IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 14, 2018, accepted December 14, 2018, date of publication December 19, 2018,
date of current version January 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2888697

The Challenges of Existence, Status, and Value for Improving Blockchain

FEI LIN AND MINQIAN QIANG
School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China

Corresponding author: Minqian Qiang (minqianqiang@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602141 and in part by the Zhejiang Provincial Science and Technology Plan Project of China under Grant 2018C01111.

ABSTRACT Blockchain is defined as a distributed ledger technology that can implement financial models. An improved blockchain provides a democratic virtual economic system (DVES) that can verify payments, reach consensus, and store encrypted data in virtual economic systems. In this paper, we review the latest progress and possibilities in improved blockchain with respect to openness, data security, and scalability. This paper outlines the challenges of value, existence, and status (VES) and the state-of-the-art solutions for improved blockchain. Then, this paper discusses the VES in terms of distributed energy, ownership certification, infrastructure, and other fields. More importantly, it analyzed the importance of scale out, which can be a key enabler to solve the main practical problems in constructing DVES.

INDEX TERMS Improved blockchain, DVES, scale out, tiered.

I. INTRODUCTION

Since the article [1] was put forward by Satoshi, blockchain has been heated up on global scale. The most successful application, Bitcoin, brought encryption technology into the sight of folk. Blockchain is a composite technique for trusted data flows in an untrusted environment. In blockchain network tier, vertification nodes legalize transactions on the longest hash chain. Each block contains multiple legal transactions. Taking transactions and clearing business in the financial industry as an example, the central database cannot solve the multi-party trust problem. Every participant needs to maintain a database for carrying their own business data to cause information island, which increase the cost of labor. Blockchain is a good solution for data transmission management in distributed networks: all transaction vertification nodes need to ensure the comprehensive backup of transaction history. It can be considered as a shared database which was inspected by multiple untrusted parties.

Unlike the concurrency control in trusted distributed database [2], [3], blockchain1.0 consider the existence of Byzantine nodes [4] in the network may perform malicious behavior. Replicable state machine model between node A and B in blockchain1.0 are generated with full backup. Transaction vertification nodes called miners always pursuit the Unspent Transaction Output (UTXO) via massive calculation. The miners are willing to spend electricity cost to pay for the record right of the next block. Competition for rights ensure blockchain1.0 are naturally able to resist double spend attack [5].In theory, neither party can completely control the process of parent chain. Miners can only update status or verify legality of the data on chains in strict accordance with rules.

In December 2013, Ethereum [6] application platform was developed by Vitalik Buterin. In addition to the built-in ether coin which implements cryptocurrency, this system also provides Turing complete engine which is the first time to be used on behalf of blockchain2.0. In December 2015, the Linux Foundation launched an open source blockchain project Hyperledger to develop the cross industry commercial blockchain platform. A few projects brought into Hyperledger, such as Fabric, Iroha and Sawtooth Lake, etc. The most striking technology is the consortium blockchain Fabric for enterprise Backend as a Service (BaaS). In April 2016, R3 released Corda, a distributed ledger platform designed for financial institutions. So far, the architecture and tiers of blockchain system caused extensive discussion in the academic community. Garay [7] deeply analyzed the key technologies of the Bitcoin system. At the SIGMOD17, Dinh *et al.* [8] proposed a performance evaluation tool for consortium blockchain in regard of throughput, latency, scalability and fault tolerance. Shortly after, they published a comprehensive performance evaluation report for Ethereum,

Parity and Fabric [9]. Lin *et al.* [10], Cohen and Zohar [11], and Muzammal textitet al. [12] separately proposed original views of the blockchain applications in the database domain. BigchainDB was proposed in 2016. It not only has the advantages of high throughput, low latency, large capacity, rich query and distributed database due to the underlying database uses the RethinkDB, but also decentralized, non-tamperable, and other blockchain characteristics. So it is considered as a database fused with blockchain. Yuan and Wang [13], Cai *et al.* [14], and Shao *et al.* [15] put forward the development of underlying blockchain. Qian [16] designed a CBDC to promote the lawful digital currency which is only used in closed loop system. In the dual model, system regulates the issuance, transfer and withdrawal of currency from circulation. The model pays more attention into the compatible integration with existing financial system. DVES proposed in this paper is based on the improved blockchain technology. In order to build a virtual economic system in the future parallel society, the breakthrough of key technologies learn from the current actual development.

The rest of the paper is organized as follows. Section 2 puts forward the basic model of encrypted ledgers and summarizes the challenges for improved blockchain. Section 3 analyzes practical value based on the perspective of decentralized applications. The challenges and solutions of existing data security for tiered blockchain are discussed and analyzed in Section 4. In Section 5, we discuss the challenges of status in expansive research and feasible solutions before concluding this paper in Section 6.

II. PREVIOUS WORK

There have been a number of discussions about the tiered blockchain. The following provide a systematic overview of data structure, network tier, consensus algorithm, and contract engine. Meanwhile, issues and challenges encountered in the key breakthrough areas are highlighted.

A. BASIC MODEL

1) DATA STRUCTURE

The integrity, sequence and validity of block are checked by block header which includes version number, previous hash, merkel root, timestamp, target difficulty, random nonce. All nodes run the blockchain application can generate a pseudo-random private key by SHA256 to encrypt payments. The corresponding public key was generated by elliptic curve encryption algorithm with the parameter Secp256k1. Public key has multiple formats with multiple encryption and format conversion. For example, a kind of public key with 33 character encoded in Base58 format for creating objects between network nodes. Both hash for block headers and merkel root plan a global association strategy by SHA256 for anchor data. In addition, blocks are not necessarily organized by single linked list. In order to solve the forks caused by the interval time between connected blocks, Ethereum proposed the protocol GHOST in 2015. The protocol GHOST allows uncle blocks on the forks can not be discarded. IOTA uses the structure of the directed acyclic graph [17] and PoW to organize the trading units. Each unit with single out-degree and several in-degree contains only one transaction. The entire graph can be calculated based on node weight after at least two units are linked to indicate means two transactions have been confirmed.

2) NETWORK TIER

The consortium blockchain improves the speed of the vertification and authentication by adjusting the decentralization or vertical scalability. The architecture pays more attention to risk management for upgrading traditional enterprise application. In public blockchain scenario, the network environment is fair although the types of nodes are different. It is unsecured for nodes that exposed network brings a multitude of security issues, including eclipse attack [18], sybil attack [19], statistics and analysis [20]. The details of network safety will be discussed in Section 2.2. In spite of the disparity of hash power exist in Bitcoin nodes, the network tier is still connected to the flat topology in the economic cycle of DVES. There are no special leaders or hierarchical structures. Each node can assume the responsibilities such as routing, verifying, propagating and discovering.

Based on mentioned above, Ethereum integrates the protocol GHOST to avoid consistency risk and high rate of block abandonment caused by rapid confirmation and spread of messages. According to the amount of data stored, nodes can be divided into full nodes and simplified payment verification (SPV) nodes. Full nodes generally needs to update and verify the growing parent chain in real time to verify payments. However, SPV nodes perform payment validation before transactions are verified and written into parent chain by the miners.

3) CONSENSUS ALGORITHM

The number of untrusted nodes and total nodes in a network are supposed as f and n. For synchronous interaction and unreliable networks, the Byzantine generals problem can be solved under the condition of $n \geq 3f + 1$ [4]. In the case of asynchronous interaction, it can be proved that deterministic consensus algorithms cannot tolerate single node failure [21]. The XFT consensus assumes that it is extremely arduous for malicious nodes to control the entire network and Byzantine nodes at the same time. What is more, it simplifies the mode of BFT message that the Byzantine general problem can be solved when $n \geq 2f + 1$. In addition, Ripple network proposed RPCA consensus algorithm based on a set of allowable nodes, which can solve the Byzantine general problem when $n \geq 5f + 1$.

