Tech. Rep., 2011.

[12] B. Obama. *Executive Order 13556: Controlled Unclassified Information*. Accessed: 2010. [Online]. Available: https://www.archives.gov/isoo/policy-documents/eo-13556.pdf

[13] B. Obama. *Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. Accessed: 2011. [Online]. Available: https://www.archives.gov/isoo/policy-documents/eo-13587.pdf

[14] H. C. Office. *Government Protective Marking Scheme Policy*. Accessed: 2010. [Online]. Available: https://www.nottinghamshire.police.uk/sites/default/files/documents/files/PS_171_GPMS_Policy.pdf

[15] H. C. Office. *Government Security Classifications*. Accessed: 2013. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

[16] J. Zhu, Y. Zhao, H. Yang, and S. Zhang, "The evolution of classified protection idea," *Inf. Secur. Commun. Privacy*, vol. 4, 2011.

[17] C. Shen, "Innovation and development of information security classified protection system," *Cyberspace Secur.*, vol. 7, no. Z2, pp. 5–6, 2016.

[18] Y. Gao, K. Huang, and X.-W. Li, "Cloud computing security requirements and measurement practices in the classified protection 2.0era," *J. Inf. Secur. Res.*, vol. 4, no. 11, pp. 987–992, 2018.

[19] Y. Tao, Y.-X. Zhang, S.-Y. Ma, K. Fan, M.-Y. Li, F.-M. Guo, and Z. Xu, "Combining the big data analysis and the threat intelligence technologies for the classified protection model," *Cluster Comput.*, vol. 20, no. 2, pp. 1035–1046, Jun. 2017.

[20] L. Z. Wang Ning, "The Internet of Things security protection level of the research," *Netinfo Secur.*, pp. 5–6 and 10, 2011.

[21] B. Xia, "Cybersecurity law and classified protection of cybersecurity 2.0," Publishing House Electron. Ind., Tech. Rep., 2017.

[22] Q. Guo, "Book of cybersecurity law and classified protection of cybersecurity," Publishing House Electron. Ind., Tech. Rep., 2018.

[23] W. Ethereum, "A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[24] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15.

[25] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[26] Y. Zhu, G. Guohua, D. Di, J. Feifei, and C. Aiping, "Security architecture and key technologies of blockchain," *J. Inf. Secur. Res.*, vol. 2, no. 12, pp. 1090–1097, 2016.

[27] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. Newton, MA, USA: O'Reilly Media, 2014.

[28] S. Ben Mariem, P. Casas, and B. Donnet, "Vivisecting blockchain P2P networks: Unveiling the bitcoin IP network," in *Proc. ACM CoNEXT Student Workshop*, 2018, pp. 1–3.

[29] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.

[30] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 4, pp. 1–14, Apr. 2017.

[31] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 1–28, 2018.

[32] D. Fullmer and A. S. Morse, "Analysis of difficulty control in bitcoin and proof-of-work blockchains," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5988–5992.

[33] A. Chepurnoy, T. Duong, L. Fan, and H.-S. Zhou, "Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 232, 2017.

[34] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[35] F. Borran and A. Schiper, "A leader-free byzantine consensus algorithm," in *Proc. Int. Conf. Distrib. Comput. Netw.* Springer, 2010, pp. 67–78.

[36] F. Saleh, "Blockchain without waste: Proof-of-stake," *SSRN Electron. J.*, Feb. 2018.

[37] D. Larimer, "Delegated proof-of-stake (DPoS)," Bitshare, White Paper, 2014.

[38] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proc. ACM Conf. Econ. Comput. (EC)*, 2016, pp. 365–382.

[39] B. Group. *Proof of Stake Versus Proof of Work*. Accessed: 2015. [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

[40] M. Levine, "Scientific method and the adversary model: Some preliminary thoughts," *Amer. Psychologist*, vol. 29, no. 9, p. 661, 1974.

