Hindawi
Complexity
Volume 2021, Article ID 5536326, 12 pages
https://doi.org/10.1155/2021/5536326

Research Article

A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics

Gongzheng Liu, Jingsha He, and Xinggang Xuan

Faculty of Information Department, Beijing University of Technology, Beijing 100124, China

Correspondence should be addressed to Gongzheng Liu; 475752719@qq.com

Received 17 February 2021; Revised 24 March 2021; Accepted 12 April 2021; Published 20 April 2021

Academic Editor: Wei Wang

Since digital forensics becomes more and more popular, more and more attention has been paid to the originality and validity of data, and data preservation technology emerges as the times require. However, the current data preservation models and technologies are only the combination of cryptography technology, and there is a risk of being attacked and cracked. And in the process of data preservation, human participation is also needed, which may lead to data tampering. To solve problems given, this paper presents a data preservation model based on blockchain and multidimensional hash. With the decentralization and smart contract characteristics of blockchain, data can be automatically preserved without human participation to form a branch chain of custody in the unit of case, and blockchain has good antiattack performance, which is the so-called 51% attack. Meanwhile, in order to solve the problem of data confusion and hard to query caused by the excessive number of cases, hash, cryptography, and timestamps are used to form a serialized main chain of custody. Because of the confliction problem of hash and judicial trial needs to absolutely guarantee the authenticity and validity of data, multidimensional hash is used to replace regular hash. In this way, the data preservation becomes an automatic, nonhuman-interventional process. Experiments have been carried out to show the security and effectiveness of the proposed model.

1. Introduction

With the high development of smart technologies, performance of terminals like smart phones and tablet personal computers becomes better and better. Under this circumstance, more and more criminals use these smart terminals to commit crimes, which results in the appearance of digital forensics. Since the digital data are easy to create, store, transfer, and use, the data in digital forensics are also easy to be modified and changed in forensic investigations; it is vital that the primitiveness and integrity of digital evidence be ensured. Thus, we need to guarantee the integrity and creditability of the data.

With the development of technologies like data preservation, such as cryptography, data-hiding, digital signature, timestamp, data digest, and programming, data preservation for crime scene investigation has grown in recent years. For example, data preservation has helped to preserve judicial evidence both in the course of investigation and court [1]. This technology has also been used at many other fields, such as preserving privacy data for cloud applications [2] and wireless sensor network applications [3]. This technology can provide many advantages: the evidence data are perfectly preserved and frozen in time, the process of preservation is automatic and nonintrusive, and evaluations and measurements can be performed independently of crime scene access [4]. With an increased development in technologies, more and more technologies can be used for data preservation, the performance will be better and the cost will be smaller.

The most popular approach for data preservation is the combination of data encryption and data digest [5]. The author has written an article about the approach [6]. This approach uses the symmetric and asymmetric encryption algorithm to encrypt data, combines the timestamp information with the data, and then generates a hash digest with the hash algorithm. In this way, when the data are used for judicial purpose, investigators can use identical approaches

in reverse order to validate if the data are manipulated. Despite these benefits, there is a fatal weakness in the data preservation approach, which is that all the processes are executed by investigator, and no one can guarantee that investigators will not make mistakes intentionally or unintentionally. In response to this point, the author visited law enforcement officers and technical experts in data preservation departments and discussed needs of the data preservation method in practical application. Both law enforcement officers and technical experts say that whether the data preservation process can guarantee the primitiveness and integrity of the data or not is the most important. Other than that people cannot intervene in the whole process is also important.

So, in this article, we present a safe, highly automatic, nonhuman-interventional, and extendable data preservation model for digital forensics. This model uses the multidimensional hash algorithm with information of devices' identifications, user information, and timestamps to form the main chain of custody and uses blockchain technology to form an intersecting branch chain of custody to guarantee the security of data effectively.

The structure of the article is as follows. The Related Work section introduces the research results of data preservation, and the Technology Background section gives the basic concepts about technologies used in the proposed model. In the section of Model, the detail description and construction process is described, and the Evaluation section introduces the experiment results to prove the validity and efficiency of the model.

2. Related Work

There are some works on blockchain for data preservation, but few works are for digital forensics.

Kishigami and colleagues designed a content distribution system based on blockchain, which could guarantee the primitiveness of providers' contents [7]. Dennis and Owen presented a reputation system based on blockchain to guarantee that the users' reputation evaluation is based on real behavior rather than fabrication [8]. Ferrag and colleagues presented research challenges on security and privacy issues in the field of green IoT-based agriculture, in which they described a layered agriculture architecture, gave a classification of threat models, and discussed possible future research directions [9]. HM Al-Khateeb and colleagues wrote a book that the blockchain technology can be incorporated into new systems to facilitate modern Digital Forensics and Incident Response [10].

Rui An and colleagues came up with an anticounterfeiting system based on blockchain which writes information into an anticounterfeiting chip [11]. Qi Xia simply solved the access control problem in the medical data sharing system by designing a data sharing scheme based on blockchain to allow everyone read data from the data sharing system after identification [12]. Xu Ruzhi and colleagues presented a digital rights management scheme of network media based on blockchain to manage production, publication, and rights [13]. Liang XuePing and colleagues gave a decentralized and trusted cloud data origin architecture using blockchain to prevent data from being tampered with [14]. Li Zhaosen and Li Caihong presented an optimized data storage method for digital forensics [15]. Xu Lei designed a decentralized, verifiable, and antitampering system for cloud forensics [16].

Although many works have been done on data preservation, there is no model or method for digital forensics. So, the problem would be as follows:

(1) Low automation level in the process of data preservation

(2) High risk level in the process of data preservation

(3) Lack of safety guarantee of digital data

(4) Lack of mutual trust

Only by solving problems above, the courtrooms would admit the validation of the data, and if there is any possibility that shows the data might be manipulated, investigators would lose their credibility in court and basically it is not possible to come back from that over time.

Although many scholars have been in study with the data preservation method, there is not a safe, automatic, nonintrusive, and nonhuman-interventional way to preserve data.

3. Technology Background

This section gives an overview of relevant technologies for data preservation, which can provide background information sufficient to understand concepts and terms.