In order to solve the security problems that arise from untrusted nodes, Bitcoin uses mechanism Proof of Work(PoW) to reach consensus with the same difficulty as the block height. The miners can only run hash enumeration for hash meet the standard. The calculation process make up a random pseudo-random nonce n and a leading block header

by SHA-256. When the result meet $H(n||H(B)) < target$, the cycle for enumerating can be broken. PoW theoretically guarantees that the probability of meeting the block header for malicious nodes in advance is next to zero before normal nodes succeed. Although Bitcoin may abandon blocks, most of the power-maintained chain grow faster than any forks. In order to obtain rewards for calculating, packaging and broadcasting, benefit-driven miners are more proactive in promoting parent chain. In mathematics, when Byzantine nodes account mining power ratio q, normal nodes account $p = 1 - q$. As long as $p > q$, the probability for evil node getting the block z meets $(q/p)^z$. The evil mining is in according with Poisson distribution. According to the paper [1] has proved the formula which can be seen the cost of any double spend attack with $\lambda = z\frac{q}{p}$ is increasing exponentially.

$$1 - \sum_{i=0}^{k} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (q/p)^{(z-k)})$$

4) CONTRACT ENGINE

Ethereum has customized the underlying virtual machine. On top of this, the scripting language such as Solidity supports Turing complete and can implement customized contract functions.Smart contracts in secure area are scripts that extend the functions of blockchain or enrich the upper interfaces. In Ethereum, deployed the contracts are loaded by Ethereum Virtual Machine(EVM). If external requests involve modification, the entire network nodes need to reach consensus.

In Fabric blockchain, deployed contracts are packaged into a Docker image. Each node launches a new container based on the image and calls initialization functions in the contracts. Then compiled smart contracts in secure area wait for calling by the external application. The modification operations can be automatically generated and recorded in the state database. Smart contracts also support registration and notification operations with the internal time so that proactively alerting external applications for critical events occurring within the contracts. The Fabric blockchain is applied to the consortium chain. The only channel for interaction between enterprise applications built by Fabric and blockchain system is smart contracts. It supports high level languages such as Java or JavaScript and the compilation technology is mature. The essence of smart contracts in Fabric blockchain platform is to implement the Init, Invoke, and Query functions in the chaincode interfaces which are used to implement initialization, modification, and query of state data.

The contracts provided by the Bitcoin platform are equivalent to a set of simple scripts for processing payments. To avoid possible vulnerabilities in bitcoin, Turing complete is not supported. Currently, the contracts only have access to intra-chain data and cannot actively listen for and respond to out-of-chain events.

TABLE 1. Comparison of the contract engines.

Project	Year	Engine	Language
Bitcoin	2009	Bitcoin script	Ivy,Balzac
NEO	2014	NeoVM	C,C++,Go
Ethereum	2015	EVM	Solidity
Lisk	2016	N/A	Javascript
EOS.IO	2017	EVM/eWASM	C,C++
Cardano	2018	IELE	Plutus
Fabric	2016	Docker	Go,Java
Sawtooth	2016	Docker	Python

B. CHALLENGES

1) THE CHALLENGE OF EXISTENCE

The challenges of existence mainly refer to security issues including preservation, interaction and key storage for the wallet.

Control re-centralized: For SHA-256 algorithm, the shortage of ASIC resistance may result in being controlled of centralized mining power. In order to avoid algorithm defect, Alcock and Ren [22] and Biryukov and Khovratovich [23] believe that algorithm Equihash [22], [23] should be added to Proof of Work. The hash power of algorithm can be weakened when the GPUs improve. But this solution does not decrease energy consumption or speed up payment validation.

Isolation interaction: To avoid vulnerable scripts or interfere with each other, the environment for implementation is effectively isolated as the form of sandbox to limit the scope of malicious code. At present, the sandboxes for popular blockchain platforms are virtual machine and container.

Private key storage: The wallet private key is directly related to account security, which needs to be sufficient protected. To prevent attackers from extracting key information for core cryptographic algorithms, one can use keyless cryptographic algorithms, code obfuscation techniques [24] or encrypting keys using encryption algorithms based on sbiometrics factor authentication [25]. A solution based on Trusted Execution Environment (TEE) and assisted hardware can be one of the options for securing digital accounts [26].

2) THE CHALLENGES OF STATUS

DVES based on blockchain not only requires safe storage, but also efficient and smooth interaction. The current blockchain systems have serious scalability bottlenecks. Bitcoin can only support up to 7 transactions per second. Transaction confirmation which includes transmission and packing delay. Obviously, increasing block capacity is a way to improve transaction throughput of system. More transactions are confirmed by a larger block in a round of consensus process. However, increasing the block size arbitrarily cannot solve the problem thoroughly.

Larger block can trigger network congestion and impact the performance of blockchain. It is still difficult for different chains to interact with another. In reality, many kinds of business scenarios carry different needs. To realize the real value interconnection, we need to realize the interaction between one chain and another so that blockchain cannot be

called islands. The details of cross chain will be discussed in Section5.5. Besides other solutions, transforming from competitive one to cooperative one can offer a better transactions per second.

3) THE CHALLENGES OF VALUE

The challenges of value are mainly related to the incentive issuance and distribution mechanism. Take bitcoin as an example, incentive model integrate reward and consensus. It guarantees the fluidity of market because of the profit seeking capital hoards bitcoin. Therefore, in the case of ensuring market liquidity and cashing out, the price of token skyrocket or plummet. If the direction of parent chain is controlled of single centralized mining pool, it means that the value of parent chain will be diluted. If the mining pool where private miners located occupy more than one third of the total computing power, the income obtained can be better than calculation cost. The rational miners continuously joined the private mining pool until the occupation of computing power exceeding 50% of the total amount [27]. Actually, characters are often not completely rational when multi-party game exists. Therefore, it is still arduous to make a private mining attack.

In P2P network, as long as a certain amount of nodes are controlled, eclipse attack which belongs to partition attack can be performed, thereby it can initiate 51% attack and control parent chain. Assume that three nodes are mining, two of which possess 30% of the total computing power and the rest has 40% of the total mining power. If attackers control the rest with 40% power, they can isolate other nodes to make them unable to reach consensus. Therefore, attackers need not possess more than half of the computing power to initiate 51% partition attack. The precondition for initiating such an attack is that all nodes to which isolated node is linked are under the control of attackers. This kind of attack is easier to achieve when the network scale is small. To avoid re-centralization or high-frequency fork, Algorand [28], [29] applies BBA algorithm to translate a multi-consensus problem into a binary result. After multiple rounds of algorithm VRF and algorithm GC, Algorand nodes can reach consensus without fork or any other parties in an untrusted environment. A design primitive for the multi-party was put forward by Bentov secure mining protocol based on anonymous lottery for hybrid blockchain system [30].

According to comparison and analysis with the three consensus algorithm in papers [31], it has been shown that current mining pool of PoW has become centralized. In order to counter the contradictions of computing power and energy conservation, folks in the industry proposed to use the competition of equity to replace the competition of power. Cryptocurrencies released recently use consensus algorithm like PoS to achieve energy reduction and transactional concurrency. In order to maintain the safety of parent chain, miners working on parent chain have a tacit understanding of maintaining their own interests and safety on parent chain. As far as Proof of Work, the designed philosophy is natural coupling of economic model and data value which makes application designers aware of computing nodes actively maintaining decentralized network security. It is apparently expensive for nodes to reach consensus in shared, open and dynamic P2P network. The existing consensus mechanisms have their own shortcomings. In order to avoid the situation that mining pools converge together, it is indispensable to provide a design paradigm for scalable consensus algorithm which can be completely decentralized as needed. Looking for a pivot or compromise is also in line with the real situation of most application scenarios in real life [32].