[41] D. Somdip, "A proof of work: Securing majority-attack in blockchain using machine learning and algorithmic game theory," Ph.D. dissertation, Modern Educ. Comput. Sci. Press, Hong Kong, 2018.

[42] J. Heusser. *Sat Solving—An Alternative to Brute Force Bitcoin Mining*. Accessed: 2013. [Online]. Available: https://jheusser.github.io/2013/02/03/satcoin.html

[43] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[44] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *Proc. 24th USENIX Conf. Secur. Symp. (SEC)*, 2015, pp. 129–144.

[45] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer Peer Syst.* Springer, 2002, pp. 251–260.

[46] U. W. Chohan, "The double spending problem and cryptocurrencies," *Available at SSRN 3090174*, 2017.

[47] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and mtgox," in *Proc. Eur. Symp. Res. Comput. Secur.* Springer, 2014, pp. 313–326.

[48] Y. Zhu, R. Guo, G. Gan, and W.-T. Tsai, "Interactive incontestable signature for transactions confirmation in bitcoin blockchain," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, Jun. 2016, pp. 443–448.

[49] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[50] K. Sekiguchi, M. Chiba, and M. Kashima, "The securities settlement system and distributed ledger technology," Bank Japan, Tokyo, Japan, Tech. Rep., 2018.

[51] A. Urquhart, "The inefficiency of bitcoin," *Econ. Lett.*, vol. 148, pp. 80–82, Nov. 2016.

[52] K. T. Son, N. T. Thang, T. M. Dong, and N. H. Thanh, "Blockchain technology for data entirety," *Sci. Res.*, vol. 6, no. 6, pp. 68–75, 2018.

[53] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Secur. Privacy*, Apr. 1980, p. 122.

[54] M. Szydlo, "Merkle tree traversal in log space and time," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2004, pp. 541–554.

[55] M. Jakobsson, T. Leighton, S. Micali, and M. Szydlo, "Fractal Merkle tree representation and traversal," in *Proc. Cryptographers Track RSA Conf.* Springer, 2003, pp. 314–326.

[56] S. Delgado-Segura, C. Pérez-Solà, J. Herrera-Joancomartí, and G. Navarro-Arribas, "Bitcoin private key locked transactions," *Inf. Process. Lett.*, vol. 140, pp. 37–41, Dec. 2018.

[57] N. Stanciu, "Importance of event log management to ensure information system security," *Metalurgia Int.*, vol. 18, no. 2, p. 144, 2013.

[58] J. Kreps, N. Narkhede, and J. Rao, "Kafka: A distributed messaging system for log processing," in *Proc. NetDB*, 2011, pp. 1–7.

[59] L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone, "A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database," in *Proc. 13th Eur. Dependable Comput. Conf. (EDCC)*, Sep. 2017, pp. 151–154.

DI WANG received the B.E. degree from the Department of School of Computer and Communication Engineering, University of Science and Technology Beijing, China, where she is currently pursuing the MA.Sc. degree. Her research interests include blockchain and smart contract.

YAN ZHU (Member, IEEE) was an Associate Professor of Computer Science with the Institute of Computer Science and Technology, Peking University, China, from 2007 to 2013. He was a Visiting Associate Professor with the Department of Computer Science and Engineering, Arizona State University, from 2008 to 2009. He was a Visiting Research Investigator with the Department of Computer and Information Science, University of Michigan-Dearborn, in 2012. He is currently a Professor with the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His research interests include cryptography, secure computation, and network security.

YI ZHANG received the M.A.Eng. degree from the Department of School of Computer and Communication Engineering, University of Science and Technology Beijing, China. She is currently a Staff with the Institute of Software Chinese Academy of Sciences, Beijing, China. Her research interests include blockchain and smart contract.

GUOWEI LIU is currently the Senior Engineer with the Beijing Municipal Bureau of Economy and Information Technology. His research interests include big data, security systems, security management, and standard.