Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210189

Anti-Counterfeiting and Traceability Mechanism Based on Blockchain

Tan Ji [a, 1] and Dr S B Goyal [a]

[a] *City University, Petaling Jaya, Malaysia*

Abstract: The anti-counterfeiting traceability system based on blockchain technology can ensure the accuracy and consistency of the data stored by each participating node, protect the legitimacy of the data, ensure the product quality, improve the credibility of enterprises, and enhance consumers' confidence in products. However, due to the low system throughput, high energy consumption and poor data availability, the combination of blockchain and traditional anti-counterfeiting traceability mode has many challenges, such as low efficiency. This paper aims to find an improved consensus mechanism based on contribution proof to improve the mining efficiency of honest miners. And plan to introduce a credit system, give priority to the high credit value of the mining block to package, improve the overall packaging efficiency of the system, to solve the problem of low feedback efficiency of the blockchain anti-counterfeiting system.

Keywords: Anti-Counterfeiting, Traceability Mechanism, Blockchain, Network.

1. Introduction

Online shopping has brought significant improvement to people's quality of life. However, the huge number of transactions also gave birth to a large number of fake and inferior commodities. The anti-counterfeiting and traceability system based on blockchain technology can ensure the accuracy and consistency of the data stored by each participating node, protect the legitimacy of the data, ensure the quality of products, improve the credibility of enterprises, and enhance consumers' confidence in products. This chapter introduces the core technology of blockchain anti-counterfeiting traceability system.

1.1 Blockchain

The concept of Blockchain first appeared in a paper "Bitcoin: A peer-to-peer electronic cash system" published by Satoshi Nakamoto on the Bitcoin Forum in 2008, the article pointed out, Blockchain is the basic technology to build the Bitcoin system, and proposes an electronic cash system that is completely realized by peer-to-peer technology, and gives the method realization [1]. Blockchain has four characteristics: decentralization, openness and transparency, consensus mechanism, and anonymity [2-4].

[1] Dr S B Goyal,City University, Petaling Jaya, Malaysia
Email: drsbgoyal@gmail.com

Table 1. Blockchain concept

S.No.	Blockchain Concepts	Descriptions	Example/ Real-life Use case
1	Decentralization	Blockchain technology does not rely on centralized hardware or management institutions [5]. The authority of each node is equal, and the processes of data verification, storage, transmission, and maintenance are implemented on the distributed system, which is the most prominent and essential feature of blockchain [6].	Distributed billing
			Distributed propagation
			Distributed storage
2	Consensus mechanism	The core component of blockchain. Using the consensus mechanism, users in the blockchain do not need to consider each other's credit or trust each other. Blockchain uses a consensus algorithm based on mathematical principles to establish a trusted network between nodes [7].	PoW consensus algorithm
			PoS consensus algorithm
			Distributed storage
			Paxos consensus algorithm
			Raft consensus algorithm
3	Smart contract	The smart contract is a transaction agreement that is processed by a computer and can execute contract terms. Its overall goal is to meet the general contract conditions, such as a mortgage, confidentiality, payment, enforcement, etc., and minimize the possibility of malicious or unexpected events, as well as the function of trust intermediary [8].	Decentralized authority

1.2 Types of Blockchain

Blockchains are divided into three types: public blockchain, private blockchain and consortium blockchain [9-10].

1)Public blockchain: It can be understood as a public blockchain, which is completely open and transparent, that is, a blockchain that everyone can participate in. In other words, the behavior on the public chain is public, and it is not controlled by anyone, nor is it owned by anyone. It is considered a "fully decentralized" blockchain.

2)Consortium blockchain: is a semi-public blockchain, which refers to a blockchain that is managed by several institutions. Each institution runs one or more nodes, and

the data in it is only allowed by different institutions in the system. Read, write and send transactions, and record transaction data together.

3)Private blockchain: It is a completely closed blockchain whose write permission is controlled by an organization and institution. The qualifications of participating nodes will be strictly limited.

1.3 Cryptography in the blockchain

In order to ensure the security and integrity of data stored on the blockchain, a variety of modern cryptographic technologies are used in the definition and construction of blocks and blockchains, including public key encryption systems, hash functions, and Merkle trees, etc. [11-14] At the same time, a large number of related cryptographic techniques are also used in the design of a variety of different consensus algorithms.

