Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 4641559, 12 pages
https://doi.org/10.1155/2022/4641559

Research Article

Application of Blockchain Technology in Intellectual Property Protection

Liya Luo

Shanxi Vocational University of Engineering Science and Technology, Jinzhong 030619, China

Correspondence should be addressed to Liya Luo; luoliya@sxgkd.edu.cn

Received 14 April 2022; Revised 1 May 2022; Accepted 10 May 2022; Published 8 June 2022

Academic Editor: Vijay Kumar

The emergence of digital copyright in the internet era altered the traditional method of information dissemination and triggered a new copyright revolution, which benefited copyright owners by increasing revenue. However, as a result of the efficiency and convenience of technical capture, the data-based form of copyright faces new challenges and the emergence of a large number of infringement acts has become a barrier to the development of the digital copyright industry. Blockchain technology is decentralized, impenetrable, timestamped, traceable, and capable of smart contracts, among other characteristics. It was initially applied in the financial sector before being expanded to other sectors, resulting in a variety of blockchain + X models. The application of blockchain technology to digital copyright protection represents an attempt to protect copyright owners' rights through the use of a novel technical method and protection concept, and it has a bright future. This study analyzes the current state of digital copyright protection in detail, discusses the benefits of applying blockchain technology in three areas: digital copyright registration and confirmation, transaction monitoring, and evidence maintenance, as well as the potential difficulties associated with the application of blockchain technology, and finally considers and proposes the system design for blockchain technology in the application of digital copyright protection. The study discovered that by utilizing blockchain technology to establish a unified blockchain digital copyright protection platform, it is possible to completely and efficiently record the entire process of copyright registration and confirmation, monitor data capture infringement, provide objective electronic evidence, reduce the cost of copyright owner rights protection, and increase the success rate of judicial remedies.

1. Introduction

With the rapid advancement of the digital information era, the traditional way of life is also rapidly changing, and online entertainment options such as e-reading, digital music, and online video are consuming an increasing amount of people's time. Along with the major industry components such as online news media, online games, and online videos, the online literature industry is steadily growing, with the market value of online literature reaching 20.17 billion yuan in 2019 and the cumulative volume of online written works exceeding 25 million. The number of online writers has increased to 19.36 million, while Chinese online literature users have surpassed 450 million. Companies in the traditional publishing industry have gradually transformed in response to the trend toward networked and digitalized copyright publishing. However, the characteristics of digital information, such as its easiness of capture, easiness of copying, and rapid dissemination, make infringement easier and more obvious. For copyright in the digital field, the high costs, strict procedures, time-consuming difficulties related to registration and confirmation of rights, the difficulties faced by individual authors of digital information in dealing with infringement, the high cost of forensics, the insufficient coverage of forensics, and the inability to detect and suppress violations have contributed to the proliferation of violations. Additionally, the high cost of manual infringement monitoring, the low cost of infringement by infringers, and the imperfection of digital copyright protection laws all contribute to the difficulty of properly punishing infringement acts, thereby impairing the digital copyright industry's sustainable and healthy development. According to

incomplete statistics, piracy on posting bars, pirated novel sites, and pirated resource download sites have resulted in at least tens of billions of dollars in losses for creators.

The traditional digital copyright protection system and technical means can hardly follow the pace of development of the times, and the emerging blockchain technology has brought new opportunities for digital copyright protection. Through distributed storage mode and peer-to-peer chain transmission technology, the data are guaranteed to be objectively immutable and traceable, thus realizing the early prevention of digital copyright infringement, while truly clarifying the attribution of digital copyright and preserving the evidence, which provides technical and legal support for the right holder's following this report that provides technical assistance and court proof for the right holder's later rights defense.

Thus, after introducing the current state of digital copyright protection, the purpose of this study is to focus on the benefits and applications of existing blockchain technology in the field of digital copyright protection, to investigate the significance of this technology for digital copyright protection, and to propose solutions to the problems associated with a lack of policies, lagging laws, and concepts in the process of applying blockchain technology in the financial sector. The implementation of blockchain technology in the sphere of digital copyright protection raises issues such as a lack of regulations, lagging legislation, and outdated concepts, and recommendations are made from the perspective of top-level system design, update and application of the law, enhancement of legal awareness, and platform construction.

2. Related Work

2.1. Digital Copyright Protection. As a hot topic of research in recent years, scholars in related fields at home and abroad have paid much attention to the application of blockchain technology combined with digital copyright protection and have made various research studies.

Through the interpretation of smart contracts, Nakamoto [1] proposed the application methods of blockchain technology in copyright confirmation, proof of prior use of trademark rights, and logistics tracking to prevent counterfeit goods, and discussed and suggested the legal regulation of smart contracts; Butertin and Around [2] analyzed the challenges encountered by the traditional digital copyright protection system, including the weakening of the value base of works, the proliferation of infringement, the obvious disadvantages of registration, the difficulty of rights maintenance, and the weak awareness of copyright from the characteristics of the technology. From the perspective of the characteristics of blockchain, they explain that the technology brings opportunities for digital copyright to reduce costs, solve the difficulties of registration and proof, and cope with transaction needs, while pointing out that there are problems in the application of the technology itself, industry standards, and the double-edged effect, etc.; Cachin [3], from the perspective of the current situation of medical journal infringement and statistics, illustrates the copyright infringement situation of medical journals. The differences between traditional digital copyright protection technology and blockchain technology are compared, and the advantages of the block liberal technology and the feasibility and prospect of applying blockchain technology to digital copyright protection of medical journals are analyzed; from the standpoint of blockchain technology, Brown et al. [4] build a digital copyright governance system, introduce the application of the technology in the field of digital copyright from the current situation of digital copyright industry, and propose that it should be fully applied in the fields of confirmation; Huang Long6 analyzed the encryption algorithm and smart contract principle of blockchain technology, proposed the copyright traceability, intelligent integration, and automated rights maintenance mechanism brought by the technology, and explained that the technology can dilute legal boundaries, integrate management systems, give rise to industrial ecology, and promote self-publishing forms, illustrating that the significant impact the technology will bring to the press and publishing industry; Corda envies [5] from the challenges encountered in the traditional online copyright protection environment, arguing that there are currently problems such as difficulty in determining the ownership of works, difficulty in obtaining evidence and limited ways, and difficulty in proving the amount of damages for infringement and proposing the new opportunities provided by blockchain technology, while also analyzing the possible problems and coping strategies in the process of technology application; McConaghy et al. explained [6] and introduced the application scenarios of block technology applied to the field of digital copyright protection. They also proposed suggestions for the sustainable development of the legal regulation of this technology in China, taking the existing platforms in the United States and Japan as examples; Yanchuan [7] introduced the logic and structure of smart contracts from the perspective of blockchain technology 2.0 smart contracts, explained the characteristics of their automatic execution, and analyzed the risks of smart contract structure and the solutions for risk prevention, and solutions for risk prevention and control; Tao [8] illustrates the problem of imbalance of interests among digital publishing stakeholders, analyzes the advantages of blockchain technology in protecting the interests of digital publishing stakeholders, and proposes practical strategies for using the technology; Yuan and Wang [9] analyze the problems in the digital copyright industry, propose blockchain digital copyright solutions, and also introduce the operation mode and solutions of existing blockchain technology digital copyright protection platforms by taking Baidu Totem, Copyright Home, and Paper Gui Technology as examples; He et al. [10] took an information network dissemination rights dispute case heard by Hangzhou Internet Court as an example, analyzed the existing blockchain rules of the Supreme Court and the blockchain electronic evidence by comparing the relevant experience of Vermont in the United States value, and proposed that strict rule restrictions should be set for the technology; Tschorsch and Scheuermann [11] argued that blockchain technology brings new application ideas to