3.1. Blockchain. Blockchain is actually a distributed decentralized database providing Byzantine fault tolerance with distributed storage, consensus mechanism [17], peer-to-peer (p2p) network, encryption algorithm, and so on. Compared with traditional centralized database management, for example, by giving fully authority to read and write database to a company or administrator, blockchain allows any capable nodes to become a member of blockchain network because of decentralization and trustfree. Once a node becomes a member of blockchain network, it has the same authority to read and write database as other nodes, and all of the nodes maintain the network together. And all nodes in blockchain network synchronize each other's information through consensus mechanism to guarantee consistency and reliability of the data in blockchain network.

Nowadays, blockchain technology is most widely used in the field of finance, and lots of commercial banks, financial institution, and even governments are developing blockchain technology. The most popular blockchain technologies at home and abroad include Bitcoin, Ethereum [18], Ripple [19], and Fabric [20]; their main technical frames and work processes are basically the same; differences are in aspects of consensus mechanism, token mechanism, fault tolerance, and applied scenes.

Table 1 compares some main blockchain architectures while n represents the number of verification nodes.

According to Table 1, we can see that Bitcoin and Ripple both do not support smart contract, and smart contract is

Table 1: Comparison of some blockchain architectures.

Blockchain	Bitcoin	Ethereum	Ripple	Hyperledger
Architecture	Electronic encrypted currency system	Electronic encrypted currency system	Electronic currency settlement system applied for payment	Blockchain platform for commercial application
Type	Public blockchain	Public blockchain	Consortium blockchain	Consortium blockchain
Consensus algorithm	Proof of work (PoW)	Proof of work (PoW)	Ripple prove of consensus algorithm (RPCA)	Practical byzantine fault tolerance [21] (PBFT)
Fault tolerance	49%	49%	(n-1)/5	(n-1)/3
Smart contract [22]	Not supported	Supported	Not supported	Supported
Block generation time	10 minutes	15 seconds	3–6 seconds	3–6 seconds
New node and block synchronization	Adding nodes dynamically not supported and synchronization takes long	Adding nodes dynamically not supported	Adding nodes dynamically supported	Nodes cannot be added dynamically and breakpoint recovery
Privacy	Anonymity, unable to audit	Anonymity, unable to audit	Support privacy of individual transaction	Member service management, strong identity authentication, auditable
Other	—	Introduce turing-complete smart contract language	Introduce UNL trust nodes list	Pluggable consensus algorithm framework, electronic currency

very important in our model that the transaction could be executed trustfully without third party involved. With no smart contract, the blockchain could lead to trust problem in data preservation for digital forensics. And the Ethereum does not support audition which means the data preserved in the model could not be checked by court when necessary. So, we choose Hyperledger, also known as Fabric, as the basic structure of the blockchain.

3.2. Hash. Hash is one kind of data digest technologies. It can transform inputs of any length into the output of fixed length by the hash algorithm, and the output is called hash value. Essentially, hash is a contractive mapping function, which means the space for hash values is usually much smaller than the space for input.

Hash is widely used for data preservation because it is nearly impossible to find the reverse law. When a hash function or a hash algorithm has the following characteristics, we say the function or the algorithm is safe.

(1) One-way calculation: for any given output, the original input cannot be calculated

(2) Anticollision attack: for any two different input information, the outputs are not equal after calculation

If the output length of a hash algorithm is n, the security complexity of one-way calculation is 2^n, and the complexity of anticollision attack is $2^{n/2}$. However, the conflict of hash cannot be completely prevented. A known conflict of CRC32 function is that you get the same output by input "plumless" and "buckeroo," which is shown in Figure 1. This means we need to figure out a way to minimize the collision rate of hash function which will be discussed in the next chapter.

To avoid the conflict problem in the hash algorithm, we replace hash with the multidimensional hash algorithm. The

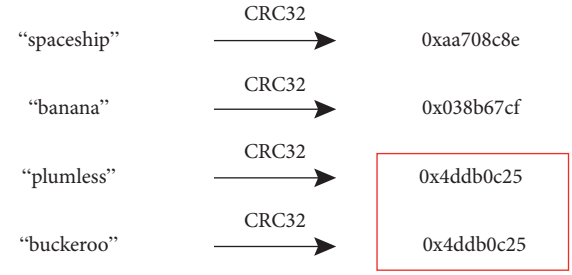


Figure 1: Conflict of CRC32 function.

regular hash algorithm turns the target content into a sequence, while the multidimensional hash turns the target content into a multidimensional group of sequences. Taking regular hash and two-dimensional hash as examples, the transfer progress is shown in Figure 2. With n-dimensional hash, the conflict rate drops rapidly to one 2^nth of the original value.

3.3. Cryptography and Signature. Cryptography is one of the essential technologies when it comes to security. In data preservation, the encryption algorithm is also used, including symmetric encryption and asymmetric encryption algorithms like DES and RSA. Usually, the symmetric encryption is used for encrypting data to prevent others from manipulating, and the asymmetric encryption is use for signing the key to confirm that the data belong to someone or extracted from some device. In this way, the primitiveness of the data could be guaranteed well.

Digital forensics needs to deal with the whole data in target devices, which means there are plenty of types of data that needs complex and diverse storage types. Also, there is huge safety risk in the data storage, and centralized storage could not avoid tamper and loss problems that make the

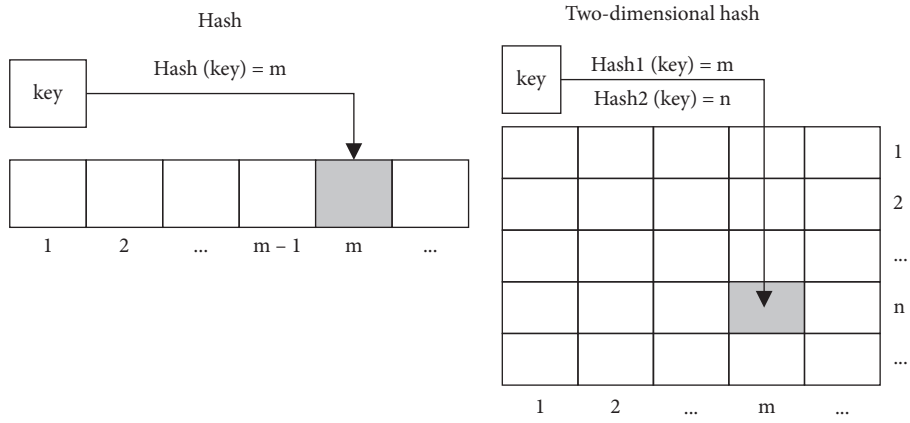


Figure 2: Hash table and two-dimensional hash.

system imperfectly reliable. Meanwhile, time of obtaining verification result is too long for user to get results in time. All of the above, we present a data preservation method based on blockchain and multidimensional hash to solve problems in data preservation for digital forensics.