Table 2. Cryptography in the blockchain

S.No.	Cryptography in blockchain	Descriptions
1	Public key encryption system	The public key cryptographic algorithm requires two keys: a public key and a private key.[15] The public key and the private key are a pair. If the public key is used to encrypt data, only the correspond-ing private key can be decrypted. On the contrary, if the private key is used to encrypt the data, only the corresponding public key can decrypt it.
2	Hash function	Cryptographic hash algorithm, also known as hash function, is a kind of math-emetically function that can create a small digital "fingerprint" from any da-ta.[16] That is, data of any length can be compressed into a fixed-length binary string within a limited and reasonable time, which is called a hash value.
3	Merkle tree	Another use of hash algorithm in blockchain is to build Merkle Tree, also known as hash tree.[17] It is a binary or multiple tree based on hash value. It consists of a root node, a set of intermedi-ate nodes and a set of leaf nodes.

1.4 Consensus algorithm and classification

Proof-of-work (Po W), also known as workload Proof, is the core consensus algorithm of Bitcoin. Its core idea is to ensure data consistency and security of consensus by in-troducing computing power competition of distributed nodes, which is also known as "mining" [18]. This algorithm makes the blockchain system need to consume a large amount of computing power, so the consensus efficiency is low.

Table 3. Consensus algorithm and classification

S.No.	Classification	Descriptions
1	PoS consensus algorithm	Proof of Stake is a voting mechanism.[19] Compared with PoW consensus mechanism, calculation power resources are too much wasted, PoS consensus algorithm only needs a small amount of calculation to ensure the normal operation of block chain.
2	DPoS consensus algorithm	The Delegated Proof mechanism of Stake by DPoS (Delegated Proof of Stake) was first proposed and applied by Bitshares in August 2013[20]. On the basis of PoS, DPoS professionalizes the role of bookkeeper. First, bookkeepers are selected through equity. Then, bookkeepers take turns to keep accounts. The advantage is that the number of participating verification and billing nodes can be greatly reduced and the consensus verification can be achieved at the sec-ond level, but at the same time, the whole consensus still relies on token, which still does not solve the pain point of commercial use.
3	Paxos consensus algorithm	Paxos algorithm is the consensus algorithm proposed by LeslieLamport in her paper in 1990 [21]. The main purpose of Paxos algorithm is to gradually reach consensus among every participant participating in distributed processing through this consensus algorithm. In the concrete implementation, it is divided into three roles: Proposer is responsible for Proposer, accept receiver is re-sponsible for making decision on Proposer, Learner is responsible for learning the results of Proposer. A process may play multiple roles simultaneously.
4	Raft consensus algorithm	Due to the complexity of Paxos algorithm, it was difficult to understand, so Diego proposed Raft algorithm [22]. As a simple implementation of the Paxos algorithm, it ACTS like Paxos and is more efficient than Paxos, but it has a very different architecture, which makes Raft much easier to understand than Paxos.

1.5 Anti-counterfeiting and traceability

We are exploring the anti-counterfeiting to prevent counterfeiting and traceability to access the product moment in the system. We are doing literature survey for the same in this section.

1.5.1 Anti-counterfeiting

Anti-counterfeiting refers to a measure taken proactively to prevent counterfeiting as a means to imitate, copy or counterfeit and sell others' products without the permission of the trademark owner.[23]
Anti-counterfeiting technologies include laser anti-counterfeiting, query digital label anti-counterfeiting (one-dimensional code), textured anti-counterfeiting label, security thread anti-counterfeiting, unlimited anti-counterfeiting, etc.
At present, the anti-counterfeiting technology has been developed to the fifth generation of products, the use of mobile phone Internet for anti-counterfeiting technology. By attaching anti-counterfeiting labels that automatically identify mobile phones to products and packaging, consumers can use their mobile phones to scan the QR code for authenticity identification. When combined with texture anti-counterfeiting and security line anti-counterfeiting, consumers will truly feel relieved and comfortable shopping.

From Figure 1, we can see that the industries affected by blockchain ecology include finance, health care, culture, social welfare, education, product supply chain, etc. At the same time, it can serve individuals and enterprises. Therefore, blockchain and anti-counterfeiting traceability will have a good combination.

1.5.2 Traceability Mechanism

The traceability is the earliest food safety management system established and perfected by the European Union in 1997 in response to the "mad cow disease" problem.[24] At present, traceability technology is usually combined with anti-counterfeiting technology. A single product is given a unique QR code as an anti-counterfeiting ID through professional machinery and equipment, so that "each product has its own identity code". Then data can be collected and tracked in various links such as product production, warehousing, distribution, logistics transportation, market inspection, sales terminals, and constitute a full life cycle management of product production, storage, sales, circulation and service.