III. DECENTRALIZED APPLICATION RESEARCH

The reasons why practical applications are difficult to land should be analyzed from the perspective of VES. The next part will be discussed with VES based on researching decentralized applications.

A. SHARED RESOURCE

Blockchain further promoted the development of a ''shared economy'' based on shared resource, which means that transactions are conducted directly between producers and consumers. It can significantly reduce the resource cost and improve the transaction efficiency. With technical reference for multi-source systems, evaluation criteria and tiered models of virtual power plants were proposed in paper [33]. Blockchain can promote the integration of energy interconnection with source flow, information flow and value flow. New business models can be introduced such as photovoltaic power station crowdfunding and asset securitization. This method can be used to reduce the difficulty of financing and operation in the photovoltaic industry.

At present, the most important problem for this model is to determine the correspondence between crowdfunding objects and value mediums [34]. Venture production studio ConsenSys and developer LO3 used Ethereum as a platform to implement a cheaper and more reliable solar trading system in the community. It proposed seven components to realize a double auction mechanism based on Ethereum [35]. The project need to be confirmed by the validation from clients in order to increase investment enthusiasm and reduce the investment risk of microgrid users. The developer also called for the improvement of relevant laws and regulations to support the format. After verifying token price, it is also necessary to use high-precision smart meters to handle with the data existence challenge.

In an unified ledger using blockchain, data flow between multiple parties can be tracked and managed in real time. The cost of shared data can be effectively reduced by simple control of access rights. When dealing with state issues, a mixed consensus or expansion approach is usually adopted. Zhang *et al.* [36] innovatively proposed that distributed energy systems designed as a tiered architecture with single blockchain model in each tier to manage its logical and physical functions. The advantages of energy blockchain include: 1) It need not an unified central organization for

scheduling control, individual in the system can make self-schedule decision [37]; 2) General type for multi-energy [38] provides an unified platform for different energy information system; 3) It guarantees data confidentiality and reliability in the case of multi-party; 4) It provides the proof of concept for a decentralized energy trading system that uses multiple signatures and encrypted information; 5) It enables peers to negotiate energy price anonymously and trade securely [39]; 6) It can handle with problems such as precise measurement problems, interaction problems, self-discipline control and optimization decisions. The theory PCV [40] considers that horizontal multi-source complementation and vertical ''source network load storage'' optimization coordination. Wide area balance which focus on three dimensions include physical, information and value is more paramount for shared resource. It proposed distributed energy nodes access verification process, a coordinated control scheme, and a trusted data distributed authentication. Chen *et al.* [41] proposed the optimal energy distance algorithm for P median layout model based on ''station-net'' graph. The OpenStreetMap system map is edited twice by Josm map software, then applied to the energy management and storage center. It was demonstrated a better economic and energy efficiency performance in the case of the P median model.

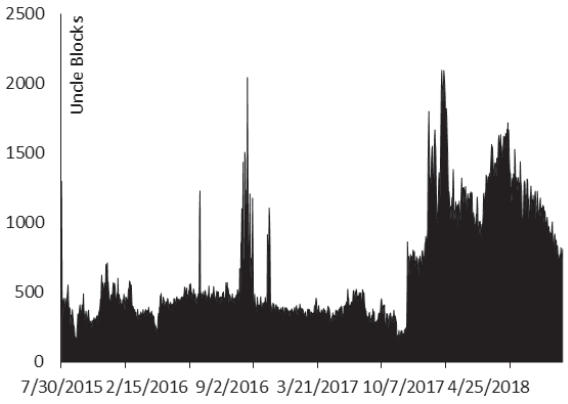

FIGURE 1. The trend of uncle block quantity.

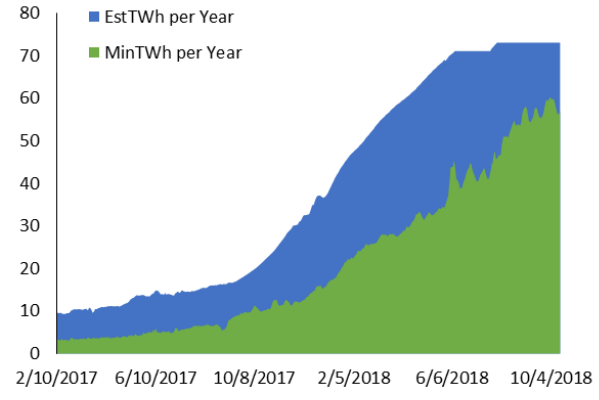

FIGURE 2. Energy consumption under the PoW.

B. OWNERSHIP CERTIFICATION

At present, a large number of enterprises are trying to obtain much user information from various ways. From the perspective of credit information, there are problems about obtaining effective information: 1) Insufficient effective data; 2) Poor data correlation. At the moment, users are so sensitive to privacy that expose fewer data to third party. 3) Insufficient timeliness. Data obtained by enterprises is often outdated or even inaccurate. Based on above, blockchain can be used to manage the ownership certification. It has low requirements on the status of data. The applications for ownership authentication in this paper focus on data security issues. Ownership management is mainly used for the management and traceability of ownership rights such as property rights or copyrights, including automobile, house, art, digital publication, etc.

There are several major problems in tenure management: 1) Confirmation and management of ownership of goods; 2) Security and reliability of transactions; 3) Certain privacy protection. Once the contract is approved, the blockchain ensure that the contract methods can be accurately executed and the asset ownership can be track. Tian *et al.* [42] and An *et al.* [43] and other scholars have done research on the blockchain applications in credit information and ownership management by cryptography techniques. Confirmation for item ownership [44] proves the existence, authenticity and uniqueness of valuable things such as text, video, audio and degree. Once the ownership is confirmed, its transaction records or change can be recorded on blockchain. In conjunction with technologies such as biometric identification [25], data source traceability can fundamentally guarantee data integrity and consistency thereby protect the uniqueness of the ownership.

At the same time, as a public service facility, public welfare facilities include voting systems which need to be traceable, non-tamperable, charity or voting elections without fraud [45], [46]. In addition, the use of blockchain to optimize the deficiencies of existing solutions can effectively simplify the process, improve efficiency and avoid the problem of information opacity and tampering. Due to the traceability of blockchain, simple source vertification is used to obtain source evidence which can be traced and solved in time.

However, there are still a host of problems in the present research of ownership certification management: 1) Data existence problems, whether the clients safely carry out key management; 2) Regulatory issues of personal data storage and transparency; 3) How to protect the ownership of individuals record; 4) The value problem is based on education, which is based on the credibility of the blockchain economic model; 5) The existing infrastructure is not enough to ensure the security and real-time of the data and how to reflect the advantage of blockchain systems. These are just issues mentioned in this article. Once they are put into operation, new problems will emerge out. At that time, it is indispensable to make corresponding changes to be realistic combine the actual process.

C. INFRASTRUCTURE

The domain name service system relies on the resolution of the root name server. Under the current Internet technology architecture, it is a centralized network topology with 13 root servers as core. The domain name service system management organization has top-level domain custodians in the department of ICANN. The service system has an organizational structure like tree. Key resources such as Ethernet IP address adopt a centralized management mode. In order to deal with the risk of status and existence for central domain name service, it is necessary to establish a decentralized organizational model.

Take centralization of the root domain name service system as an example, more and more scholars have begun to study the decentralization of the root domain name service system. Zhu and Zhang [47] an autonomous open decentralized network domain name service system DDNS. The distributed consistency algorithm in DDNS was designed to construct a decentralized domain name resolution model. Park and Hyuk [48] proposed a secure, efficient and scalable hybrid network architecture based on SDN. The blockchain architecture is used to make the mining storage nodes and terminals closer. The hybrid consensus algorithm of Argon2+PoW is adopted. The block confirmation time, block size and TPS relationship model are analyzed under the network architecture. It is believed that there are limitations in the effective deployment and cache activation of edge nodes.