4. Model

The developed data preservation models usually build one chain of evidence custody based on blockchain or cryptography, which might exist security risks of 51% attack. Once the attacker breaks the 51% attack barrier of blockchain technology, the whole data on the custody chain would be exposed and the data would be invalid.

Therefore, this article presents a new data preservation model consisting of two intersecting chains of evidence custody, one is main chain and the other is branch chain. Branch chain is established in the unit of case based on blockchain, and each process of the case generates a node on the branch chain. All head nodes of all branch chains form the main chain based on multidimensional hash. The architecture of the model is shown in Figure 3.

In Figure 3, the nodes 1–4 in branch custody chain represent data node generated after each operation on original data, and these nodes, together with other nodes, consist of a Merkle tree of a blockchain. The timestamps in main custody chain are the system time when the node is generated.

The advantages of the presented model are obvious. First, dual custody chains strengthen the digital data preservation and makes sure the data of different cases are separated and noninterfering. Second, attackers need to break through both main chain and branch chain to get data. Because data of different cases are all linked to the main chain, it is more difficult for attackers to locate the target data. Finally, if attackers break through both chains, they still have to decrypt the data and can only operate that data while other data are still safe.

4.1. Application Scenario. Before describing the presented model, we need to describe the application scenario of the data preservation model.

The proposed model can be transformed into an independent data security system in application, and the system is based on B/S architecture shown in Figure 4. After extracting data from target device, the original data are automatically packaged and sent to server for further process and redundant server for back-up. And the branch chain server hashes the data and other information to get the hash set, and the hash set is used to build a blockchain as a branch chain. All the head nodes of branch chains constitute the main chain after processed by cryptography in chronological order.

4.2. The Branch Chain Based on Blockchain. Compared with other blockchain platforms in architecture design, computing power, application scenario, and contract support in Table 1, as a consortium blockchain, Hyperledger (also known as Fabric) could support application better, so we choose Fabric as the basic blockchain architecture. However, Fabric does not support adding nodes dynamically, so we first need to solve that problem.

4.2.1. Dynamic Addition of Network Nodes. The current Fabric could work well while number of verification nodes is fixed, but the network expansion performance is poor. While there is a new verify node needing to join the network and participating consensus, Fabric needs to cut off all consensus activities of all active verification nodes, updates profile information and new node information uniformly in verification nodes, and then restarts message broadcast, process of blockchain transactions, and consensus services. Such circumstances are definitely not allowed in data preservation for digital forensics. When the consensus activities of verification nodes are cut off, attackers could take advantage of this period of time to tamper the data, which would lead to the loss of data originality and validity. Under these circumstances, we need to come up with a solution to avoid the cut off of consensus activities.

Our solution, shown in Figure 5, is to treat dynamic access as a certain type of transaction. When there is a new node applying for becoming new verification node, the new

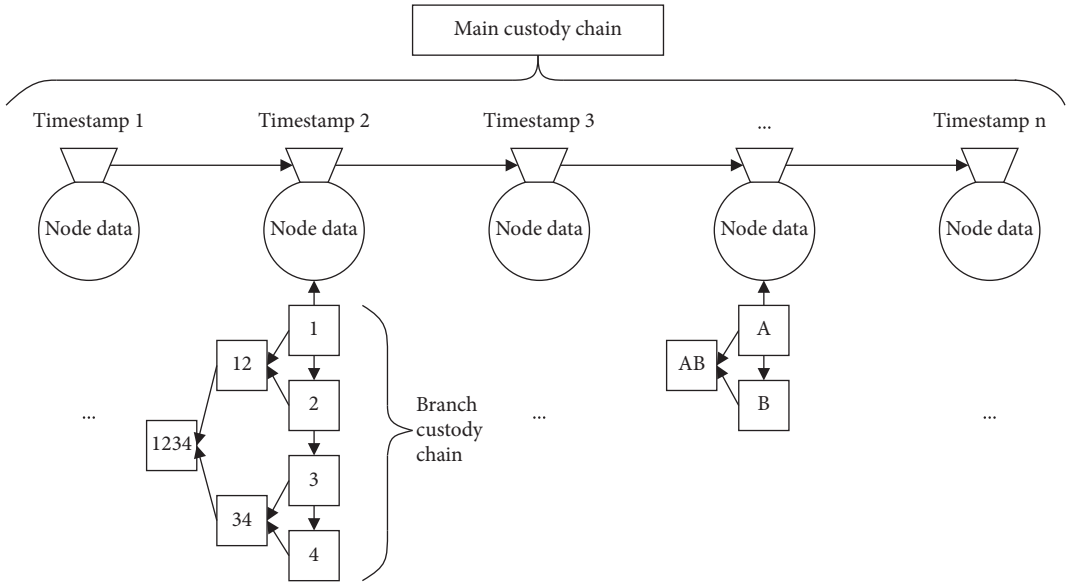


Figure 3: Architecture of the presented data preservation model.

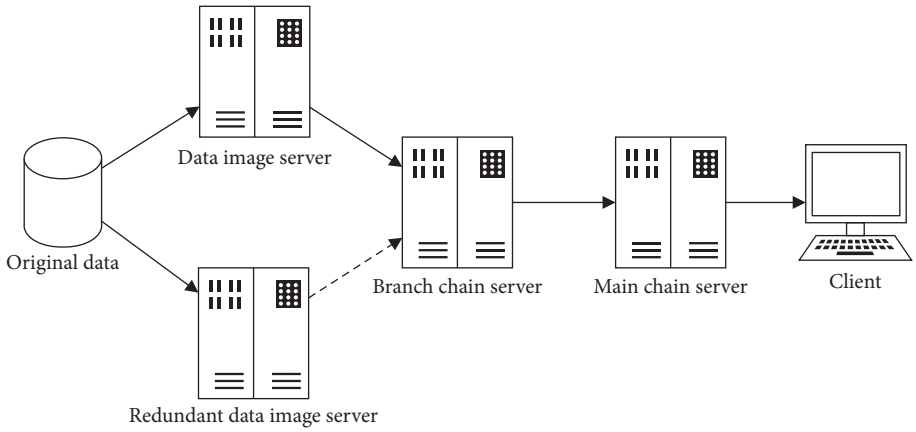


Figure 4: Application scenario for the presented model.

node should get registered and verified at the member service management node, and after that, dynamic join and quit of the new node are carried out by triggering the certain type of transaction.