digital copyright protection and has a wide range of prospects in the areas of confirmation, storage, transaction, and maintenance of rights, analyzed the advantages of the technology in the protection of personal rights and realization of property rights of digital copyright, while also arguing that the technology may affect freedom of publication, and proposed national-level and legal-level regulatory proposals.

See Gribble et al. [12] believe that the public chain under the technical application of blockchain has the problem of difficulty to confirm the legal subject, and the arbitrary access of users directly leads to the difficulty of regulation. The private chain-based alliance chain sets the access threshold and regulatory subject, which solves the contradiction between the regulatory subject and the decentralized one and reduces the cost of going on the chain. However, how to solve the relationship between platform provider, technical support provider, and on-chain users, and how to use the alliance chain to realize the advantages of the public chain are to be studied; Yu et al. [13] introduced Minelab, an American startup company focusing on blockchain technology development, which has developed Mediachain's system collaboration joint media metadata protocol to realize digital copyright by using blockchain technology and IPFS protocol to achieve digital copyright protection, mainly for the field of digital images, including the identification of newly uploaded images and encrypted signature of the creator of the work.

In summary, most domestic researchers analyze the feasibility of blockchain technology for resolving the problems associated with the current state of digital copyright protection, and the technical characteristics of blockchain technology offer unique advantages in corresponding to the construction of digital copyright authentication, transaction, deposit, maintenance, and management systems. However, it should be noted that the technology is not yet perfect, industry standards have not been established, and there is still considerable conflict with existing domestic laws. Additionally, while each enterprise has established its own blockchain-based digital copyright protection platform, there is a lack of unified regulation and information sharing. Foreign research on blockchain technology is primarily focused on specific applications, and the optimal path for blockchain technology application is analyzed through case studies. In practice, China's Supreme Court has solicited comments on draft electronic evidence rules, and various internet courts are also experimenting with electronic deposition and evidence collection, indicating that technology application is the general trend. As a result, the application of technology is required to provide the necessary theoretical foundation.

2.2. Blockchain Technology

2.2.1. Blockchain Technology Connotation. Blockchain technology includes distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm [14]. In layman's terms, blockchain is a kind of electronic bookkeeping model. In the traditional model, the electronic data changes of personal funds should be recorded by the banks of the country due to the arbitrary tampering of the personal record books, which is the so-called centralized institution, while in blockchain, due to its inherent characteristics, it is possible to make the bookkeeping of personal accounts possible anytime and anywhere. Blockchain has features such as tamper-evident, timestamp, and traceability possibility, and every change of data will be judged by the preset system and sent to all other devices involved in the network, so that each device gets the complete book of this process and can understand the change of data in real time, which solves the problem of trust between the two parties in the process of direct human-to-human transactions and even third parties in the process of direct human-to-human transactions. The data are objectively and unalterably recorded once recorded and are known to all, which allows subjects to exchange information and trade values with confidence even without the participation of an authoritative central authority guarantee.

2.2.2. Features of Blockchain Technology. Decentralization is the essential characteristic that distinguishes blockchain technology. For example, when registering and confirming copyright information, creators need to go to the local copyright office or copyright registration center institution and go through a series of processes such as submitting applications, preliminary examination by the institution, paying fees or supplementing information, re-examination by the institution, passing and publicizing or rejecting, issuing certificates, etc. The whole process requires the participation of a third-party institution, which greatly consumes time and expense costs. The two parties also need to verify the authenticity of the information when trading, or when one party to the transaction does not fulfill the contract or arbitrarily tampers with the transaction information, a third-party institution is also required to confirm, bind, and adjudicate. Therefore, the central institution plays an important role in trust provision and control in the whole process of information from making to flowing. The regional chain technology, however, enables information to be recorded in all data blocks in a distributed manner through peer-to-peer transmission, real-time information recording, dissemination, and shared consensus. Each participant participates in the recording, dissemination, or transaction confirmation of information, and each participant's data block records a complete copy of data changes, and the loss or damage of one block of data will not affect the integrity of other data blocks, which solves the trust problem that one party may arbitrarily change data during the recording and transaction process if there is no central institution involved. All the data information in the blockchain is open, transparent, and unchangeable, and any party who knows the block location and key can get the complete data information in the data block. It also realizes decentralization.

In blockchain technology, every change of data or generation of new data needs to be verified and confirmed and recorded by all participating data blocks, which means

that all participating data blocks have corresponding backups, that is to say, even if the data of a block are maliciously tampered with, such tampering, which is not due to information sharing or value trading, will not be confirmed and recorded by other data blocks. All other blocks still record the data before being maliciously tampered with, which makes malicious tampering by a single node meaningless and unrecognized. Even if theoretically more than 50% of the blocks are tampered with at the same time, in practice, the data blocks infinitely spread and new blocks are rapidly generated, which makes it almost impossible to control more than 50% of the blocks at the same time under the existing computer computing and storage conditions. Therefore, once the registration information and transaction information of digital copyright are recorded by blockchain, the authenticity of the recorded information can be presumed.

Blockchain faithfully records each new data generation and puts an indelible record of the time of each new data generation, just like a steel stamp. As new data keep increasing, each newly generated data block is linked to the previous data block by an encryption algorithm and passed to the next data block, and the new data of the latter data block are also confirmed and recorded by the previous one, which forms a nearly infinite blockchain with first and last links, and one timestamp also forms an uninterrupted continuous time record, and this record is distributed and recorded in all. This record is distributed in the data blocks of all participants so that all participants can trace the whole process of data changes. Each transaction record of the digital copyright information will be timestamped and recorded throughout the entire process. By querying the public blockchain or requesting the private key from the copyright owner to query the nonpublic blockchain at the time of transaction, the entire traceability of the information from creation to several transactions can be realized.