Differ from the distributed file system IPFS [49], Dong *et al.* [50] believed multi-tier metadata information can be extracted from shared data set and domain indexes. It can be established to solve the efficient discovery service by consensus nodes. What is more, the paper begins with the transaction record format and consensus mechanism, then establish a blockchain based data transaction to achieve transparency, anti-collision and other fraudulent behaviors. Finally, it writes calculation contracts based on the mining needs for data demand. With secure multi-party mining and differential privacy technologies, it guarantee data owner calculation and output privacy.

Value issues are reflected in other infrastructures. Matthew investigated the value model of Bitcoin for payroll [51]. This combination of certifying incentives and traditional financial means is a new opportunity in the future. Specifically mentioned in Section2.2.2 above, no longer repeat them. Song *et al.* [52] realized data governance collaboration by building multi-party collaborative processes, standardization process and update process. Secure, reliable data and access control increased the efficiency and security of data and laid a theoretical foundation for improved blockchain systems.

D. EDGE COMPUTING

Edge computing for blockchain has captured industry attention in recent years. Robert *et al.* [53] and Xiong *et al.* [54] have conducted in deep research in the IoT blockchain field. Prior to above, Robert designed the open IoT system bIoTope as a five tiers architecture, including physical tier, access tier, search tier, shared tier and component tier. It built a digital trading market environment in the control of incentive strategy. It does not depend on the service provider operator for LoRa technology any longer. Individual with LoRa antenna at the gateway can be granted access to any third parties. The model effectively controlled the interoperability and independence between physical units. Khan and Salah [55] designed the hierarchical computing architecture based on edge computing and blockchain and discussed the role of blockchain to security problem for edge computing.

E. SUPPLY CHAIN MANAGEMENT

There are multiple entities involved in supply chain, including capital flow, information flow and logistics. A large amount of complex collaboration and information exchange between these entities. Different entities hold their own flow information. It leads to serious opaque information in supply chain, which spends more time and money. But fraud and counterfeiting in the complex flows are arduous to trace and deal with. For supply chain applications, Leng *et al.* [56] and other researchers constructed double-chain structure which can apply to production, sales, storage, resource rent-seeking and matching mechanisms, which cover the entire process of agricultural data collection and processing. It can be used in full aspects of agricultural supply chain information management to ensure the quality and safety of agricultural products.

From the perspective of agricultural supply and marketing, double-chain model is analyzed to reconstruct the agricultural supply chain, including incentives and punishment for behavior analysis. In the control of PoS, transaction data flow is open and secure. It can adaptively complete rent-seeking or matching resources to improve the reputation and overall efficiency for the public service platform. Although the simulation experiment did not consider a multitude of practical factors, it achieved fast response at system level.

IV. SECURITY AND OPENNESS

A. PRIVACY PROTECTION

Transaction data on public chain can prevent data from tampering, it brings privacy problem. Take the blockchain platform Ethereum as an example, public key is generated by SHA256. The address is not directly related to real identity information. The platforms achieved a certain degree of anonymity [57], but attackers can cluster association technology for public content such as public key address and transaction information in an open trading environment. For real name authentication of e-wallet or bitcoin exchange, it can reveal the true identity of the user by association between multiple inputs within the same transaction, correspondence between IP address, bitcoin address in network messages, etc [58].

Blockchain privacy protection needs to cover up the details in the transaction and verify the correctness. The current privacy protection schemes for blockchain

include mixed currency, ring signature, zero-knowledge proof, homomorphic encryption. Relevant scholars have done a lot of research on this field [20], [26], [59]. Tang and Gao [60] proposed a secure multi-party mining key shared protocol and implemented multi-signature wallet for cryptocurrency. It proposed that each transaction uses a brand new address so that eliminate association between different address. It achieved the irrelevance between multiple transactions [61].

CoinParty rebuilt financial privacy, using threshold signatures in hybrid network portfolios and providing user-mixed transaction services at the browser level. Although it supports better privacy protection, cross-chain operation and high scalability, defects that it is limited to the cryptocurrency applications are also obvious [24]. Cecoin used token impact to punish malicious nodes who generate fake key or connections. It firstly proposed related technical support to illustrate the system implementation goals as an enhanced version for PKI services [62]. Monroe applied ring signature to hide the sender of the transaction. It encrypts the transaction data by private key from sender and public key from random unrelated node, then decrypts it with recent public key. The limitation of the mixed currency lies in the need to face the test of supervision.

Zerocoin implemented unrelated transaction technology for blockchain. On the basis of Bitcoin, it allows traders to prove the transaction is correct. Zerocoin without leaking the transaction data or any other information. When one redeems Zerocoin, it present a UTXO certification and a zero-knowledge proof to derive the unlinkability of the transaction [63]. By extending Zerocoin, Hawk implemented a privacy-protected smart contract [64] which supports privacy protection for any transactions. Zero-knowledge proof is now more used in the field of cryptocurrency. The homomorphic encryption based on the homomorphic mapping guarantees the same result of the first operation and the first encryption so that transaction can be verified depend on the encrypted data. To resist the attack of quantum mining, homomorphic encryption algorithm compromise computing performance and it is still a big gap from the actual application.

zkSNARKs is an implementation of zero-knowledge proof for Zerocash that verifies the correctness of a calculation without performing or achieving input. At the camp in Cornell of Ethereum/IC3Boot University in July 2016, the researchers completed a demonstration for zkSNARKs code in Ethereum. Fabric1.0 used multi-channel that two or more parties need to establish a link with each other for the first transaction [65]. Then, all transactions can be completed rapidly on the channel later. On separate blockchain, only users on this channel can access data. Multi-channel can assign different transactions to multiple chains which are isolated from each other to enable private transaction and ensure the privacy of data. Therefore, the current major security issues are concentrated on public chain.

How to balance security and transparency? For privacy protection schemes such as zero-knowledge proof and homomorphic encryption, how to expand application, improve mining efficiency or speed up application landing is the most urgent research work in the future.

B. VULNERABLE CONTRACT

Smart contracts deployed on the public chain are easily exposed by hackers because they are exposed on the open network. They are gold mines for hackers that it easily caused irreparable damage. Velner *et al.* [66] proposed that contract tier script vulnerability easily leads to centralized mining control of 95%. In this case, members of the malicious pool could also attack other miners. Strengthening smart contracts check is a paramount guarantee to improve the security of blockchain. The literature [67] innovatively proposed smart contract organization method based on semantic analysis by the semantic analysis of application scenarios and transaction conditions of the smart contracts.

Formal verification is an effective way to audit smart contracts. It is used to standardize, develop and test hardware or software by mathematical verification based on logic calculus, discrete events, program semantics, formal language, automata theory, type systems and algebraic data types. The method improves the security and reliability of the contracts. Formal verification mainly includes two techniques: theorem proof and model verification. The existing theorem prover includes user-guided automatic derivation tool, proof tester and composite prover. User guided automatic derivation tools are ACL2, Eves, LP, Nqthm, Reve, and RRL. These tools are guided by lemma or defined sequences. Each theorem uses established derivation, lemma-driven rewriting, and simplified heuristics. Model verification is a technique based on a finite model and testing the expected characteristics of the model. The test is the brute force search of the state space.

The searching can be terminated due to the finiteness of the model.Before applying this model to Ethereum, the contracts are automatically compiled by Solc to generate binary bytecode and corresponding ast parse tree. All member functions of the contract can be extract according to the ast tree. Function signature is generated and input parameters are constructed by using ABI encoding from the rule set. The contract function is called in turn, and the bytecode of the contract can be run on EVM to generate a test report. There are already a lot of academic studies about semantic model for EVM, which are applied to the formal verification framework and verification method for different scenarios [64], [68]. Formal verification cannot ensure the Dapps must be correct, but it can maximize the understanding for smart contracts and find out the inconsistency, ambiguity and incompleteness errors as much as feasible.