According to Figure 5, the new node firstly registers and authenticates with member management node. After that the new node establishes a link with traction node to communicate with others. Then, the new node sends the addition transaction information to a verification node to trigger consensus procedure. After consensus with other verification nodes, every node starts to update information of consensus module and rebuilds new broadcast module. In this way, the new node obtains the right to synchronize data, and after synchronization, the new node officially joins the blockchain network.

4.2.2. Procedure of Building Branch Chain. The whole process is shown in Figure 6.

In order to bind the data with the device more closely to prove the primitiveness of data, the model needs more information including unique identification information of the device, user identification information, and operation information than just data and timestamps.

First, hash the data to get $h_1(x)$, obtain the unique identification information like MAC address or IMEI number, timestamp, current user, and operation information, and combine $h_1(x)$ and all these information into a string. According to the actual situation of storage device and security needs, choose the number of hash algorithm's dimension and calculate to get a hash value set. The data then are stored in the data image server taking the hash value set as addresses.

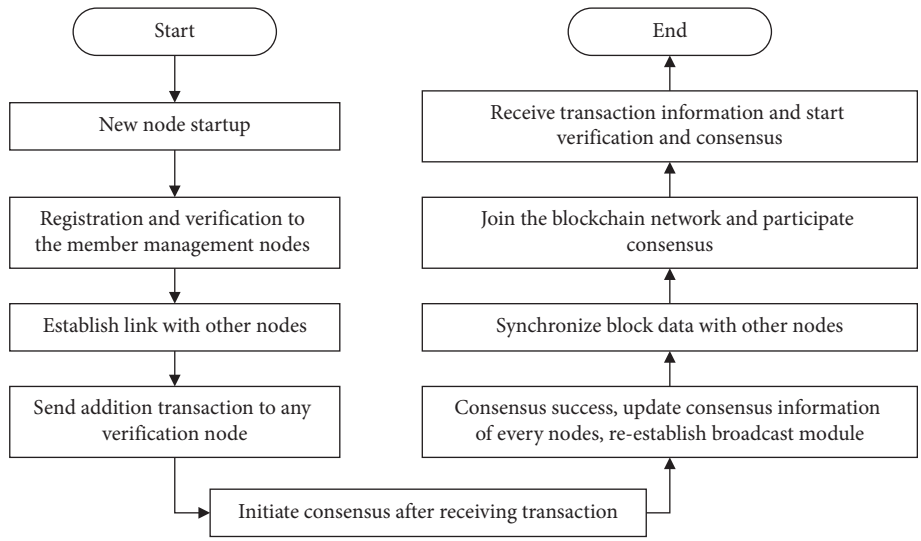


Figure 5: Process of dynamic addition of new verification node.

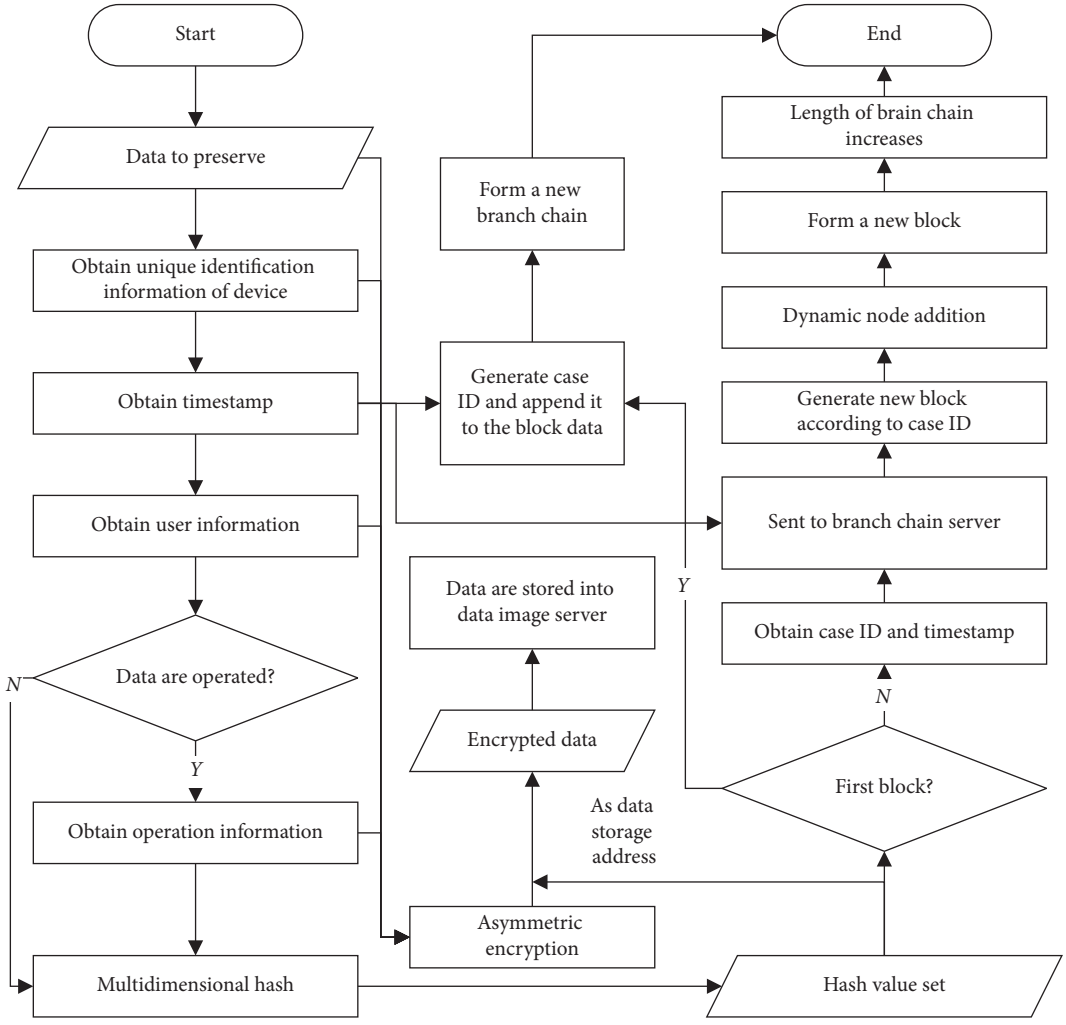


Figure 6: Process of building branch chain.