The term smart contract originated from cryptographer Nick Szabo, which means the organic combination of computer computing and contract, by setting the starting conditions of the computer computing code in advance; once the trigger occurs, the computer can automatically execute the contents of the contract. The most common form of this model is the vending machine, where the seller sets the price of each item in the vending machine in advance and sets that once the product is selected and the corresponding amount of currency is invested, then the vending machine will automatically ship the product, and if the corresponding amount is not reached, then the coins will be automatically refunded.

As a result, the copyright holder can upload his work to the blockchain platform at the start of its creation, and the decentralized nature of blockchain technology simplifies and reduces the cost and time associated with authentication. The timestamp feature is the first to capture the copyright owner's work information, ensuring the acquisition of rights; the untamperability feature also ensures the authenticity of the work information and evidence information when rights are infringed; the traceability feature records the entire transaction, ensuring the monitoring and recording of the process of the work information being captured when the right holder receives the infringement; The automatic execution of the smart contract ensures that the transaction is automatically completed, that the seller receives the digital information in real time after payment, without having to convince the buyer to execute it, and that no dispute arises as a result of differing interpretations of the terms. The smart contract's self-executing nature ensures that the transaction is automatically completed.

3. System Architecture

3.1. Scheduling Algorithm Constraints. From Bitcoin, which was the first to apply blockchain technology, to Ether, which was the first to introduce smart contracts in the blockchain, to Hyperledger Fabric, which is the most widely used alliance chain, they have many commonalities in the overall architecture, despite their different implementations. As shown in Figure 1, the overall blockchain platform can be divided into five layers: network layer, consensus layer, data layer, smart contract layer, and application layer.

3.1.1. Networks. In 2001, Antonopoulos [15] proposed combining P2P and database research. Early P2P databases lacked a global schema and were incapable of adapting to network changes for enterprise-level applications [16, 17]. The blockchain network has no central node, and each node can join or leave the network at any time. Each node in the blockchain network is equal, autonomous, and distributed, and each node has the ability to discover and broadcast new nodes, transactions, and blocks [18].

To ensure the validity of newly received transactions and blocks from neighbors, nodes in the blockchain network constantly monitor network security for data broadcasts, which includes digital signatures in transactions and workload confirmation in blocks. Only valid transactions and blocks are processed and forwarded in order to prevent the spread of invalid data.

3.1.2. Consensus Layer. To solve the distributed consistency problem, distributed databases primarily employ the Paxos [18] and Raft [19] algorithms. These databases are managed and maintained by a single organization, all nodes are trusted, and the algorithms must only support crash fault tolerance (CFT). Assuming that the network has no more than f untrustworthy nodes out of a total of n nodes, the Byzantine general problem can be solved in $n3f+1$ for a network with synchronous communication and reliability [19]. Fischer et al. [20] demonstrated that a deterministic consensus mechanism cannot tolerate any node failure in the case of asynchronous communication. Practical Byzantine fault tolerance (PBFT) was proposed by Castro and Liskov [21], which reduces the complexity of Byzantine protocols from an exponential to a polynomial level. Practical Byzantine fault tolerance (PBFT) was proposed by Castro and Liskov [21], which reduces the complexity of Byzantine protocols from an exponential to a polynomial level and enables the use of Byzantine protocols in

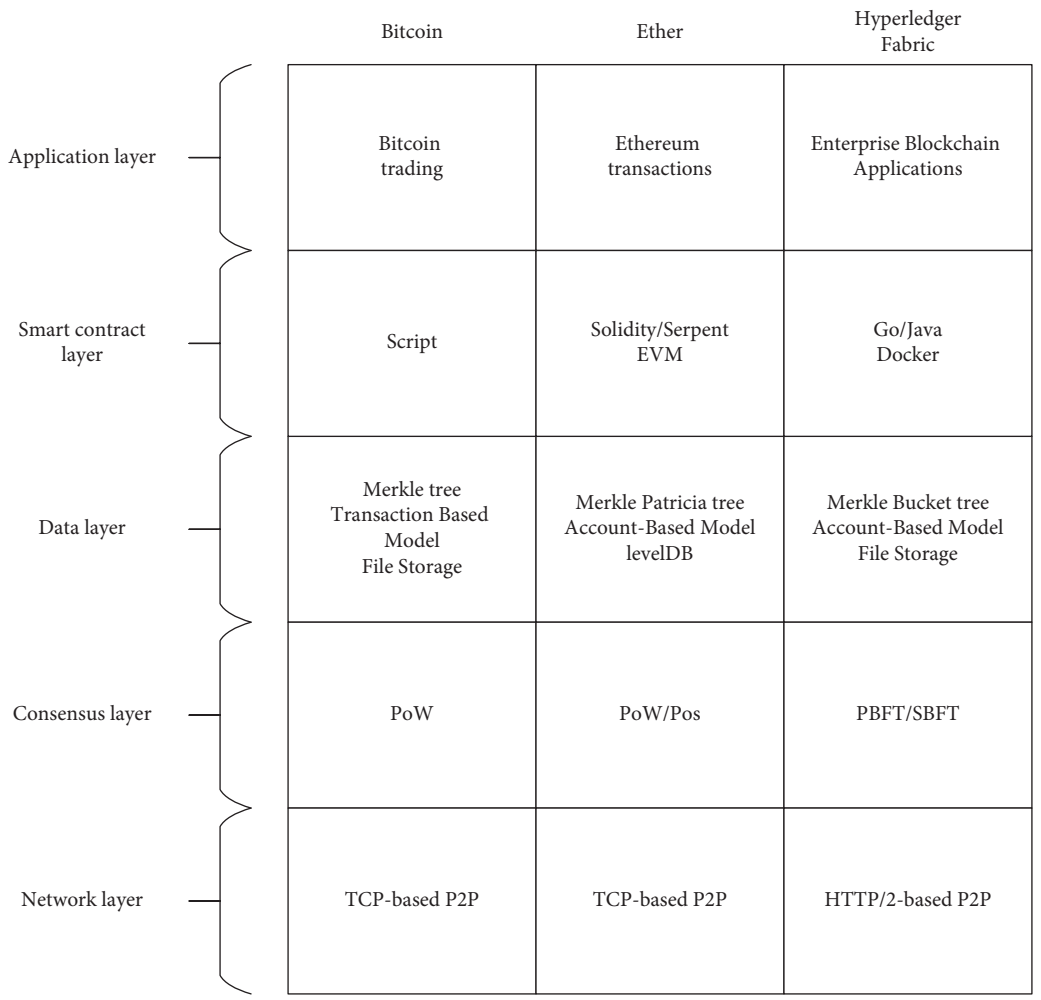

Figure 1: Blockchain architecture.

distributed systems. Kotla et al. [22] proposed Zyzzyva to improve the performance of PBFT by assuming that network nodes are in a normal state most of the time and do not need to agree on each request before executing it, but only when an error occurs. Tendermint, proposed by Kwon [23], assigns different weights to each vote based on node-by-node vote counting. Important node votes can be assigned higher weights, and the consensus is considered reached if the weight of the votes exceeds 2/3. In digital currency-based applications, the weights can also correspond to the number of coins held by users, achieving a proof-of-stake-like consensus mechanism. Cross fault tolerance (XFT) was proposed by Liu et al. [24], which implies that it is difficult for a malicious person to control the entire network and Byzantine nodes at the same time, simplifying the BFT message model. Furthermore, the industry has proposed the BFT enhancement algorithms such as scalable BFT [25], parallel BFT [26], optimistic BFT [27], and so on. The Ripple payment network proposes the Ripple protocol, which is based on a group of trusted authentication nodes. The Ripple payment network proposes the Ripple protocol consensus algorithm (RPCA), which is based on a set of trusted authentication nodes and can solve the Byzantine general problem with $n5f+1$ [28].