V. PROGRESS IN SCALABILITY RESEARCH

A. ONCHAIN EXPAND

Blockchain systems should be scalable which represents system resiliency. In the process of increasing the concurrent

workload, the linear growth for entire system can be only achieved by the addition of physical devices to realize high throughput and low latency.

The simple solution for capacity expansion is to change the limit of size for single block in data tier. There are now several proposals to directly increase the size of single block by hard fork: In BIP101, it is recommended that the block size limit should be directly increased to 8MB, after which the limit is doubled every 2 years until it reached 8G. In BIP102, it is recommended that the block capacity directly increased from 1MB to 2MB. The current dilemma [69] can be solved without changing any other rules. Bitcoin proposed that unlimited block capacity ceiling is no longer a fixed value and can be changed by miners. The expansion criteria should respect the democratic resolution of community. Miners can vote by the current block capacity limit and decide for the new block capacity cap within a certain floating range [70].

The advantage of increasing the capacity for single block is easy to implement and hardly increased complexity of the system. However, in this case, miners need to spend a longer time on verifying the synchronization blocks generated by the new nodes. It may seem ineffective to the old nodes, which inevitably increased the risk of forking. So the old nodes chose to extend the chain which does not contain the new block rather than accept the block generated by the new nodes. Therefore, as long as hard fork deployed with the old nodes existing, two parallel branches can run independently.

B. IMPROVED CONSENSUS ALGORITHM

Bitcoin-NG: This performance improvement is achieved by breaking the bitcoin blockchain operation into two parts: leader election and transaction serialization [71].The algorithm PoW is reused, but PoW is only used to select the leaders. The leaders can write a block containing public key and multiple microblocks that they can prevent forking. These blocks are generated and broadcasted after an intensely short interval. The scope that a leader is responsible for writing called a ''domain''. The last of critical block used for consensus leader elections point to the last micro block with newest transaction. Public key of the miner is merely included in the key block. All subsequent micro-blocks are signed with the corresponding private key to prevent faking micro-block. The incentive mechanism is a hard-coded split-incentive, which may have an allocation vulnerability [72].

Algorand: Gilad *et al.* [29] proposed an improved consensus protocol with encrypted lottery. In order to avoid the high risk of fork, recentralized of power and bad performance with resource wasting, Algorand adopts a round robin election method. First, each round passes the PoS weight to select the committee to ensure the witnesses could maintaining data asset security on the parent chain. The round robin results need to adjust the weights and filter the sub accounts to prevent sybil attacks. Anonymous lottery algorithm which is green and random will be a crucial algorithm instead of PoW. The committee has the legitimacy of the block signatures packaged by the election leader and the vertification leader.

Algorithm 1 Trusted Anonymous Lottery Algorithm. N is Oridinary Node,N_v Is Verifier Node, N_s Is Proposer Node,k Is the Number of the Current Block,L_i is the Leader in i-th Turn, j is the Amount of Potential Sybil Object

hypothesis and letterre presentation
$N \geq 3t + 1, \rho \geq 95\%$,
$\mu(complete\ block) \gg \pi(signature\ hash)$,
$\Lambda(broadcast\ delay) \gg \lambda(encryption\ delay)$,
$\mu \propto \Lambda, \pi \propto \lambda, \omega = 50000$,
when N_v,$\tau_v \approx 4000, p_v = \frac{\tau_v}{\omega}$;
when N_s,$\tau_s \approx 26, p_s = \frac{\tau_s}{\omega}$;
func $VRF_v(sk, seed, role, \tau_v)$:
$H_{sk}(seed, role).R \rightarrow \pi, hash, p$;
if $p < p_v$,*choose k as* N_v;
when $\ni B(k'; \varpi', p_v) = k$ *do* $j = j + 1$,
$Weigh\&Update(B, \varpi', seed, role) \rightarrow hash'$;
return $hash', \pi, j$;
func $VRF_s(sk, seed, role, \tau_s)$:
$H_{sk}(seed, role).R \rightarrow \pi, hash, p$;
if $p < p_s$,*choose k as* N_s;
when $\ni B(k'; \varpi', p_s) = k$ *do* $j = j + 1$,
$Weigh\&Update(B, \varpi', seed, role) \rightarrow hash'$;
return $hash', \pi, j$;

Each round has reached a partial consensus. After at least three rounds, they can write Into the block and broadcast to the remaining nodes when more than two thirds nodes reach a consensus in the network. In a large scale, this consensus with VRF(details in Algorithm1) are more scalable than BFT and PoW. In a small scale, Algorand is more random and democratic than that like PoS. Similarly, David *et al.* [73] proposed an adaptive consensus algorithm based on encrypted lottery. Reference [74] proposed a new consensus mechanism PoP that avoid defects of PoS and PoW, which can identify physical entities based on IP and prevent recentralizing. But PoP requires a decentralized organization to verify the identity. In addition to Algorand, other hybrid consensus algorithms are used for public chain to design tiers, such as PoW joint with BFT used by Nervos, in order to ensure TPS that can meet the financial processing level and preserve decentralization characteristics. The protocol Algorand is firstly described in detail in the form of algorithms show in Algorithm 1 and 2.

C. PAYMENT CHANNEL

Lightning Network and Duplex are plans for Bitcoin to expand transaction scale and decrease consensus delay [75]. The key technologies of Lightning Network are sequence expiration revocation and hash time locking.

The protocol sequence expiration revocation firstly requires transaction parties to use their hash address to spend some token fund on the deposit pool. After contract vertification, outputs are directed to their respective address according to the proportion of tokens paid. The total amount of the deposit pool is broadcasted on parent chain. When

Algorithm 2 Improved Algorithm Based on Algorand

func BinaryBA(B_i):
1.*broadcast* v_i;
2.*wait for* λ;
3.*if number*$(v_i) > 2t$,
stop and broadcast $(v_i, sig(sk, seed))$,
4.*else return* 2;
5.*when* $n > 60$, *return default*,
func GC(N_i):
1.*init* v_i',*boolean*;
2.*broadcast* v_i';
3.*if boolean*,*return* 5;*else wait for* λ,
4.*if number*$(x \in all) > 2t$,*broadcast* x,
boolean $=$ *true*,*else return* 3;
5.*comment*() :*if number*$(x) > 2t$,
return $v_i = 0, g_i = 2$;
else if number$(x) > t$, *return* $v_i = 1, g_i = 1$;
else return default $= 0, g_i = 1$;
func BA $*$ $(seed_i)$:
1.$VRF_v(H(seed_{i-1}, i), role, \tau_v) \rightarrow N_v$;
2.$VRF_s(H(seed_{i-1}, i), role, \tau_s) \rightarrow N_s$;
3.*findLeader*$(N_s, p_s) \rightarrow L_i$;
4.$GC(L_i) \rightarrow getB_i(v_i, g_i)$;
5.*when BinaryBA*$(v_i, sig(sk, seed))$
$\rightarrow$ *result* $= 0, 1$,
6.*if number*$(result = 0||1) = number(N_s)$,
Verify$(Block_i) \rightarrow$ *boolean*, 7.*if boolean*, *broadcast* $Block_i.ok()||Block_i.null()$ *return* 1, *else return* $Block_{bad}$,

the amount of payment required for both parties do not exceed the total amount of the pool, it only need to change the allocation plan of the fund pool and invalidate the old scheme. The distribution plan will not be announced on blockchain or retrieve their funds until the final agreement reached between the two parties. As long as one of the validation result is incorrect, the request for legal validation of the contracts can be submitted during specified time according to the preconditions in the contracts. If illegal contracts are discovered, the funds held by the fraud party in the pool can be automatically paid as compensation to the other parties.