Second, the hash value set is sent to the branch chain server as the data of a new transaction, and then after verifying the authenticity and validity, the nodes would take the data to create a new node on the blockchain.

Third, if the node represents a brand new case, a case ID according defined rules is generated and timestamp is obtained. The branch chain server will generate a new blockchain according to the case ID and timestamp and then the new node is appended to the new blockchain. If the new node belongs to an existed case, the case ID and timestamp would be obtained to confirm which blockchain the new node should be appended to.

Finally, when the new node enters the blockchain network, the dynamic node addition scheme is triggered. The node finally becomes a node of a certain chain.

4.3. The Main Chain Based on Multidimensional Hash. The building process of main chain is shown in Figure 7.

From Figure 7, we can see that the case ID and timestamp information is firstly extracted from first blocks of existing branch chains. And the multidimensional hash is applied to get a hash value set. Then, a random key is generated to encrypt this information, and after encryption, the information is stored according to hash value set. The Public Key Infrastructure is used to protect the random key and execute digital signature. After all these, the hash value set and encrypted random key are combined and form a new node appended by a timestamp. Finally, the new node is inserted into the main chain in chronological order by the timestamp.

To illustrate the benefits of multidimensional hash, we analyze the conflict rate, failure rate, and storage efficiency.

We suppose that $H(x) = \{h_1(x), h_2(x), \cdots, h_n(x)\}$ is a n-dimensional hash function and the conflict rate of its one-dimensional hash function is $\{\beta_1, \beta_2, \ldots, \beta_n\}$, then it can be concluded that the conflict rate of the n-dimensional hash function is as follows:

$$\beta_N = \theta \prod_{i=1}^{n} \beta_i, \tag{1}$$

where $\theta \in [1, (\prod_{i=2}^{n} \beta_i)^{-1}]$ is adjustment coefficient, and, which is determined by the similarity between hash functions. From formula (1), the conflict of n-dimensional hash is $10^{2(n-1)}$ or $10^{4(n-1)}$ smaller than that of one-dimensional hash.

The failure rate is related fill rate and conflict rate. We suppose that the fill rate is α and the conflict rate is β_n, then the failure rate is

$$\delta = \alpha + (1 - \alpha)\beta_n. \tag{2}$$

If the fill rate of the one-dimensional hash is also α and conflict rate is β_1, then the failure rate is

$$\delta_1 = \alpha + (1 - \alpha)\beta_1. \tag{3}$$

We can get (4) with (2) and (3).

$$\delta_1 - \delta = (1 - \alpha)(\beta_1 - \beta_n). \tag{4}$$

Since $0 \le \alpha \le 1$ and $\beta_1 > \beta_n$, $\delta_1 \ge \delta_n$. Only if $\alpha = 1$, $\delta_1 = \delta_n$, which means n-dimensional hash has better performance in failure rate.

The storage efficiency could be measured with average storage time, and the average storage time could expressed as

$$t_a = t_h + t_s, \tag{5}$$

where t_h is calculation time of hash value and t_s is the actual access and storage time. If the failure rate of one-dimensional hash is δ_1, then the average storage time would be

$$t_{a1} = t_h + t_s + \delta_1 t_s. \tag{6}$$

And the average storage time of two-dimensional hash would be $t_{a2} = 2t_h + t_s + \delta_2 t_s$. Since we already know that is $10^2 \sim 10^4$, smaller than δ_1 from formula (1) and supposing that $t_s = 5t_h$, we can get that

$$t_{a1} = t_h + t_s + \delta_1 t_s = t_h + (1 + 2000\delta_2) \cdot 5t_h = (6 + 10000\delta_2)t_h, \tag{7}$$

$$t_{a2} = 2t_h + t_s + \delta_2 t_s = 2t_h + (1 + \delta_2) \cdot 5t_h = (7 + 5\delta_2)t_h. \tag{8}$$

Combining with the analysis before, we can get $0.99 \le (t_{a1}/t_{a2}) \le 15$, which means two-dimensional hash's average storage time is 99% of one-dimensional hash's in the worst case, and in the best case, the number is 1500%.

5. Evaluation

As described before, we selected Fabric as the basic blockchain architecture, and the version is v0.6.0-preview. And the experiments were run on a 16-node commodity cluster. Each node has a core-i5-3365 3 GHz CPU, 16 GB RAM, 1 TB hard drive, and running windows 7 and connected to the other nodes via 1 GB switch.

First, we do some coding on Visual Studio 2010 to test the dynamic addition of nodes, which is shown in Figure 8.

Since the model is used for data preservation, we focused on the fault tolerance and security of the model. To evaluate how resilient and reliable the model is to crash failures, we run tests on Fabric compared with Ethereum and Parity and on two-dimensional and three-dimensional hash compared with C# hash table function.

Figure 9 shows the blockchain forks caused by attacks. The attack essentially creates network partition at 100^{th} second that lasts for 150 seconds.

As we can see from Figure 9, Ethereum and Parity both fork at 150^{th} second, and the difference between number of blocks on the main chain and number of total blocks is getting larger as time goes while Fabric, on the contrary, has no fork because of the safety of its consensus protocol.

Then, we tested the conflict rate, average storage time, and failure rate of hash, which are shown in Figures 10–12. We select random 8 bit fixed long strings from 1 million to 50 million as input data and compare the performance of hash algorithms when fill rates are 0.5, 0.75 and 1.0.