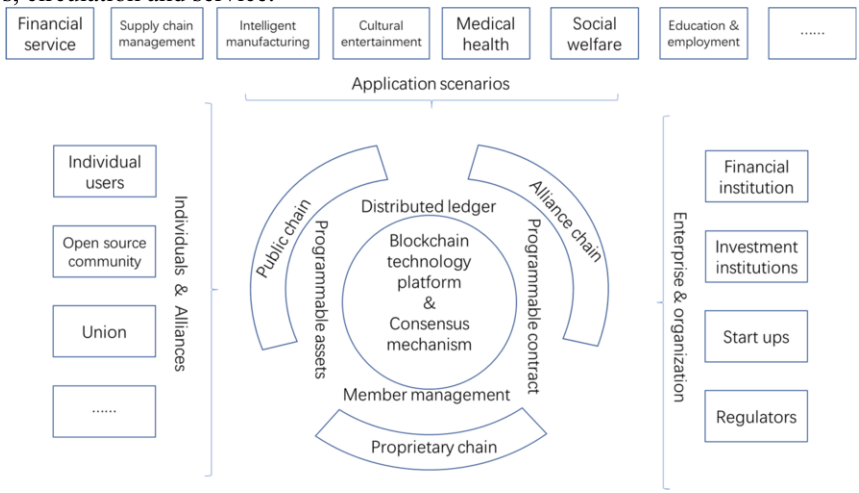

Figure 1. Blockchain ecology

It can be seen from Picture 2 that the existing anti-counterfeiting traceability system stores data in the traceability management system server through raw materials, logistics, storage, production, sales, and other processes. The anti-counterfeiting requirements of products can be queried through the traceability chain to find the corresponding information in each link of production. At the same time, government regulatory agencies, corporate regulatory agencies, and consumers can access the traceability management system server through the Internet and the Internet of Things to query the required information.

2. Literature Survey

At present, the application of blockchain in anti-counterfeiting is less in the world. The first application example is to input the information of containers and goods into the blockchain system, which arranges the transportation route and date of containers, so as

to realize the intelligent anti-counterfeiting and traceability of the goods in the container. Other applications mainly focus on luxury traceability, banks, insurance companies, etc.

China's domestic e-commerce companies introduced blockchain technology earlier. Both Alibaba and jd.com make use of blockchain, Internet of things, big data and cloud computing technology component blockchain anti-counterfeiting traceability platform to realize the whole process traceability of one code for one thing or one code for one batch across brands, retailers, consumers and channel providers.

