2018 3(1) 13-19 Submission: 2018/05/10, Peer review: 2018/05/20, Accepted: 2018/05/25, Published: 2018/06/30

International journal of police and policing

Publication state: Japan
ISSN: 2423-8279

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: allee@cku.ac.kr

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/police.2018.3.1.13

ⓒ 2018 J-INSTITUTE

A Study on the Integrity Assurance of CRIME Digital Evidence

Lee Ae-ri

Catholic Kwandong University, Gangneung, Republic of Korea

Abstract

With advances in digital technologies, vast quantities of information have been processed and reported in a digital form. This has resulted in an increase in the scale and number of crimes related to digital information, and the relative importance of digital evidence in criminal proceedings has also increased significantly. In addition, it is a reality that such a huge amount of evidence is confiscated in a digital form at the crime scene and submitted to the court, but digital evidence is still not recognized as satisfactory proof due to its characteristics as well as insufficient legal and institutional support. Likewise, although the importance of digital evidence continues to increase, there is still a lack of research on the technologies and procedures to ensure integrity, such as the prevention of forgery and tampering with acquired digital evidence.

Since digital evidence is easily altered, tampered with or destroyed through improper handling, it has been faced with a challenge of securing the reliability of investigation and ensuring its integrity. Therefore, it is required to devise measures to ensure the integrity of digital evidence so that digital evidence can be accepted as legally valid in court. In this regard, this study proposed a method to guarantee the integrity of digital evidence by using blockchain technology that allows all nodes in the network to share distributed database securely without the use of a central server, and thus can prevent the forgery and tampering with data. The use of this method is expected to reduce the time and cost burden, while ensuring a high level of integrity.

[Keywords] ***Policing, Digital Evidence, Integrity, Blockchain, Crime***

1. Introduction

In recent years, the rapid development of information and communication technologies has led to the digitalization of information at an accelerating rate, and thus the scale and frequency rate of crimes related to digital information has increased accordingly. As digital forensics become common in cybercrime investigations, an interest in digital evidence is also increasing, and electronic evidence confiscated in a digital form at the crime scene is increasingly presented as important evidence at a trial.

Digital evidence is probative information that is stored or transmitted in a digital form. Therefore, digital information plays a very important role in identifying allegations of all crimes, and its importance will further increase in the future. Digital evidence, however, has not yet been recognized as satisfactory proof in the court due to its characteristics as electronic evidence which is fragile and can be easily deleted, tampered with or destroyed unlike physical evidence. Accordingly, there is a need for a method that can ensure the integrity of digital evidence which is admissible in court.

This study seeks to investigate blockchain technology that can prevent the forgery and tempering with data in a way that generates a block in which information on all of the transactions that occur within a certain period of time is recorded, transmits the generated block to all computers connected to the blockchain network instead of a central server and shares it with them, and to propose a method to guarantee the integrity of digital evidence.

2. Related Studies

2.1. Digital evidence

As shown in the following The precise conceptualization of digital evidence is not yet complete, but it refers to information reliable enough to stand up as evidence in court that is either stored in a computer or on digital storage media, or transmitted over a network[1]. In other words, digital evidence is information that is either stored in a computer or on digital storage media, or transmitted over a network, and it is evidence that is necessary for criminal investigations and prosecutions[2].

Unlike general physical evidence, digital evidence is characterized by non-visibility/non-readability, vulnerability(possibility of forgery)/ease of duplication(media independence), mass quantities, expertise, volatility and trans nationality. Digital evidence has characteristics that distinguish it from traditional physical evidence. Digital evidence includes six main characteristics[3].

1)Media independence: The independence of media in digital evidence means that the content of the original does not change even if it is transferred from one digital storage medium to another one, the value of the content is not changed although the identity of the entity is transferred to any digital storage medium unless the content stored in the original of digital evidence is transmitted or stored after being manipulated or altered, and the identity of digital evidence can thus be recognized.

2)Non-visibility/non-readability: It is evidence made of non-visible forms of 0 and 1, which are not visible to the naked eye.

3)Vulnerability(possibility of forgery): It is easily damaged, deleted and forged by mistake or on purpose, and it is difficult to find the deletion and forgery. Ease of duplication(media independence): It is easy to create the duplicate that is the same as the original, which is difficult to distinguish.

4)Mass quantities: When a large-scale server system or a file server is the subject of investigation, the amount of data to be collected and analyzed is enormous.

5)Expertise: The collection and analysis of digital evidence requires professional skills and needs a forensics expert.

6)Trans nationality(network association): In the current digital environment, digital evidence is being transmitted across the walls of a space because each computer is connected to one another through various networks including Internet rather than being isolated As a result, there are characteristics regarding the extent to which the law enforcement over domestic jurisdictions is recognized and the issue related to sovereignty when crossing national borders[3][4].

As such, it is often difficult to apply the conventional process of collecting and analyzing traditional evidence to digital evidence due to the above characteristics[5].

2.2. Digital evidence considerations

Digital evidence with characteristics distinct from those of physical evidence can be used as evidence in criminal proceedings only if it meets the requirements of authenticity and integrity as evidence. In this case, the authenticity of digital evidence is in the same vein as the formal and practical authenticity of physical evidence. The integrity of digital evidence should be preserved so that there can be no improper alternation, modification and damage of digital evidence in the process of being collected from the original, stored and analyzed, and this should be verifiable[6]. In order to use digital evidence in a criminal action, special precautions need to be taken from the generation of the original by the actor to the collection and analysis during the investigation process as well as the presentation of evidence in court. Therefore, the probative value of digital evidence cannot be recognized unless technical issues such as authenticity and integrity are resolved[7].