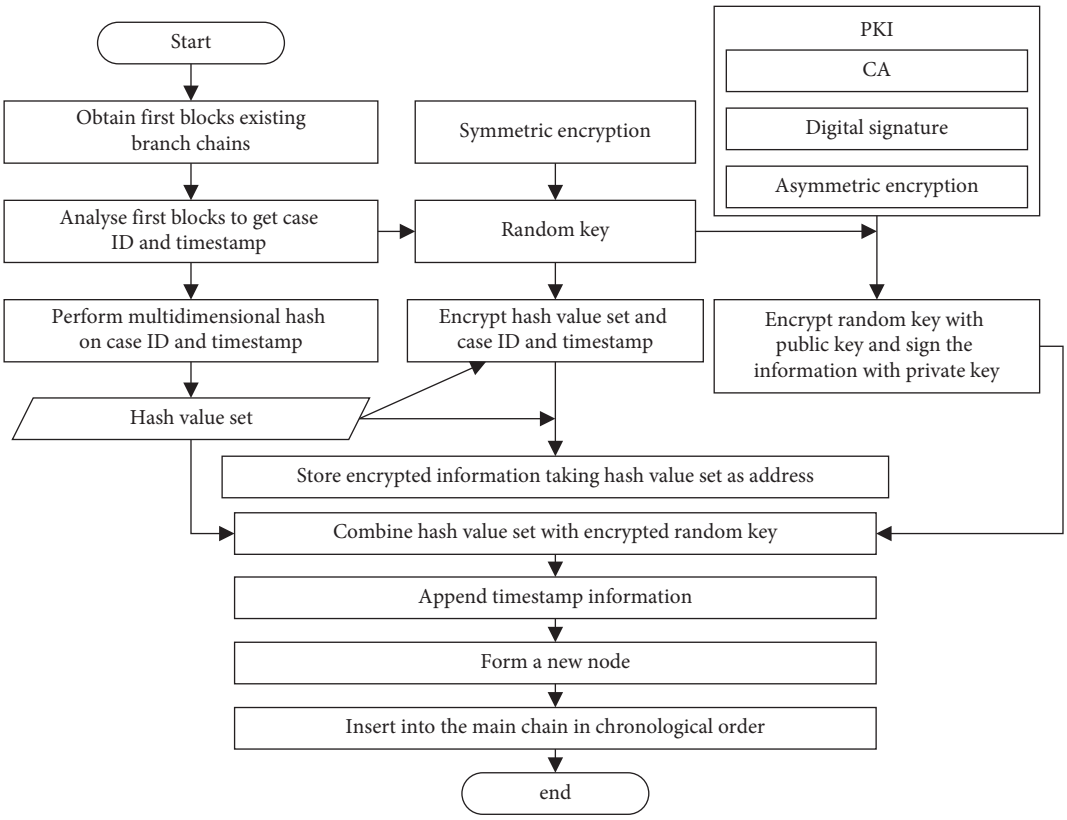


Figure 7: Process of building main chain.

It should be noted that the conflict rate is the inherent characteristics of functions and is not relevant to the fill rate. While in evaluation of failure rate, when the hash table is filled 100%, the failure is zero, so we do not need to test the failure rate when fill rate is 1.0.

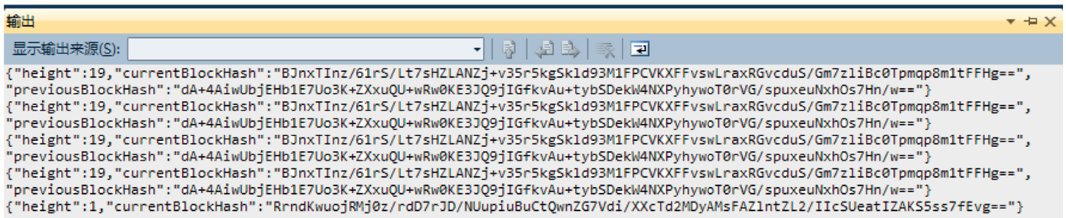
6. Discussion

Today, digital crime becomes more easy because of the powerful performance of smart terminals and such cases keeps coming all the time. Digital forensics is the technology to deal with this kind of situation. With today's technologies, it is not hard to get evidence from the terminals if it existed. While now in forensics, the problem is how to prove the primitiveness and validity of digital data. While the proposed model lays an important framework for data preservation, the model is only first step and is not all-encompassing.

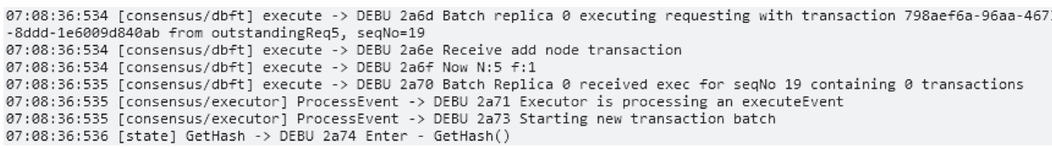
First, the presented solution is only a model, and lots of work needs to be done before the model is put into practice. In this article, we just give an architecture of the application scenario, but to develop and implement, the whole system still needs lots of work.

Second, we take Hyperledge Fabric as the blockchain architecture, but the Fabric is not designed for digital forensics, which means it cannot completely meet the need of data preservation for digital forensics. For further study, we will continue to design a customized blockchain to be more suitable for data preservation.

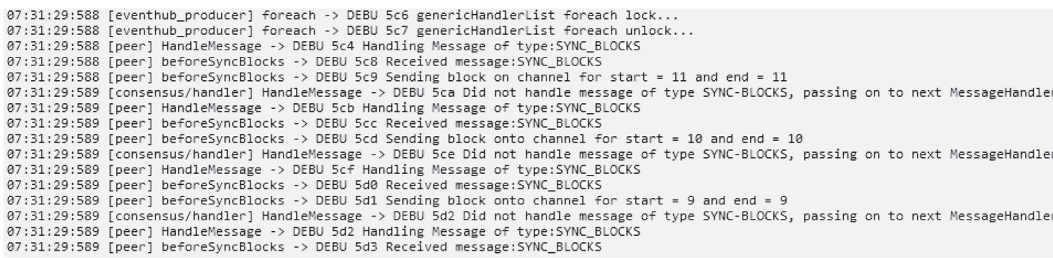
Third, the presented model encrypts data before being hashed, and as everyone knows, the encryption could take up lots of resources and time. The hard drive capacity of smart terminals is getting larger and larger; the data extracted from these terminals are also more and more. The encryption will be the bottleneck of this model. Under these circumstances, we need to continue our research in the partial encryption algorithm, by which we can just encrypt information we want instead of encrypting the whole data image. In this way, the model could be more practical.



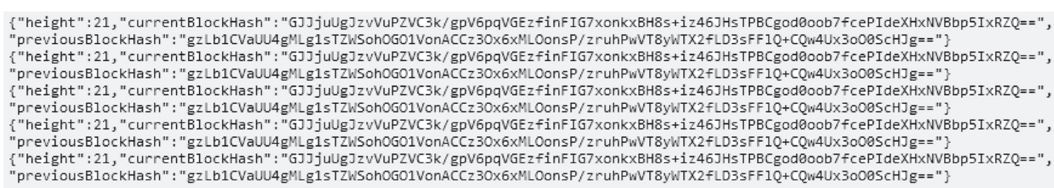
(a)



(b)



(c)



(d)

FIGURE 8: Process of dynamic node addition: (a) state before the now node joins the blockchain; (b) updating of node configuration; (c) block synchronization; (d) block synchronization completes.