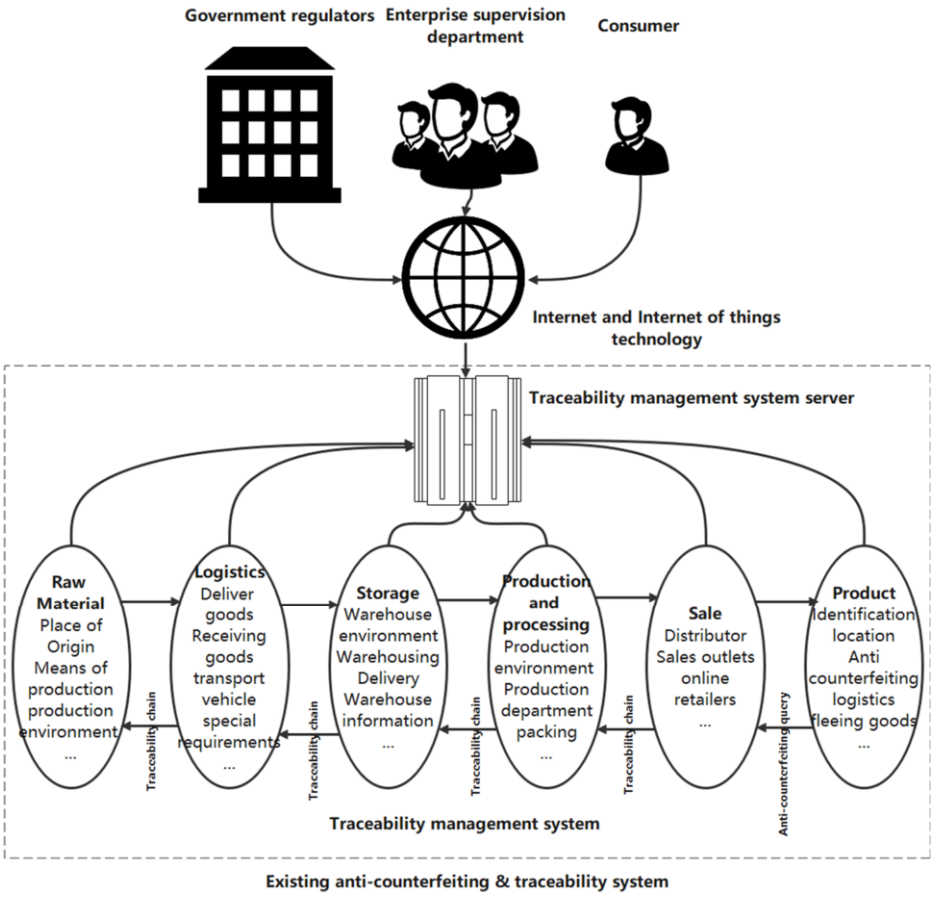

Figure 2. Existing anti-counterfeiting & traceability mechanism system

In terms of system efficiency, Jia Dayu et al. proposed an effective blockchain storage capacity scalable model query method Elastic QM, which stores data in the user layer, query layer, storage layer and data layer modules to improve system query [25]; Qiao Rui et al. designed a consensus mechanism for the security of dynamic data storage based on blockchain and gave a mathematical model for the security of dynamic data storage. Experiments have shown that this solution can effectively improve dynamic data. [26]; Based on the blockchain traceability platform, Liu Yadong proposed a rapid

block generation strategy and a dual-chain storage mechanism, which improved the storage performance and security of the platform [27].

3. Research Gaps

First, a method needs to be found to modify consensus mechanism based on contribution proof. Without modifying the existing data structure of bitcoin, we can reward the miners who successfully publish the block and punish the miners who publish the false block. Then, different mining difficulties are given to different addresses, so that honest miners have a higher probability of obtaining bookkeeping rights and rewards. However, it is necessary to control the probability curve so that the whole mining process is still friendly to the miners with only 0 or a few successful times.
Secondly, the credit system is introduced to pack the blocks issued by miners with high credit value, and improve the efficiency of package system, so as to solve the problem that enterprises and consumers can find the fake and inferior goods in the market for the first time.
Thirdly, we should decentralize the credit system to solve the problem that the transaction information is false when it is first released.

4. Objectives

1) Find a way to modify the consensus mechanism based on proof of contribution to improve the mining efficiency of honest miners.
2) Introduce a credit system, prioritize the packaging of blocks released by miners with higher credit values, and improve the overall packaging efficiency of the system.
3) Decentralize the management of the credit system to solve the situation that the transaction information is false when it is initially released.

5. Proposed Hypothesis

The research challenges of blockchain-related issues involved in this research:
1) How to design a contribution proof system to count the contribution of honest miners?
We are focusing on a contribution proof system using the concept of proof-of-stack.
The contribution system can reward honest miners and increase their probability of becoming bookkeeper.
2) How to join the contribution system into the consensus mechanism?
Joining the consensus mechanism is the way to apply the contribution system. The combination of the two algorithms can verify whether the contribution system can improve the probability of honest miners becoming bookkeeper.
3) How to design the contribution system so that it is still friendly to new miners?
In the same contribution system, if the honest miners' contribution is large enough, it will get a higher probability to become bookkeeper. But this is not friendly to new miners. It is necessary to make the probability curve tend to be flat in a certain probability.

4) Can credit system improve the overall discrimination efficiency of the system?
The introduction of credit system can make the block produced by honest miners with high credit degree pack in advance, rather than fixed time package, so as to improve the overall discrimination efficiency of the system.
5) How to decentralize the credit system?
Credit systems need to be managed as decentralized as other data. This can avoid the appearance of fraud.

6. Proposed Methodology

The research methods considered and selected in this study mainly include the following three types:
1) Literature research method: Extensively consult related literature materials related to the application of blockchain technology in anti-counterfeiting and traceability systems.
2) On-site investigation method: specifically investigate the needs of enterprises with anti-counterfeiting and traceability requirements, and conduct on-site visits to relevant government departments, logistics companies, commodity wholesale markets, supermarkets and other locations that may produce counterfeit and inferior products, and clarify the existing anti-counterfeiting and traceability systems Propose corresponding solutions to the problem.
3) Comparative analysis method: By studying relevant documents, comparing existing anti-counterfeiting and traceability systems, analyzing the advantages and disadvantages of each system, and providing technical and theoretical support for subsequent research.