Based on the sequence expiration revocable agreement, the protocol hash time locking can establish the micropayment channel [63]. With time restriction and compulsory trading, it is guaranteed that parties to the transaction cannot break it privately after the contract is signed. Based on the ''six degrees theory'', it can eventually be expanded into a massive payment network. Once the payment network lives up to a big scale, users can find nodes with a large number of channels for connecting to others. Since data is not required to be thoroughly wound up unless the final liquidation, the transactions in lightning network are completed in real time.With the maturity of lightning network, a large number of transactions can be completed outside blockchain, alleviating the pressure of system [70].

However, in lightning network solution, establishment of the network for offchain and routing protocol still exist major deficiencies. Miller Andrew proposed a new type of lightning network protocol [76] to further optimize and upgrade the lightning network for performance in network setup and routing. A public chain was designed to avoid side-chain micropayments on Bitcoin to avoid affecting the ecosystem and support full-duplex channels, reaching 2480 TPS [77]. Block expansion and lightning network are strongly supported by bitcoin core developers in the roadmap.

D. TIERS

As mentioned in above consensus algorithm, the fragmentation mechanism divides the whole network into different partition so that each set runs the consensus protocol independently and completes the transaction confirmation in parallel. Differ from the traditional blockchain consensus mechanism, the challenges of the fragmentation mechanism are 1% attack and how to ensure that the attacker can not achieve the double-flower attack in the process of fragment transactions while the original system fault tolerance keeps invariant. The attacker was unable to achieve 51% attack in any of the shards during the sharding [78].

Random algorithm: The effective defense against 1% attack is that in the process of fragmentation. Nodes participating in the consensus need to be randomly assigned to different fragments so that the probability of 51% attack in the fragment can be neglected when the fragment size is large enough. The random algorithms currently used in blockchain fragmentation mechanism are mainly based on two categories include workload and stake, both of which are pseudo random process. PoW were used as random algorithms for fragmentation in Nervos schemes. The above scheme adopts the PBFT algorithm when consensus is made on chip. The security assumption of the PBFT algorithm is based on the conditions that less than one third nodes participates in the consensus. In order to defend against the sybil attack, the nodes need to perform a simple workload proof at the beginning of the consensus to obtain the identity of PBFT consensus. The criteria for dividing nodes into different sets are based on PoW. It is feasible to obtain a slice size of 600 by establishing a probability model. Even if the attackers account one third of the mining power, the possibility of controlling a slice is 2^{-20}. The specific process can be abstracted as follows: 1) The nodes perform PoW to obtain the identity and be divided into different sets; 2) PBFT algorithm is used for each fragment to carry out the transaction consensus within the slice; 3) Consensus after fragmentation. The signature of the transactions set and consensus process can be broadcasted to a certain slice and verified. The intra slice consensus is carried out and then packaged into blocks before broadcasted in the whole network [79].

Multi channel solution: From the perspective of resource balance, the sharding technology for Ethereum can be used to divide the entire blockchain network into multiple fragments with the same size. Besides, the channel technology for Fabric

can be used to divide the entire blockchain network into multiple fragments based on transaction rules. A logical channel, each node chooses to join the corresponding channel according to the transaction that it needs to participate in. Each node can receive and process blocks simultaneously on multiple chains, and transactions on multiple chains can be executed independently and concurrently. Compared to the original single-chain structure, the overall network throughput can be significantly improved. The ordering service node provides a plug-in consensus service. Each transaction on chain can be uniformly ordered by Kafka messaging system or consensus SBFT. When it consists of a trusted party or a regulatory agency, it does not involve the transaction privacy disclosure. However, if you do not desire the ordering service node to know the transaction specific content. In Bitcoin and Ethereum based on the PoW consensus mechanism, nodes are free to join or exit at any time. The PBFT algorithm used by Hyperledger Fabric requires that all nodes be known and statically unchanged, which is not conducive to the dynamic expansion of the blockchain network. To solve this problem, Fabric is divided into a consensus node and a billing node, decoupling the consensus service and billing service, thereby realizing the dynamic joining or exiting of the billing node.

E. CROSS CHAIN TECHNOLOGY

Cross chain technology includes sidechain [80] and children chain which can increase scale but do not mean scalability. Sidechain is not better than increasing block size in terms of scalability. Sidechain allows us to test and build network that can load more applications with high concurrency in the future. The main technologies for implementing cross chain include public notary, relay, hash based locking and distributed key control. Among them, the notary public technology need a trusted third party. As an asset custodian in cross chain, the multi signature scripts in blockchain can realize the bidirectional exchange for data between one chain and another. Relay realize the trustworthy communication between different blockchains. Scripts based hash are used to achieve fair cross chain asset exchange. Taking BTC Relay as an example, BTC Relay stores the headers in Bitcoin by the smart contract in Ethereum so that the events in Bitcoin can be learned in Ethereum. In this model, Ethereum is realized as a sidechain for Bitcoin.

Function using bitcoin block header data is equivalent to creating a simple bitcoin blockchain in Ethereum. But its decentralization is insufficient because the block header information of Bitcoin in Ethereum smart contract is provided by centralized node [81]. Distributed key control utilizes the distributed key generation algorithm so that asset custodian in the cross-chain process is borne by the whole network nodes, rather than a few third parties. It ensures security that the asset lock or unlock in cross chain process is supported by the system. Only cross chain support bidirectional information interaction. It requires the latest status of the chain from another chain such as relay and distributed key. Most of them use mature SPV technology to make use of block headers in different chains to construct the miniature target chain. However, when a large number of chains need to interact, the added overhead can inevitably affect the transaction per second of the system. In current cross chain technology, in addition to some supporting hash based locking schemes, the remaining schemes introduce third parties for security and efficiency considerations such as the provider of block headers in SPV certification.

VI. CONCLUSIONS AND FUTURE WORK

Improved blockchain has great prospects in the fields of finance, supply chain, group collaboration, and strong distributed storage. Rely on this technology, folks can significantly improve the efficiency of business processing, decrease labor costs and shorten settlement period without any third parties. However, not only its scalability bottlenecks but also technical standardization issues, the level of present blockchain can not exert its potentiality in traditional manufacturing. The rigid operation mode between enterprises should be broken as soon as possible.

We analyzed the progress of consensus algorithm, chain interoperability and technology realization in the aspect of existence, status and value base on practical applications. Before realizing DVES which could represent a new tendency, so many decentralized applications can bring much positive thinking to corporate development and social governance even if some of them are still imperfect. We propose the analysis of VES for existing uses of blockchains and appeal to perfect the laws and regulations concerned. To card these problems, our future work will investigate more solutions to improve the scalability and security of blockchain from the perspective of underlying.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] A. Thomson, T. Diamond, S.-C. Weng, K. Ren, P. Shao, and D. J. Abadi, "Calvin: Fast distributed transactions for partitioned database systems," in *Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD)*, New York, NY, USA, 2012, pp. 1–12, doi: 10.1145/2213836.2213838.

[3] P. Bailis, A. Fekete, M. J. Franklin, A. Ghodsi, J. M. Hellerstein, and I. Stoica, "Coordination avoidance in database systems," *Proc. VLDB Endowment*, vol. 8, no. 3, pp. 185–196, Nov. 2014. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2735508.2735509

[4] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982, [Online]. Available: http://portal.acm.org/citation.cfm?id=357176

[5] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 906–917. [Online]. Available: http://dl.acm.org/citation.cfm?id=2382292

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[7] J. Garay, A. Kiayias, and N. Leonardos, *The Bitcoin Backbone Protocol: Analysis and Applications*. Berlin, Germany: Springer, 2015. [Online]. Available: http://www.researchgate.net/publication/312829899_The_Bitcoin_Backbone_Protocol_Analysis_and_Applications

[8] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 1085–1100, doi: 10.1145/3035918.3064033.