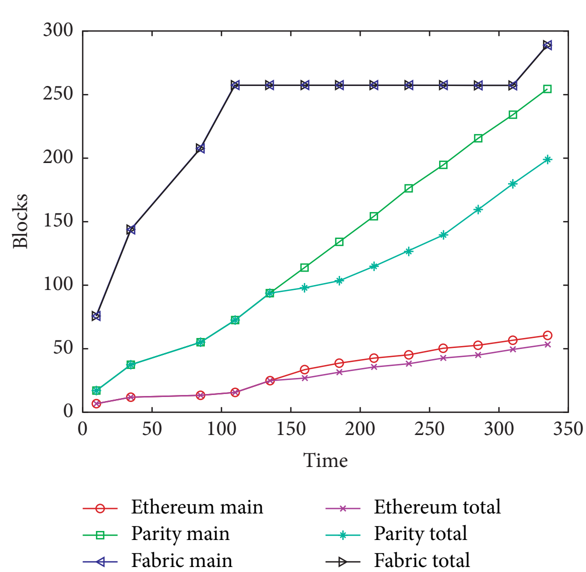


FIGURE 9: Blockchain forks caused by attacks.

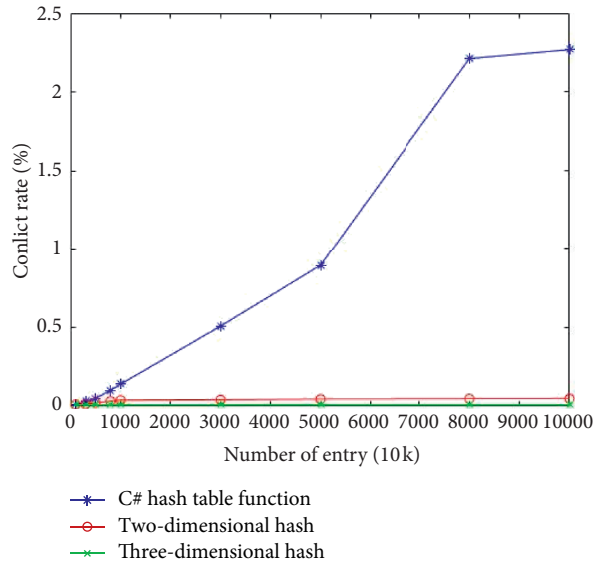


Figure 10: Comparison of conflict of two-dimensional, three-dimensional, and C# hash table algorithms.

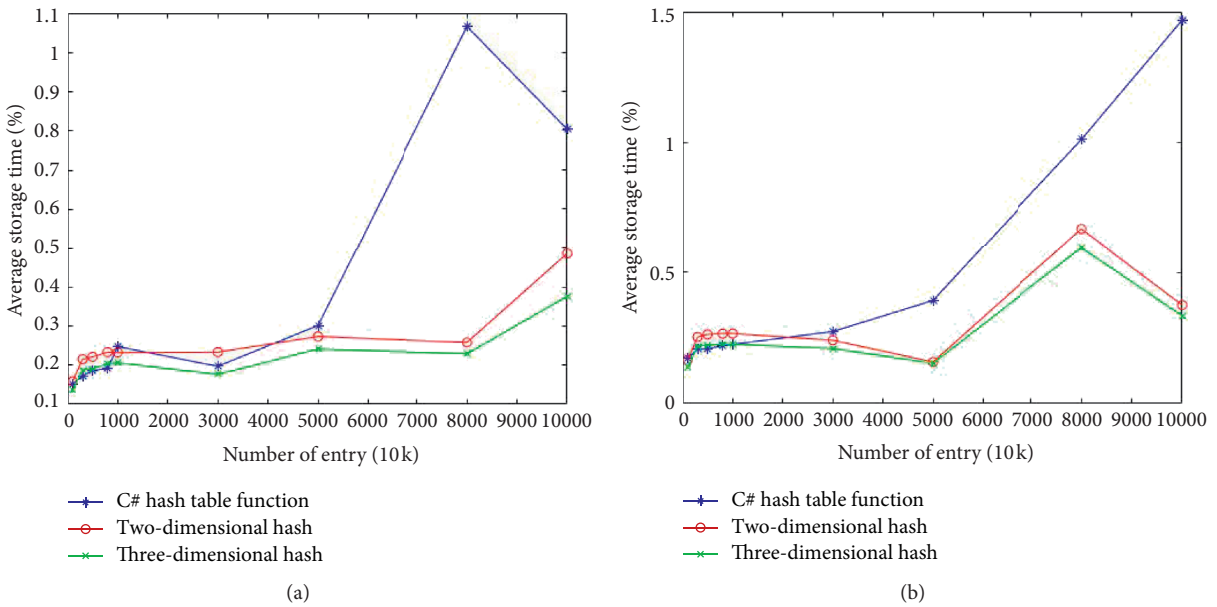
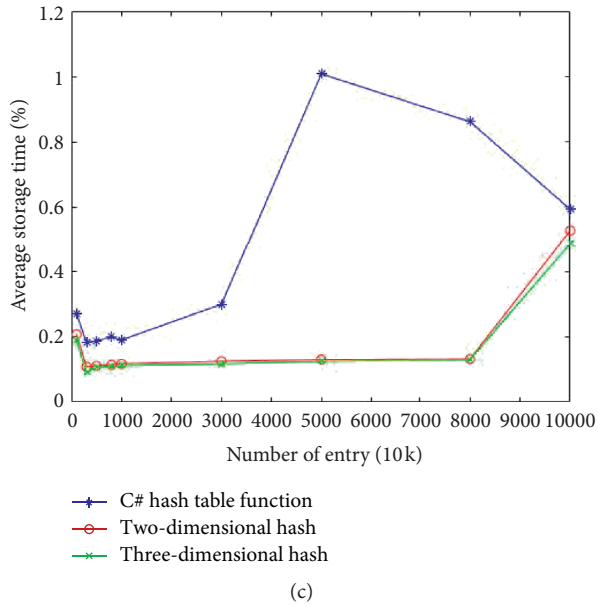
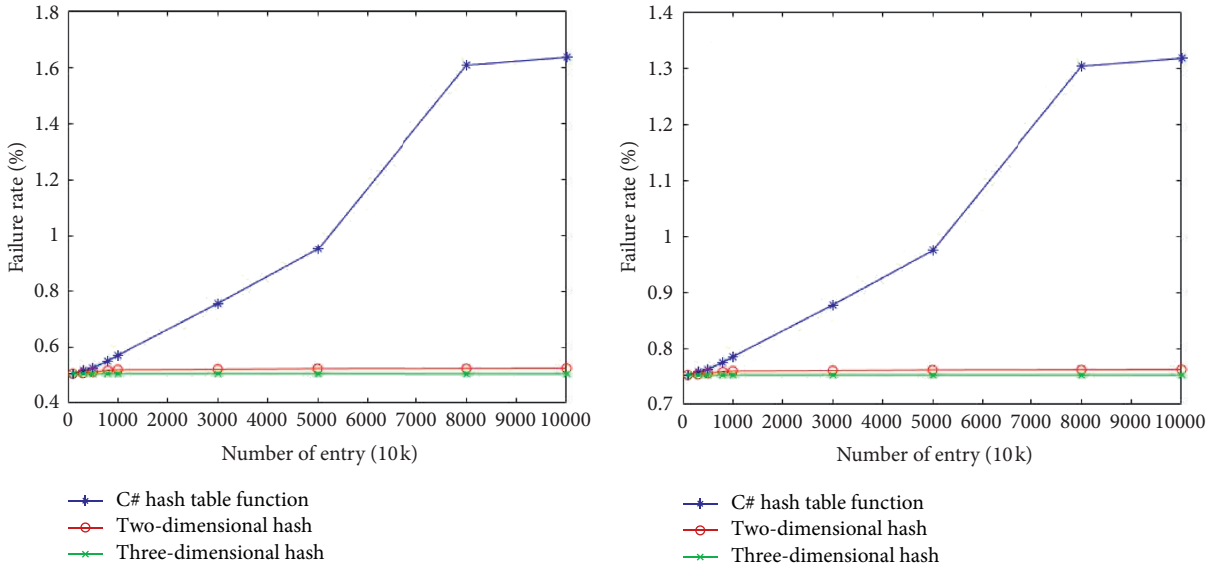