7. Expected Result

1) The introduction of a contribution proof mechanism can improve the reward system of honest miners. The blocks distributed by honest miners can be packed first, which reduces the space occupied by blocks, reduces the block packing time, and effectively improves the efficiency of the system.
2) The decentralized management of credit systems can effectively avoid source data fraud.
3) Expected system architecture: Based on the traditional anti-counterfeiting traceability system, the contribution proof algorithm is added. The improved system architecture is shown in Figure 3.

8. Discussion

1) The introduction of a contribution proof mechanism can improve the reward system of honest miners. This kind of incentive mechanism makes more and more honest miners join the system, so as to realize the process that consumers help enterprises monitor and identify fake and shoddy products, and save a lot of costs. In addition, due to the decentralized and anonymous characteristics of blockchain, it can effectively avoid the occurrence of false information in the transaction process.

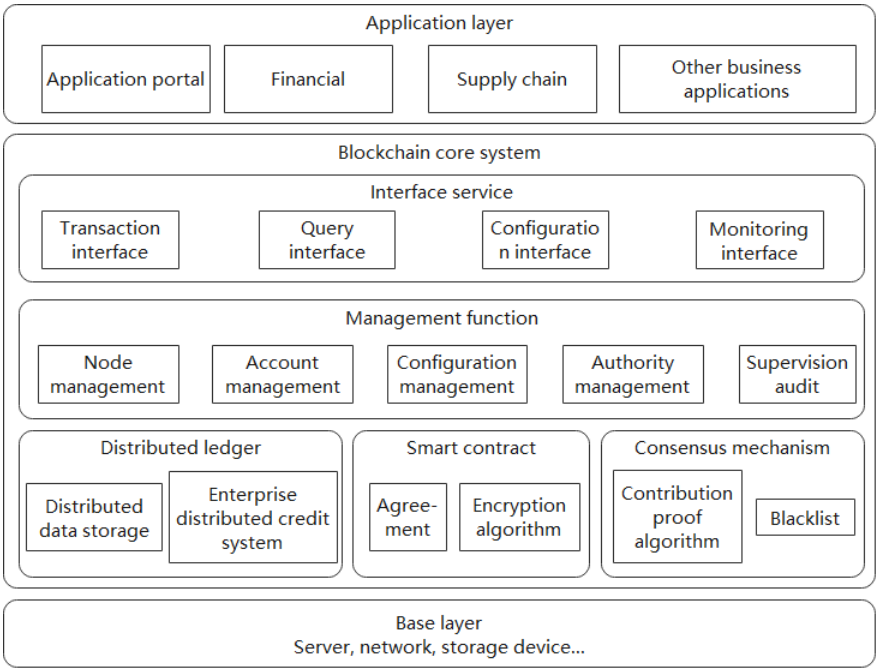

Figure 3. Optimized anti-counterfeiting traceability system architecture

2) The introduction of a credit system and the priority credit principle for enterprises and users with high reputations can effectively avoid the occurrence of source data fraud. At the same time, the distributed management of the credit system can improve the credibility and security of the credit system.

3) Figure 3 is the improved expected system architecture. As can be seen from Figure 3, the entire system architecture is divided into three parts, the application layer, the blockchain core system, and the base layer. The application layer contains the front-end architecture of the system, which is the user-accessible part. The core system of the blockchain is a key part of the entire architecture. Among them, the interface service provides a data link connecting the application layer and the data layer. The management function is the overall management part of the system. The distributed ledger stores all blocks generated by transactions. The smart contract contains part of the transaction agreement and encryption algorithm. The consensus mechanism includes an improved contribution proof algorithm and a blacklist. Finally, the basic layer includes hardware facilities such as servers, networks, and storage devices.

9. Conclusion

In this proposal, we have identified problems of counterfeiting and non-traceability concerns in traditional computing network system. Counterfeiting and non-traceability increases the inaccuracy and inconsistency in the system.

We are working on these problems to improve the accuracy and maintain the consistency of the data stored by each stakeholder and protect the acceptability of the data and credibility of the system; Effectiveness - The credit system is introduced into the consensus algorithm to improve the overall efficiency of the system. Decentralization - Management of the credit system can avoid the phenomenon that product information is false information at the beginning, and on the other hand can avoid the drawbacks of centralized management of the credit system and reduce the possibility of system attacks.