Bitcoin employs the proof-of-work (PoW) mechanism to address the issue of Sybil attacks [29]. PoW is based on the work of Dwork and Naor [30] to prevent spam, in which emails are accepted only after they have completed a certain amount of computational work and provided proof. Back Hashcash 1 was proposed as a proof-of-work algorithm based on hashes. Only nodes that have completed a certain amount of computational work and provided proofs are permitted to generate blocks, and each network node competes for block-keeping rights by performing hashing operations using its own computational resources; as long as the computational resources are controlled by trusted nodes across the network exceed 51%, the entire network can be proven to be secure [31]. BitShares employs the delegated proof-of-stake (DPoS) mechanism, in which representatives with the most shareholder votes take turns generating blocks over a specified time period [32]; BitShares employs the delegated proof-of-stake (DPoS) mechanism, in which representatives with the most shareholder votes take turns generating blocks over a specified time period [33]. Hyperledger Sawtooth utilizes the proof-of-elapsed time (PoET) mechanism, which is based on Intel SGX2 trusted hardware. Proof-based consensus is typically used on public chains with open nodes, such as Bitcoin and Ether.

The voting-based consensus mechanism is typically used in federated chains where nodes are authorized to join; Hyperledger Fabric employs the PBFT algorithm.

3.1.3. Data Layer. All three blockchain technologies have distinct features in terms of data structure, model, and storage. Based on document timestamps to prove the creation time of various electronic documents, the existing blockchain platform data structure draws on the work of Haber and Stornetta [34–36]. As a result, a timestamp-based certificate chain is formed, which reflects document creation order and cannot be tampered with. Haber and Stornetta also propose signing blocks of documents. The Merkle trees [37–39] are used to organize the documents within the blocks, as proposed by Haber and Stetta. The block body contains the bulk transaction data, while the block header contains the Merkle root, previous block hash, timestamp, and other data. The Merkle root provides tamper-evident and simple payment verification of the transaction data within the block; the preblock hash links the isolated blocks together to form a blockchain; and the timestamp indicates when the block was created.

With a transaction-based data model, each transaction has an input indicating the source and an output indicating the destination, with all transactions linked together by the input and output, making each transaction traceable. Networks and Hyperledger Fabric use an account-based model to support rich applications. A quick balance or status check [40] is feasible.

Unlike traditional databases, blockchain data are stored in log files, similar to prewritten logs. Since the system relies on hash-based key-value retrieval (e.g., transaction data retrieval based on hash and block data retrieval based on block hash), claim and status data are usually stored in key-value databases.

3.1.4. Smart Contracts. A smart contract is a digital protocol that creates contractual terms using algorithms and procedures. Szabo defined smart contracts as a set of digitally defined commitments, including the agreements required for their execution by the contracting parties. Due to early computing constraints, smart contracts received little research attention until blockchain technology emerged and redefined smart contracts. Smart contracts enable decentralized computation on top of the blockchain. Due to the limited functionality and single type of instructions, Bitcoin scripts can only be considered a prototype of smart contracts. Users can write and run smart contracts on Ethernet using the Turing-complete footprint languages Solidity 5 and Serpent 6 and the Ethereum virtual machine (EVM) [41] and the Docker container.

The Docker container comes with signed base-disk images, runtimes, and SDKs for Go and Java [42]. 2.5 The Bitcoin platform's application layer is based on Bitcoin transactions. It also supports decentralized applications (Dapps), in which are web front-end JavaScript applications that communicate with Ethereum smart contracts via JSON-RPC. It is for enterprise blockchain apps and does not support crypto. Smart contracts running on Hyperledger Fabric nodes can be accessed via gRPC or REST-based applications built on SDKs in Go, Java, Python, Node.js, etc.

3.2. Blockchain Data

3.2.1. Blockchain Data Structure. Immutability is achieved via a block-based chain structure. In principle, the data structure of any blockchain platform is similar. We consider Bitcoin: the block body holds recent transactions; the block header stores PrevBlockHash, nonce, Merkle Root, etc. Table 1 shows the structure.

The blockchain is based on two hash structures that guarantee the immutability of data, namely, the Merkle tree and the blockchain table, and Figure 2 depicts the blockchain data structure of Bitcoin.

(1) Merkle. Originally designed to digest digital certificate directories, Ralph Merkle's Merkle tree has undergone numerous enhancements since its inception. We concatenate the values of the two-child nodes and then hash them to obtain the value of the parent node; this process is repeated until the root hash is obtained.

Figure 3 shows the Merkle Patricia tree's extension, branch, and leaf nodes. It contains a common key prefix: a branch node that implements the tree's branch based on a single hexadecimal character key prefix and an Ether account state. The Merkle Patricia tree has limited depth, and the root value is independent of node update order. The decision tree is a multinomial tree with each leaf node representing a key-value state dataset. The Merkle Bucket tree's depth and width can be adjusted by changing the number of buckets and branches, allowing for performance and resource trade-offs.

(2) PrevBlockHash. To obtain the block hash, PrevBlockHash, nonce, and Merkle root are all SHA256 hashed in the block header. PrevBlockHash stores the hash of the previous block, and all subsequent blocks are linked in order of generation using PrevBlockHash as the hash pointer. To detect tampering, the block hash uses the Merkle root of the transaction, which is stored in the block header, along with the previous block hash PrevBlockHash. Due to the fact that all blocks rely on the previous block's hash pointer PrevBlockHash, any change to any block results in a chain change for all subsequent block hash pointers. When downloaded from an untrusted node, the block hash-based verification of whether each block has been modified is possible.

3.2.2. Data Model. Ethernet and Hyperledger Fabric are account-based, while Bitcoin is transaction-based.

(1) Model Transactional. Figure 4*Depicts a Bitcoin Transaction's Data Structure*. To transfer Bitcoins from one account to another, as shown in Table 2, a transaction can merge them. The previous transaction's hash PrevTxHash, output index Index, and input script ScriptSig are all inputs. Each transaction's output is a previous transaction's output.