Figure 11: Continued.



(c)

Figure 11: Comparison on average storage time at (a) 0.5 fill rate; (b) 0.75 fill rate; (c) 1.0 fill rate.



(a) (b)

Figure 12: Comparison on failure rate at (a) 0.5 fill rate; (b) 0.75 fill rate.

7. Conclusion

With the digital forensics becoming widely applied in courtroom, there will be more and more questions about the primitiveness and integrity of the data. The investigators need more support of tools, models, and methods than just qualification certificate.

In this point of view, it is important to provide models, methods, and tools, which are qualified, to investigators to make sure the result of their work is valid. This paper presents a

data preservation model for digital forensics based on blockchain and multidimensional hash. While not all-encompassing, we hope that this work will inspire others to keep studying and presenting new and better models, which would ensure the validity of digital data.

Data Availability

The image data used to support the findings of this study have not been made available because the data are extracted from suspect's terminal of real case.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Kim, Y. Lee, and S. Lee, "Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices," *The Journal of Supercomputing*, vol. 74, 2017.

[2] R. V. Sudhakar and T. C. M. Rao, "Security aware index based quasi–identifier approach for privacy preservation of data sets for cloud applications," *Cluster Computing*, vol. 23, no. 1, 2020.

[3] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia Computer Science*, vol. 132, pp. 1243–1252, 2018.

[4] K. Ritz, L. Dawson, and D. Miller, "Microbial community analysis of human decomposition on soil," *Criminal and Environmental Soil Forensics*, vol. 24, pp. 379–394, 2009.

[5] Đaltur, Vahidin, and K. Hajdarevic, "Digital forensic investigation, collection and preservation of digital evidence," *International Burch University*, vol. 16, 2014.

[6] J. He, G. Liu, B. Zhao et al., "Ensuring the authenticity and non-misuse of data evidence in digital forensics," *Journal of Harbin Institute of Technology*, vol. 22, no. 1, pp. 85–90, 2015.

[7] J. Kishigami, S. Fujimura, and H. Watanabe, "Etc. The blockchain-based digital content distribution system," in *Proceedings of the 2015 IEEE fifth international conference on BigData and cloud computing*, pp. 187–190, IEEE Computer Society, Dalian, China, August 2015.

[8] R. Dennis and G. Owen, "Rep on the block: a next generation reputation system based on the blockchain," *Internet Technology and Secured Transactions*, IEEE, vol. 10, pp. 131–138, 2016.

[9] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 1–23, 2020.

[10] H. M. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger," *Blockchain and Clinical Trial*, Springer, Berlin, Germany, 2019.

[11] R. An, D. He, Y. Zhang et al., "The design of an anti-counterfeiting system based on blockchain," *Journal of Cryptologic Research*, vol. 4, no. 2, pp. 199–208, 2017.

[12] X. Qi, B. S. Emmanuel, S. Abla et al., "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[13] R. Z. Xu, L. Zhang, H. Zhao et al., "Design of network media's digital rights management scheme based on blockchain technology," in *Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, Bangkok, Thailand, March 2017.

[14] X. P. Liang, S. Shetty, D. Tosh et al., "ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 468–477, IEEE, Madrid, Spain, May 2017.

[15] Z. Li and C. Li, "Research on application of electronic evidence based on blockchain," *Computer Engineering & Software*, vol. 38, no. 8, pp. 63–67, 2017.

[16] L. Xu, *Research and Implementation of Cloud Forensic System Based on Blockchain Technology*, Southwest University, Sichuan, China, 2017.

[17] D. Bo, *Design and Implementation of Distributed General Ledger Consensus Mechanism*, University of Chinese Academy of Sciences, Beijing, China, 2016.

[18] W. Gavin, "Ethereum: a aecure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 10, pp. 1–32, 2014.

[19] D. Schwartz, N. Youngs, and A. Britto, *The Ripple Protocol Consensus Algorithm*, pp. 1–8, Ripple Labs Inc. White Paper, San Francisco, CA, USA, 2014.

[20] Hyperledger Fabric [OL]..

[21] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages & Systems*, vol. 4, no. 3, pp. 382–401, 2002.

[22] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," *AI Matters*, vol. 1, no. 2, pp. 19–21, 2014.