[9] T. Tuan, A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[10] Q. Lin, P. Chang, G. Chen, B. C. Ooi, K.-L. Tan, and Z. Wang, "Towards a non-2 pc transaction management in distributed database systems," in *Proc. Int. Conf. Manage. Data (SIGMOD)*, New York, NY, USA, 2016, pp. 1659–1674, doi: 10.1145/2882903.2882923.

[11] S. Cohen and A. Zohar, "Database perspectives on blockchains," *CoRR*, vol. abs/1803.06015, 2018.

[12] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," *Future Generation Comput. Syst.*, vol. 90, pp. 105–117, Jan. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18308732

[13] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future," *Acta Automatica Sinica*, 2016.

[14] W. Cai, L. Yu, R. Wang, N. Liu, and E. Deng, "Blockchain application development techniques," *J. Softw.*, vol. 28, no. 6, pp. 1474–1487, 2017. [Online]. Available: http://www.cqvip.com/QK/96857X/201706/672421345.html

[15] Q. Shao, C. Jin, Z. Zhang, W. Qian, and A. Zhou, "Blockchain: Architecture and research progress," *Chin. J. Comput.*, vol. 41, no. 5, pp. 969–988, 2018. [Online]. Available: http://www.cnki.com.cn/Article/CJFDTotal-JSJX201805001.htm

[16] Q. Yao, "Experimental study on prototype system of central bank digital currency," *J. Softw.*, vol. 29, no. 9, pp. 2716–2732, Jun. 2018. [Online]. Available: http://www.jos.org.cn/1000-9825/5595.htm

[17] M. Divya and N. B. Biradar, "IOTA-next generation block chain," *Int. J. Eng. Comput.*, vol. 7, no. 4, pp. 23823–23826, 2018, doi: 10.18535/ijecs/v7i4.05.

[18] A. Singh, T.-W. Ngan, P. Druschel, and D. S. Wallach, "Eclipse attacks on overlay networks: Threats and defenses," in *Proc. INFOCOM IEEE Int. Conf. Comput. Commun.*, Apr. 2006, pp. 1–12. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4146884

[19] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.*, 2002, pp. 251–260. [Online]. Available: http://link.springer.com/chapter/10.1007%2F3-540-45748-8_24

[20] L. Zhu, F. Gao, M. Shen, Y. Li, B. Zhen, L. Mao, "Survey on privacy preserving techniques for blockchain technology," *J. Comput. Res. Develop.*, vol. 54, no. 10, pp. 2170–2186, 2017.

[21] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, 1999, pp. 173–186. [Online]. Available: http://dl.acm.org/citation.cfm?id=296824

[22] L. Alcock and L. Ren, "A note on the security of Equihash," in *Proc. Cloud Comput. Secur. Workshop (CCSW)*, New York, NY, USA, 2017, pp. 51–55, doi: 10.1145/3140649.3140652.

[23] A. Biryukov and D. Khovratovich, "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," *Ledger*, vol. 2, pp. 1–30, Apr. 2017.

[24] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, K. Wehrle, "Secure and anonymous decentralized Bitcoin mixing," *Future Gener. Comput. Syst.*, vol. 80, pp. 448–466, Mar. 2016.

[25] Z. Zhou, L. Li, S. Guo, and Z. Hui, "Biometric and password two-factor cross domain authentication scheme based on blockchain technology," *J. Comput. Appl.*, vol. 38, no. 6, pp. 1620–1627, 2018. [Online]. Available: http://www.wanfangdata.com.cn/details/detail.do?_type=perio&id=jsjyy201806015

[26] K. Zhao and Y. Xing, "Security survey of Internet of Things driven by block chain technology," *Netinfo Secur.*, 2017.

[27] G. Yonglin and C. Xiaorong, "Research and analysis of selfish mining for blockchain," *Comput. Eng. Appl.*, 2018.

[28] S. Micali. (2016). *ALGORAND: The Efficient and Democratic Ledger*. [Online]. Available: http://arxiv.org/abs/1607.01341v5

[29] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. Symp.*, 2017, pp. 51–68. [Online]. Available: http://www.researchgate.net/publication/320362651_Algorand_Scaling_Byzantine_Agreements_for_Cryptocurrencies

[30] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Proc. Cryptol. Conf.*, 2014, pp. 421–439. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-662-44381-1_24

[31] Q. Xia, F. J. Zhang, and C. Zuo, "Review for consensus mechanism of cryptocurrency system," *Comput. Syst., Appl.*, 2017.

[32] Y. Zhang and X. Li, "The research and implementation of an improved blockchain's consensus mechanism," *Electron. Des. Eng.*, vol. 26, no. 1, pp. 38–42, 2018. [Online]. Available: http://www.cqvip.com/QK/98233A/201801/674231341.html

[33] P. Mancarella, "MES (multi-energy systems): An overview of concepts and evaluation models," *Energy*, vol. 65, no. 2, pp. 1–17, 2014.

[34] J.-L. Deng, F.-Y. Wang, Y.-B. Chen, and X.-Y. Zhao, "From industries 4.0 to energy 5.0: Concept and framework of intelligent energy systems," *Acta Automatica Sinica*, vol. 41, no. 12, pp. 2003–2016, 2015. [Online]. Available: http://www.aas.net.cn/EN/abstract/article_18774, doi: 10.16383/j.aas.2015.c150259.

[35] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn microgrid," *Appl. Energy*, vol. 210, pp. 870–880, Jan. 2017.

[36] J. Zhang *et al.*, "Chinese blockchain based intelligent distributed electrical energy systems: Needs, concepts, approaches and vision," *Chin. Zidonghua Xuebao/Acta Automatica Sinica*, vol. 43, no. 9, pp. 1544–1554, 2017, doi: 10.16383/j.aas.2017.c160744.

[37] C. Gao, Y. Ji, J. Wang, and X. Sai, "Application of blockchain technology in peer-to-peer transaction of photovoltaic power generation," in *Proc. 2nd IMCEC*, May 2018, pp. 2289–2293.

[38] B. Li *et al.*, "Transaction system and key technologies of multi-energy system based on heterogeneous blockchain," *Autom. Elect. Power Syst.*, no. 4, pp. 183–193, 2018. [Online]. Available: http://www.wanfangdata.com.cn/details/detail.do?_type=perio&id=dlxtzdh201804024

[39] G. S. Aujla, N. Kumar, M. Singh, and A. Y. Zomaya, "Energy trading with dynamic pricing for electric vehicles in a smart city environment," *J. Parallel Distrib. Comput.*, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731518304416, doi: 10.1016/j.jpdc.2018.06.010.

[40] N. Xiaojing *et al.*, "Energy blockchain system based on integrated physical-cyber-value perspectives," *Power Syst. Technol.*, 2018.

[41] J. Chen, Y. Huang, and B. Lu, "Research on 'stations-pipelines' layout and optimization of regional energy Internet," *Proc. CSEE*, vol. 38, no. 3, pp. 675–684, Feb. 2018.

[42] H. Tian, J. He, and L. Fu, "A privacy preserving fair contract signing protocol based on block chains," *J. Cryptologic Reseatch*, vol. 4, no. 2, pp. 187–198, 2017. [Online]. Available: http://d.wanfangdata.com.cn/Periodical/mmxb201702009

[43] R. An, D. He, Y. Zhang, and L. Li, "Design and implementation of anti-counterfeiting system based on block chain technology," *Mod. Inf. Technol.*, vol. 4, no. 2, pp. 199–208, 2017. [Online]. Available: http://d.wanfangdata.com.cn/Periodical/mmxb201702010

[44] R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. Internet Technol. Secured Trans.*, 2016, pp. 131–138. [Online]. Available: http://ieeexplore.ieee.org/document/7412073/

[45] L. I. Qi *et al.*, "Model and platform of charity application based on block chain technology," *J. Comput. Appl.*, 2017.