Table 1: Bitcoin block header structure.

Field	Description	Size (bytes)
Version	Version of Bitcoin software	4
Previous block hash	Hash of the previous block	32
Merkle root	Calculated for all transactions in the block	32
Timestamp	Approximate time of generation	4
Difficulty target	Difficulty target for generating the block	4
Random number	The block header hash less than the difficulty target	4

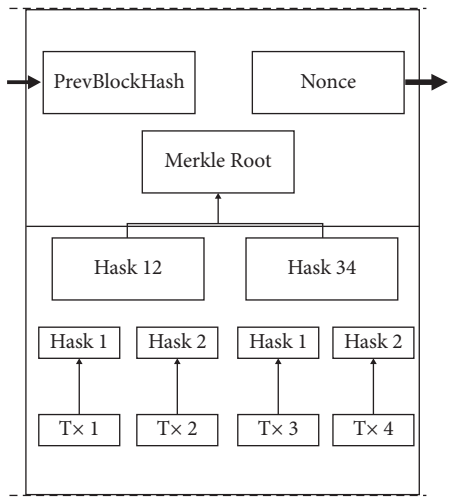

Figure 2: Two hash structures of the Bitcoin blockchain.

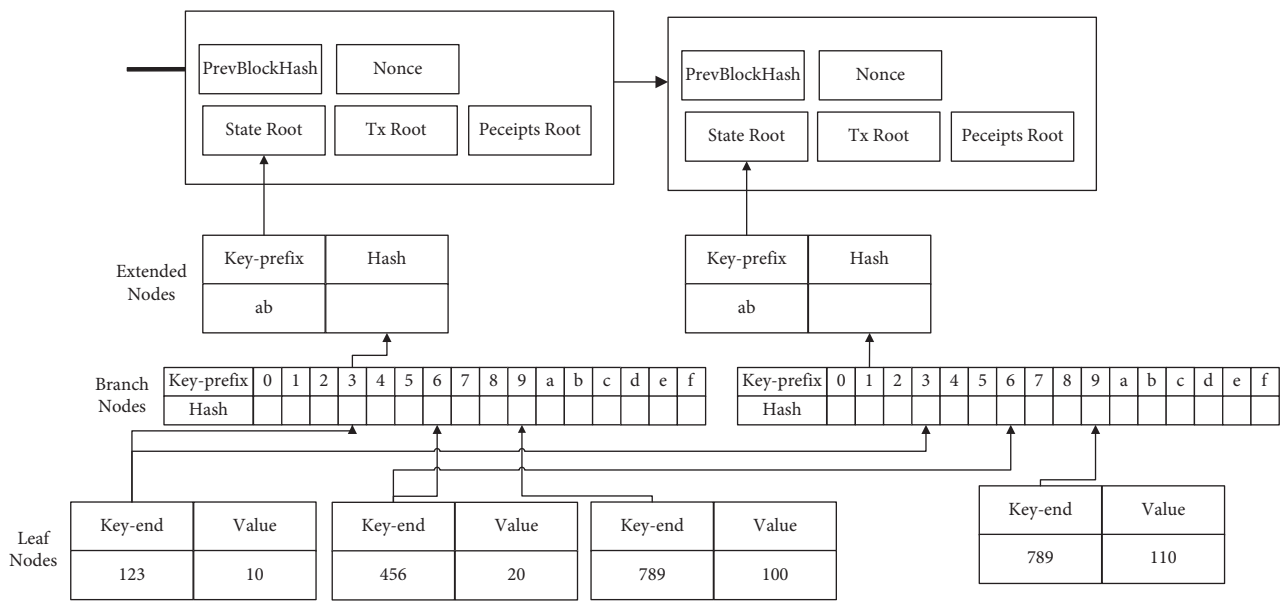

Figure 3: Merkle Patricia tree.

The input is the first transaction output from that historical transaction, and the script ScriptSig includes the current transaction's Bitcoin holder's signature. Table 3 displays the transaction output structure. An output's Bitcoins have not been spent if it has no input. You can quickly verify that a transaction's Bitcoins have been spent by collecting all current unspent transaction outputs (UTXOs). The Bitcoin balance of an account is the sum of all unspent transactions for a given Bitcoin address. The transaction-based model effectively prevents currency forgery, double spending, and other attacks.

(2) Account-Based Model. Accounts in Ethereum are classified as externally owned or contract accounts. The external

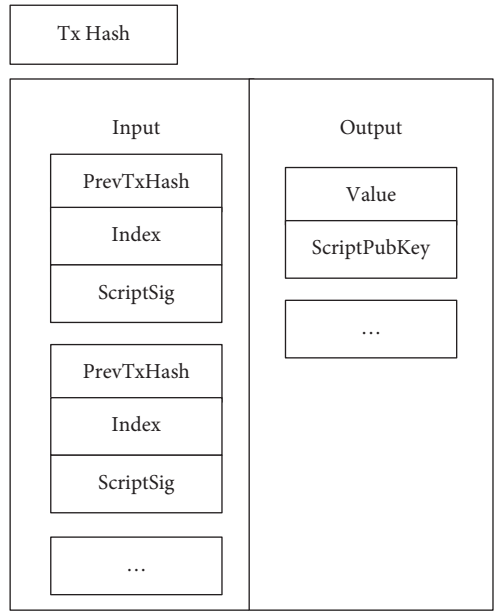

Figure 4: Data structure account of Bitcoin transactions.

Table 2: Structure of the Bitcoin transaction input.

Field	Description	Size
Previous transaction hash	Pointing to the last transaction	32 bytes
Output from the previous transaction	First output of last transaction is related to, counting from 0	4 bytes
Input script size	In bytes	1~9 bytes
Input script	Contains the proof required to spend Bitcoins, such as the holder's signature	Variable
Index	Not enabled	4 bytes

Table 3: Transaction outputs in Bitcoin.

Field	Description	Size
In (10–8 Bitcoin)	In (10–8 Bitcoin)	8 bytes
Output script size	In bytes	1~9 bytes
Output script	Defines the conditions under which the Bitcoin will be spent, e.g., the recipient's Bitcoin address	Variable

account represents an ordinary account's ether balance, which is an Ethereum smart contract. The ordinary account balance and smart contract state variables are both Ethereum data. Figure 5 depicts the Ethereum account's state transition. The state shows the current value of each account attribute. The account state changes when a transaction occurs. ETH accounts have the same data structure with four attributes: Balance, nonce, CodeHash, and StorageRoot. In a smart contract, CodeHash is the code hash, and in the state data, StorageRoot serves as the Merkle Patricia tree's root. The amount of gas consumed for the transaction is limited by GasPrice and GasLimit. To is followed by the recipient's account address and the sender's ECDSA signature.