References

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, pp. 1-9. https://bitcoin.org/bitcoin.pdf

[2] Zhang N , Wang Y , Kang C , et al. Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications[J]. ZhongguoDianjiGongchengXuebao/Proceedings of the Chinese Society of Electrical Engineering, 2016, 15(36):4011-4022.

[3] Zhu X . Research on blockchain consensus mechanism and implementation[J]. IOP Conference Series: Materials ence and Engineering, 2019, 569:042058-.

[4] Lan, Wang, Ranran, et al. A Study on the Influence of Blockchain Technology on Auditing[C]// 2018.

[5] Chu S , Wang S . The Curses of Blockchain Decentralization[J]. 2018.

[6] Li X , Mei Y , Gong J , et al. A Blockchain Privacy Protection Scheme Based on Ring Signature[J]. IEEE Access, 2020, 8:76765-76772.

[7] Xu Y , Li Q , Min X , et al. E-commerce Blockchain Consensus Mechanism for Supporting High-Throughput and Real-Time Transaction[J]. 2016.

[8] LinoyS ,Stakhanova N , Matyukhina A . Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution[C]// 2019 15th International Conference on Network and Service Management (CNSM). IEEE, 2020.

[9] Deng L , Chen H , Zeng J , et al. Research on Cross-Chain Technology Based on Sidechain and Hash-Locking[M]// Edge Computing – EDGE 2018. Springer, Cham, 2018.

[10] Guillaume Vizierécole Vizier, GramoliV .ComChain: Bridging the Gap Between Public and Consortium Blockchains[C]// ComChain: Bridging the Gap Between Public and Consortium Blockchains. 2018.

[11] Pinch R G E . On using Carmichael numbers for public key encryption systems[C]// Springer, Berlin, Heidelberg, 1997.

[12] Chen L , Lee W K , Chang C C , et al. Blockchain based searchable encryption for electronic health record sharing[J]. Future Generation Computer Systems, 2019, 95(JUN.):420-429.

[13] BelejO ,Staniec K , Wickowski T . The Need to Use a Hash Function to Build a Crypto Algorithm for Blockchain[C]// International Conference on Dependability and Complex Systems. 2020.

[14] BaohongH ,Yihui Z , Sude Q . Overview of Blockchain Technology[J]. Computer Engineering, 2019.

[15] Chen B , Wu L , Wang H , et al. A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6):5813-5825.

[16] BelejO ,Staniec K , Wickowski T . The Need to Use a Hash Function to Build a Crypto Algorithm for Blockchain[C]// International Conference on Dependability and Complex Systems. 2020.

[17] Mohan A P , Mohamed A R , Gladston A . Merkle Tree and Blockchain-Based Cloud Data Auditing[J]. International Journal of Cloud Applications and Computing (IJCAC), 2020, 10.

[18] Mohan A P , Mohamed A R , Gladston A . Merkle Tree and Blockchain-Based Cloud Data Auditing[J]. International Journal of Cloud Applications and Computing (IJCAC), 2020, 10.

[19] Bach L M ,Mihaljevic B , Zagar M . Comparative analysis of blockchain consensus algorithms[C]// 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). 2018.

[20] Chen S Y , Liu X . Data mining from 1994 to 2004: an application-orientated review[M]. Inderscience Publishers, 2005.

[21] Yang F , Zhou W , Wu Q , et al. Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism[J]. IEEE Access, 2019, PP(99):1-1.

[22] Zi-Can X U , Rong-Quan W U . Research on Paxos Algorithm Based on Messages Passing[J]. Computer Engineering, 2011, 37(21):287-290.

[23] TuylsP , Guajardo J , Batina L , et al. Anti-Counterfeiting[M]// Security with Noisy Data. Springer, 2007.

[24] Ajila S A ,Kaba A B . Using traceability mechanisms to support software product line evolution[C]// Information Reuse and Integration, 2004. IRI 2004. Proceedings of the 2004 IEEE International Conference on. IEEE, 2004.

[25] FazlaliM ,Eftekhar S M , Dehshibi M M , et al. Raft Consensus Algorithm: an Effective Substitute for Paxos in High Throughput P2P-based Systems[J]. 2019.

[26] Da-Yu J , Jun-Chang X , Zhi-Qiong W , et al. Efficient Query Model for Storage Capacity Scalable Blockchain System[J]. Journal of Software, 2019.

[27] Rui Q , Shi D , Qiang W , et al. Blockchain Based Secure Storage Scheme of Dynamic Data[J]. Computer ence, 2018.