[46] H.-B. Fan, H.-C. Xie, and J. Zhang, "A trusted electronic voting method based on block chain technology," *Softw. Guide*, 2018.

[47] G. Zhu and W. Zhang, "A decentralized domain name system for the network," *Inf. Secur. Technol.*, vol. 8, no. 1, pp. 14–18, 2017. [Online]. Available: http://d.wanfangdata.com.cn/Periodical/xxaqyjs201701004

[48] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, May 2018.

[49] J. Benet. (2014). "IPFS—Content addressed, versioned, P2P file system." [Online]. Available: https://arxiv.org/abs/1407.3561 and http://www.oalib.com/paper/4065640

[50] X. Dong *et al.*, "An efficient and secure decentralizing data sharing model," *Chin. J. Comput.*, vol. 41, no. 425, no. 5, pp. 55–70, 2018.

[51] S. Matthew and E. Nezhadian, "Conditions of full disclosure: The blockchain remuneration model," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Apr. 2017, pp. 64–67. [Online]. Available: http://ieeexplore.ieee.org/document/7966972/

[52] S. Jundian, "Data governance collaborative method based on blockchain," *J. Comput. Appl.*, vol. 38, no. 9, pp. 2500–2506, 2018.

[53] J. Robert, S. Kubler, N. Kolbe, A. Cerioni, E. Gastaud, and K. Främling, "Open IoT ecosystem for enhanced interoperability in smart cities-example of métropole de Lyon," *Sensors*, vol. 17, no. 12, p. 2849, 2017. [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5751623/

[54] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, 2018.
[55] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[56] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 86, pp. 641–649, Sep. 2018.
[57] S. Meiklejohn *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names," in *Proc. Conf. Internet Meas.*, 2013, pp. 127–140. [Online]. Available: http://dl.acm.org/citation.cfm?id=2504747
[58] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using P2p network traffic," in *Financial Cryptography and Data Security*, vol. 8437, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2014, pp. 469–485. [Online]. Available: http://link.springer.com/10.1007/978-3-662-45472-5_30
[59] N. Zhang and S. Zhong, "Mechanism of personal privacy protection based on blockchain," *J. Comput. Appl.*, vol. 37, no. 10, pp. 2787–2793, 2017. [Online]. Available: http://d.wanfangdata.com.cn/Periodical/jsjyy201710009
[60] C. Tang and L. Gao, "Multi-parties key agreement protocol in block chain," *Netinfo Secur.*, 2017.
[61] A. Gervais, G. O. Karame, 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.*, 2016, pp. 3–16. [Online]. Available: http://dl.acm.org/citation.cfm?id=2976749.2978341
[62] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Gener. Comput. Syst.*, 2017.
[63] S. Agrawal, C. Ganesh, and P. Mohassel, "Non-interactive zero-knowledge proofs for composite statements," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2018.
[64] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. Secur. Privacy*, 2016, pp. 839–858. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/SP.2016.55
[65] M. Green and I. Miers, "Bolt: Anonymous payment channels for decentralized currencies," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 473–489. [Online]. Available: http://dl.acm.org/citation.cfm?id=3134093
[66] Y. Velner, J. Teutsch, and L. Luu, "Smart contracts make bitcoin mining pools vulnerable," in *Proc. Financial Cryptogr. Workshops*, vol. 10323, Nov. 2017, pp. 298–316. [Online]. Available: https://dblp.uni-trier.de/search?q=Smart%20Contracts%20Make%20Bitcoin%20Mining%20Pools%20Vulnerable
[67] B. Huang, Q. Liu, Q. He, Z. Liu, and J. Chen, "Towards automatic smart-contract codes classification by means of word embedding model and transaction information," *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1532–1543, 2017. [Online]. Available: http://www.cnki.com.cn/Article/CJFDTotal-MOTO201709005.htm
[68] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town Crier: An Authenticated Data Feed for Smart Contracts," in *Proc. 23rd ACM Conf. Comput. Commun.*, Feb. 2016, pp. 270–282. [Online]. Available: http://xueshu.baidu.com/s?wd=Town+Crier%3A+An+Authenticated+Data+Feed+for+Smart+Contracts&tn=SE_baiduxueshu_c1gjeupa&cl=3&ie=utf-8&bs=Revive%3A+Rebalancing+Off-Blockchain+Payment+Networks&f=8&rsv_bp=1&rsv_sug2=0&sc_f_para=sc_tasktype%3D%7BfirstSimpleSearch%7D&rsv_n=2
[69] C. Pan and Z. Liu, "Research on scalability of blockchain technology: Problems and methods," *Comput. Res. Develop.*, vol. 55, no. 10, pp. 2099–2110, 2018. [Online]. Available: http://crad.ict.ac.cn/CN/abstract/abstract3781.shtml
[70] Z. Zhang, H. Yu, and J. Liu, "Research on scaling technology of bitcoin blockchain," *Comput. Res. Develop.*, vol. 54, no. 10, pp. 2390–2403, 2017. [Online]. Available: http://crad.ict.ac.cn/CN/abstract/abstract3555.shtml
[71] I. Eyal, A. E. Gencer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. Usenix Conf. Netw. Syst. Des. Implement.*, 2016, pp. 45–59. [Online]. Available: http://dl.acm.org/citation.cfm?id=2930615
[72] L. Eckey, S. Faust, and J. Loss, "Efficient algorithms for broadcast and consensus based on proofs of work," Cryptol. ePrint Arch., Tech. Rep. 2017/915, 2017.
[73] B. M. David *et al.* "Ouroboros Praos: An adaptivelysecure, semi-synchronous proof-of-stake protocol," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 573, 2017.
[74] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Apr. 2017, pp. 23–26. [Online]. Available: http://ieeexplore.ieee.org/document/7966966/
[75] J. Poon and T. Dryja. (Jan. 2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. [Online]. Available: https://lightning.network/lightning-network-paper.pdf
[76] R. O'Connor and M. Piekarska, "Enhancing bitcoin transactions with covenants," in *Financial Cryptography Data Security* (Lecture Notes in Computer Science), M. Brenner *et al.* Eds. Cham, Switzerland: Springer, 2017, pp. 191–198.
[77] J. Lind, I. Eyal, P. Pietzuch, and E. G. Sirer, "Teechan: Payment Channels Using Trusted Execution Environments," *Cryptogr. Secur.*, 2016.
[78] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 507–527. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-662-47854-7_32
[79] C. Lin, N. Ma, X. Wang, Z. Liu, J. Chen, and S. Ji. (Aug. 2018). "Rapido: A layer2 payment system for decentralized currencies." [Online]. Available: http://arxiv.org/abs/1808.01561
[80] A. Back *et al.* (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains
[81] A. Hope-Bailie and S. Thomas, "Interledger: Creating a standard for payments," in *Proc. Int. Conf. Companion World Wide Web*, 2016, pp. 281–282. [Online]. Available: http://dl.acm.org/citation.cfm?id=2889307

FEI LIN was born in 1977. She graduated from the CAD Institute, Hangzhou University. She is involved in information system research and development for a long time. She has a wealth of experience in project management, software research and development, and product planning. In recent years, she presided over and participated in projects, including that of the National Natural Science Foundation of the State, the Provincial Natural Science Foundation, the Provincial Public Welfare Projects, twice, and in various types of enterprise customization system. She has five published teaching materials, including that of a provincial key teaching materials' department. She published nearly 30 papers. She received the School Teaching Achievement Award, many times, the school-grade Sage Rookie, the Teaching Excellence Award, the Teaching Outstanding Award, and the Outstanding Graduation Design Guidance Teacher.

MINQIAN QIANG was born in 1994. He received the bachelor's degree in engineering from Suzhou University, in 2017. He is currently pursuing the degree in computer technology with Hangzhou University. He holds two invention patents and one software copyright. His research interests include distributed system and cryptography technology.