4. Consensus Mechanism

Even if the message is lost or delayed, these algorithms assume that every node is loyal and good. All distributed database nodes must be managed by a single institution. In a decentralized blockchain network, participants do not know or trust each other, and there is the potential for deception and malpractice. This section introduces the PoW mechanism for public chains and the PBFT algorithm for federated chains, and Table 4 compares the two.

4.1. PoW. The public chain's nodes are anonymous and publicly accessible, so the consensus algorithm based on node voting is unsuitable for the public chain because a malicious attacker can create any number of nodes to increase voting power and deceive the system. The PoW mechanism effectively counters the witch attack, which relies on distributed nodes competing for arithmetic power to ensure data consistency and security across the PoW network. This means that each node must find a random number of nonces that is less than the block header's difficulty target.

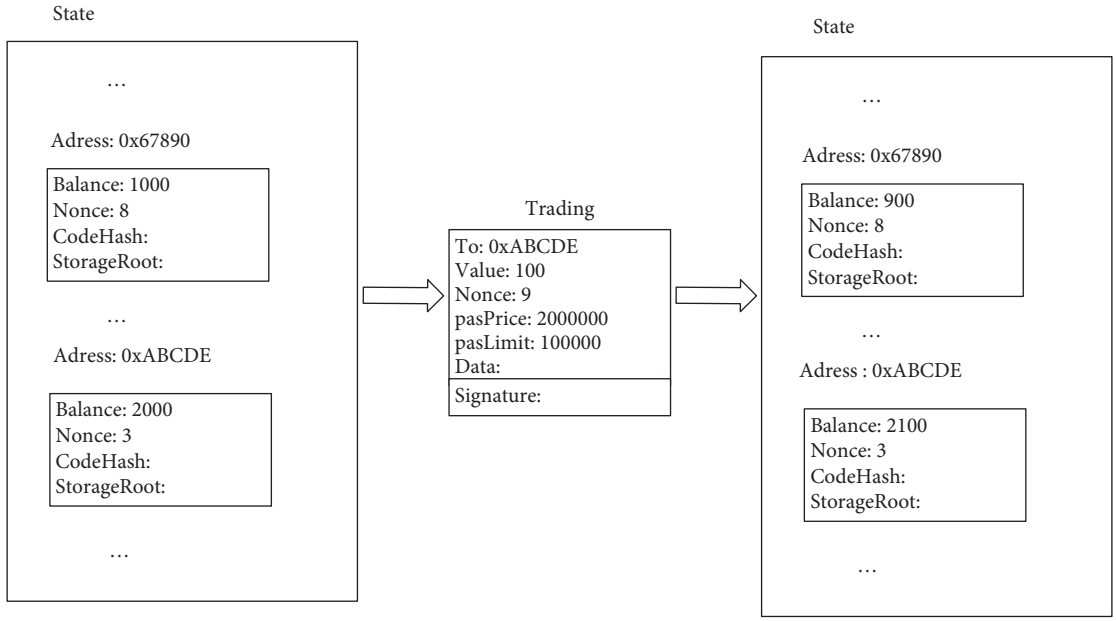

Figure 5: State transition of an Ethereum account.

Table 4: Comparison of PoW and PBFT.

	PoW	PBFT
Node access mechanism	Public chain	Alliance chains
Transaction throughput	7 TPS (Bitcoin) 20 ~ 30 TPS (ether)	200 ~ 2000 TPS (fabric 0.6)
Transaction confirmation time	60 min (Bitcoin) 3 min (ether)	Milliseconds (fabric 0.6)
Scalability	Number of nodes < 100000	Number of nodes < 100
Byzantine fault tolerance	<50% of arithmetic power	<33% of votes
Resource consumption	Hash consumes computational resources	Broadcast consumes network resources
Bifurcation possibility	Yes	No
Final consistency	No	Yes

$$H(N \| h) \leq t, \tag{1}$$

where H is the SHA256 hash function, n is the random number nonce, h is the block header data, mainly containing the previous block hash, Merkle root, etc., t is the difficulty target, the smaller the t value, the harder the n value is to find, and the first node to find it gets the bookkeeping right of the new block. In the blockchain network, the following is the PoW consensus process.

(1) All nodes in the blockchain network receive a copy of each new transaction.

(2) Each node collects all the transactions received since the previous block was generated and calculates the Merkle root of the block header based on these transactions. Once the two SHA256 hashes in the block header are less than or equal to the difficulty target, the block header's random number nonce is increased by 1. Each node in the network contributes its processing power to the overall calculation at the same time.

(3) If a node finds the correct random number first, that node will receive the bookkeeping rights to the new block and the reward (the reward includes the block reward in the new block and the transaction fee for each transaction), and will broadcast the block to the entire network.

(4) To ensure the transactions and random nonce contained in a new block are valid, other nodes must first verify the validity of the block before incorporating it into their own local blockchain and creating a new block based on it. In the absence of algorithms, a block header hash with multiple leading zeros is the essence of mining, and the more leading zeros there are in a block header hash, the less likely it is that a suitable random number will be found, so the more difficult it becomes to mine. To tamper and forge the chain, the PoW mechanism means finding the random number nonce again in the block header for each subsequent block, which requires using at least 51% of the network's computing power. As a result, the attack is both difficult and expensive. Performance on a PoW-based blockchain platform is low due to the trade-off between data consistency and security and the PoW mechanism. Bitcoin currently generates blocks every 10 minutes on average, with a block size limit of 1 MB and an average transaction size of 250 B. At a

rate of 7 TPS [43], Ether's transaction throughput is about 20–30 TPS and is generated every 12–15 seconds on average.

The two key parameters that determine the transaction throughput are block size and block-out interval. Large blocks can accommodate more transactions, but they take longer to propagate in the network, which increases the risk of forking; large blocks also require more powerful mining machines, which increases the risk of centralization. The number of nodes in the network that can successfully mine multiple blocks at the same time will surge as the block interval is reduced, ending in a fork if multiple blocks are produced at the same time. When a bifurcation occurs, the longest chain, i.e., the one that spends the most arithmetic power, is considered the main chain, while the others are considered branches, and all transactions in the branches are ignored. The bifurcation not only increases the invalidation rate of valid blocks but also causes double-spend attacks. Bitcoin refers to blocks on branch nodes as orphan blocks and discards them as scrap blocks. In order to ensure the fairness of mining and avoid the waste of mining arithmetic, Ether has introduced the GHOST (Greedy Heaviest-Observed Subtree) [44] protocol to deal with the fork, which considers the valid blocks on the branch to contribute to the confirmation of the transactions on the main chain. Instead of discarding the block, the GHOST protocol treats the block as an uncle block and gives a reward equivalent to 87.5% of the main block, gives a reward equivalent to 12.5% of the main block to the direct child of the uncle block, and gives a reward equivalent to 3% of the main block for each uncle block quoted by the miner. Although Bitcoin assumes a transaction is irreversible after 6 blocks, and Ether assumes a transaction is irreversible after 12 blocks, these transactions are not finally confirmed.

In response to the inefficient and energy-consuming PoW mechanism, the PoS mechanism determines the difficulty of mining based on the equity (i.e., the amount of digital currency) that miners have in the blockchain.

$$H(N\|h) \le s(M).t, \tag{2}$$

where M is a miner, the function s returns the equity owned by the miner, the more equity owned by the miner M, the lower the overall difficulty of mining, and the easier it is to find the right n. Ethernet proposes Casper1 based on the PoS mechanism, which requires miners to buy Ether and inject Ether as collateral. Casper is implemented as a smart contract, which proportionally allocates the bookkeeping rights and rewards of blocks to the amount of Ether and time collateralized. Casper also introduces penalties, and once a miner is found to be cheating, all of his or her pledged Ether will be forfeited, and the right to participate in consensus and block issuance will be revoked. Casper virtualizes the Bitcoin mining process, reducing the block issuance time to 4 s without mining and consuming additional power.

4.2. PBFT. While the PoW is focused on numerical competition in order to ensure data security, it consumes a significant amount of computing power and electricity. For the purpose of software applications, for federated chains, the PBFT algorithm is preferable. The PBFT algorithm can tolerate up to 1/3 of the network's total nodes for data consistency and security.

(1) The master node selects a new block from the network nodes.

(2) The master node sorts and broadcasts the list of multiple transactions to the network.

(3) Each node then simulates the execution of transactions based on the sorting. After all transactions are completed, the new block's hash digest is calculated and broadcast to the network.

(4) Commit messages are broadcast to the entire network if a node receives 2f and are digested from other nodes that are same as its own.

(5) The local blockchain and state database can be upgraded if a node receives $2f+1$.

However, in a network with N nodes, the algorithm has two phases that need to transmit network messages of O ($N2$), which can cause a large network overhead. Therefore, the system performance of the current PBFT algorithm-based blockchain is not high. In addition, how to support the dynamic joining and dropping of consensus nodes is an issue. Currently, Hyperledger Fabric 1.0 is developing consensus modules such as BFT-SMaRT, simplified Byzantine fault tolerance (SBFT), and HoneyBadgerBFT based on plug-in. The SBFT assumes that master nodes do not become malicious nodes, thus building a Raft-like messaging model that reduces broadcast communication in the network. HoneyBadgerBFT is the first practical asynchronous BFT protocol that does not rely on any time assumption to guarantee network effectiveness and is fault tolerant even in wide area networks where network behavior is unpredictable.

5. Smart Contracts

Due to the decentralized nature of blockchain, smart contracts can concurrently run on all network nodes without the involvement of a central administrator, and no institution or individual can force them to stop. Because Bitcoin does not support smart contracts, this section will concentrate on Ether and Hyperledger Fabric.

5.1. Mechanism. When the Docker container is started, it performs the contract's initialization operation prior to being invoked. Smart contracts are used by applications to execute transactions. Prior to the network being able to record changes to the blockchain and their associated outcomes in the state database, a query request does not require consensus and is, therefore, not recorded on the blockchain. In smart contracts, events can be registered and notified to external applications. However, smart contracts are unable to actively monitor or respond to off-chain events at the moment.

To execute transactions and access state data, external applications (such as the decentralized application Dapp in Ethernet) must invoke the smart contract.

5.2. Programming. The Bitcoin platform provides simple transaction scripts. To avoid possible vulnerabilities and attacks, these scripts are stack-based and do not use circular instructions or system functions. So Bitcoin scripts are not Turing-complete, and the Bitcoin platform does not have smart contracts.

Ethernet has customized Solidity, Serpent, and other Turing-complete scripting languages to develop smart contracts. Ethernet smart contracts include an account address data type that supports digital currency payment applications. Transactions sent to the contract address will trigger the smart contract. The contract execution process consumes gas, which is converted from Ether. In June 2016, the DAO1 smart contract, the largest crowdfunding project on Ether, was attacked due to a recursive call vulnerability, resulting in the loss of approximately 12 million Ether coins. For such a rationale, the Solidity group is considering formal verification.

Hyperledger Fabric supports Go and Java smart contracts, both of which are Turing-complete, and compilation technology is very mature. It is the only way to communicate with the blockchain and generate transactions. Writing a contract involves implementing the Chaincode interface's Init, Invoke, and Query functions, which are used to initialize, modify, and query state data.

6. Conclusions

The digital copyright industry is thriving in the internet era, and the emergence of blockchain technology has accelerated innovation in digital copyright protection. There are a number of issues with the traditional digital copyright protection model, including difficulty in registering and confirming rights, difficulty in monitoring infringement, and so on. The establishment of a unified blockchain-based digital copyright protection platform offers a unique opportunity to address the aforementioned issues. In terms of digital copyright registration and confirmation, blockchain technology eliminates the time-consuming, high-cost, and difficult-to-audit problems associated with traditional registration methods, transcends space and time constraints, and enables any creator to register and confirm their rights. The digital copyright registration and rights confirmation platform developed by Baidu Totem and Paper Gui Technology has provided us with extensive practical experience and protected the legitimate creators' rights to digital copyright. By utilizing smart contracts, the ledger digital copyright trading platform can improve oversight of digital copyright transactions and enable decentralized transactions, thereby resolving issues of ownership confusion and revenue generation from transactions involving massive collaborative creative works and tiny works, among others. The complete record and transparency provided by blockchain technology for transactions enable purchasers to gain a better understanding of the rights status of works. Blockchain technology has the potential to provide purchasers with a more complete understanding of the rights status of works and to eliminate the occurrence of erroneous swipes. In the forensic aspect of digital copyright protection, the timestamp, difficulty of tampering, and traceability of blockchain technology can help establish the authenticity of electronic evidence and alleviate the problems associated with high forensic costs and lengthy verification times. Each internet court and several provincial high people's courts have established their own blockchain-based electronic evidence registration platform, utilizing the blockchain technology alliance chain to achieve complete coverage of evidence information deposition, forensics, verification, and sharing, resolving the contradiction between judicial institutions' centralization of trial power and decentralization of judicial deposition.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This study was supported by the 020 Project of Business College of the Shanxi University (Study on the Legal Regulation of Malicious Litigation of Intellectual Property Rights, 2020033), China.

References

[1] S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," 2008, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802.

[2] V. Buterin, "A Next-Generation Smart Contract and Decentralization Application Platform," *White Paper*, vol. 3, 2014.

[3] C. Cachin, "Architecture of the Hyperledger blockchainfabric," in *Proceedings of the Workshop Distributed Cryptocurrencies and Cons (Csensus) Le*, IBM Research, Chicago, IL, USA, June 2016.

[4] R. G. Brown, J. Carlyle, I. Grigg, and H. Mike, *Corda: An Introduction*, Wiley-blackwell, Hoboken, NJ, USA, 2016.

[5] H. M. Corda, *A Distributed Ledger*, Blockchain, Luxembourg, Luxembourg, 2016.

[6] T. McConaghy, R. Marques, and A. Müller, *BigchainDB: Ascalable Blockchain Database*, Blockchain, Luxembourg, Luxembourg, 2016.

[7] Beijing Peer Safe Technology Co Ltd, *White Paper for Blockchain Data Base Application Platform*, Beijing Peer Safe Technology Co Ltd, Beijing, China, 2017.

[8] T. Fit, *Whitepaperfortencent Trust SQL*Tencent Research Institute, Beijing, China, 2017.

[9] Y. Yuan and F.-Y. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[10] P. He, Y. Ge, and Y. F. Zhang, "Survey on blockchain technology and its application project," *Computer Science*, vol. 44, no. 4, pp. 1–7, 2017.

[11] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: a technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[12] S. D. Gribble, A. Y. Halevy, and Z. G. Ives, "What can data base do for peer-to-peer?" in *Proceedings of the Fourth International Workshop on the Web and Databases (WebDB)*, pp. 31–36, Santa Barbara, CA, USA, February 2001.

[13] M. Yu, L. Zhan-Huai, and L. B. Zhang, "P2P data management," *Journal of Software*, vol. 17, no. 8, pp. 1717–1730, 2006.

[14] W.-N. Qian, "Data Management in Peer-To-Peer Systems," Ph. D. Dissertation, Fudan University, Shanghai, China, 2004.

[15] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc, Sebastopol, CA, USA, 2014.

[16] L. Lampport, "The part-time parliament," *ACM Transactions on Computer Systems*, vol. 16, no. 2, pp. 133–169, 1998.

[17] L. Lampport, "Paxos made simple," *ACM Sigact News*, vol. 32, no. 4, pp. 18–25, 2001.

[18] D. Ongaro and J. K. Osterhout, "In Search of an Understandable Consensus algorithm," in *Proceedings of the USENIX AnnualTechnical Conference*, pp. 305–319, Berkeley, CA, USA, June 2014.

[19] L. Lampport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[20] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *Journal of the ACM*, vol. 32, no. 2, pp. 374–382, 1985.

[21] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[22] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva," *ACM SIGOPS - Operating Systems Review*, vol. 41, no. 6, pp. 45–58, 2007.

[23] J. Kwon, *Tendermint: Consensus without Mining*, Blockchain, Luxembourg, Luxembourg, 2014.

[24] S. Liu, P. Viotti, and C. Cachin, "XFT: Practical Fault tolerance beyond crashes," in *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 485–500, Savannah, GA, USA, November 2016.

[25] J. Behl, T. Distler, and R. Kapitza, "Scalable Bft for Multi-Cores: Actor-Based Decompation and Networksus-Oriented Parallelization," in *Proceedings of the 10th Workshop on Hot Topics in SystemDependability (HotDep)*, pp. 9–14, Broomfield, CO, USA, October 2014.

[26] M. Zbierski, "Parallel Byzantine Fault tolerance, Advances in Intelligent Systems and Computing," in *Soft Computing in Computer and Information Science*, I. Fray and J. Pejas, Eds., Springer International Publication, Salmon, NY, USA, pp. 321–333, 2015.

[27] W. Zhao, "Optimistic Byzantine fault tolerance," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 31, no. 3, pp. 254–267, 2016.

[28] D. Schwartz, N. Youngs, and A. Britto, *The Ripple Protocolconsensus Algorithm*, Blockchain, Luxembourg, Luxembourg, 2014.

[29] J. R. Douceur, "The sybil attack," in *Proceedings of the International Workshop on Peer-To-Peer Systems (IPTPS)*, pp. 251–260, Cambridge, MA, USA, March 2002.

[30] C. Dwork and M. Naor, "Pricing via Processing or Communicating junkmail," in *Proceedings of the Advances in Cryptology-Crypto'92(CRYPTO)*, pp. 139–147, Santa Barbara, CA, USA, August 1992.

[31] J. Aspnes, C. Jackson, and A. Krishnamurthy, "Exposing Computa-tionally-challenged Byzantine impostors," Technical Report YALEU/DCS/TR-1332, Yale University, London, UK, 2005.

[32] S. King and S. Nadal, *PPCoin: Peer-To-Peer Crypto-Currency Withprov-Of-Stake*, Blockchain, Luxembourg, 2012.

[33] D. Larimer, *Delegated Proof-Of-Stake*, Blockchain, Luxembourg, Luxembourg, 2014.

[34] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *Sequences II*, Springer-Verlag, pp. 329–334, Salmon, NY, USA, 1993.

[35] S. Haber and W. S. Stornetta, "Howto Time-Stampa Digital document," in *Proceedings of the Advances in Cryptology-Crypto'90 (CRYPTO)*, pp. 437–455, Santa Barbara, CA, USA, August 1990.

[36] S. Haber and W. S. Stornetta, "Secure Names for Bit-strings," in *Proceedings of the 4th ACM Conference on Compute and Communications Security (CCS)*, pp. 28–35, Zurich, Switzerland, April 1997.

[37] R. C. Merkle, "Protocols for Publickey cryptosystems," in *Proceedings of the 1980 IEEE Symposium on Security and Privacy (S&P)*, pp. 122–134, Oakland, CA, USA, April 1980.

[38] R. C. Merkle, "A Digital Signature Based on a Conventional encryption function," in *Proceedings of the Advances in Cryptology-CRYPTO '87, (CRYPTO)*, pp. 369–378, Santa Barbara, CA, USA, December 1987.

[39] M. Szydlo, "Merkle Tree Traversal in Log Space and time," in *Proceedings of the Advances in Cryptology-EUROCRYPT 2004 (EUROCRYPT)*, pp. 541–554, Interlaken, Switzerland, May 2004.

[40] A. Narayanan, J. Bonneau, and E. Felten, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, NJ, USA, 2016.

[41] C. Dannen, *Introducting Ethereum and Solidity: Foundation of Cryptocurrency and Blockchain Program for Beginners*, Apress, New York, NY, USA, 2017.

[42] S. Qing-Chun, *Development Guide of Blockchain*, China Machine Press, Beijing, China, 2017.

[43] D. R. Morrison, "PATRICIA-practical algorithm to retrieve information coded in alphanumeric," *Journal of the ACM*, vol. 15, no. 4, pp. 514–534, 1968.

[44] R. Hagmann, "Reimplementing the Cedar file system using logging and group commit," *ACM SIGOPS-Operating Systems Review*, vol. 21, no. 5, pp. 155–162, 1987.