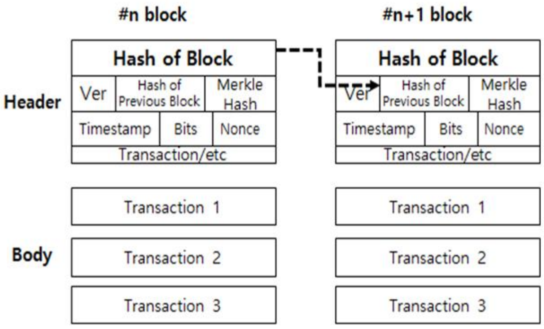
2.3. Blockchain

Blockchain is a P2P(Peer to Peer) distributed ledger technology, which distributes and shares transaction details to and with all participants in a blockchain network, rather than managing them in a centralized server. As participants manage the transaction details distributed to the P2P network, participants in the network can jointly record and manage them, and they can verify the forgery and falsification of transaction details through the chain of blocks. Users(nodes) participating in the Bitcoin blockchain create transactions and sign the transactions with their private keys[9]. The created transactions are broadcasted and transmitted to other users, and the transactions are generated as one block through a specific agreement algorithm in the settlement process. The generated block is connected to the existing blockchain, and the information of the block is broadcasted to other users. The users can confirm the integrity and reliability of data between users without the use of a central system based on the information of the blocks connected to the blockchain. The blockchain uses hash functions and data chaining techniques to provide data integrity. It also uses public key-based digital signatures to ensure the reliability of data[11].

The block of blockchain consists of a header and a body. The body of the block is composed of transactions, and the block header is composed of the block's own hash, the hash of the previous block, a Merkle tree and timestamp. With respect to the transactions of the block registered in the blockchain network, the data cannot be forged and modulated due to the hash of the previous block contained in the block header. The block structure of the blockchain is shown in<Figure 1>[10].

The blockchain uses a P2P network in which each peer participating in the network must replicate the same file, and new data is propagated and verified through the network. However, it takes a long time and costs a lot of money to propagate and verify the data through the P2P network. Therefore, a larger data structure can be checked safely and efficiently by allowing the Merkle tree to transmit only the hash value of data instead of sending the data and the receiving peer to check the hash value of the root hash of the Merkle tree. In addition, the integrity of data is also ensured. The Merkle tree, also called a hash tree, is organized in the form of a binary tree, and all peers/nodes must have the same legitimate and unaltered data which is not damaged. If the data is changed in one node, all nodes participating in the blockchain network must be informed of the change[8].

Figure 1. Blockchain block structure.

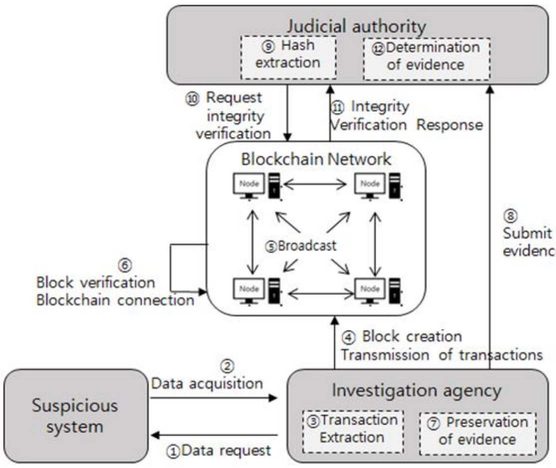


The blockchain work flow has five steps which include transaction definition, transaction authentication, block creation, block validation and block[10]. Transaction definition is the model of the transaction pre-defined by the blockchain network, and the sender's digital signatures, the transaction payload and receiver's public key are cryptographically signed with the sender's digital key. Transaction authentication is the process by which the nodes validate if the user A has the asset, enough balance to send the asset and is authenticated to move the asset. Block creation is the process of creating blocks by node from the transaction pool where transactions are grouped together based on the creation time. Block validation is the process of validating the blocks by checking if there is previous hash and nonce which provides the proof-of-work. Block chaining is the process of adding the blocks to the blockchain once the nodes reach a consensus[12].

3. Proposed System

This chapter presents a way to prevent the integrity of digital evidence from being damaged in the investigation process and proposes a method based on the blockchain technology that can detect the forgery and falsification of digital evidence through distributed blockchain nodes without the operation of the central authentication system. The proposed framework operates through a connection with the blockchain network that stores authentication and integrity verification information. The organization of each institution can be divided into the suspicious system to be investigated, the investigation agency that conducts investigations and collects actual evidence, the enforcement authority that exercises the powers of jurisdiction and the blockchain network that provides integrity. The composition of each institution and the procedure of the system are shown in <Figure 2>.

Figure 2. Proposed system.


Judicial authority
⑨ Hash extraction
⑫Determination of evidence
⑩ Request integrity verification
⑪ Integrity Verification Response
Blockchain Network
Node
Node
Node
Node
⑤Broadcast
⑧ Submit evidence
⑥ Block verification Blockchain connection
④ Block creation Transmission of transactions
② Data acquisition
①Data request
Suspicious system
Investigation agency
③Transaction Extraction
⑦ Preservation of evidence

The prevention of damage to the integrity of digital evidence is achieved through the blockchain network. The investigation agency with a seizure and search warrant collects information about the suspicious system, when the investigation agency broadcasts the collected evidence information to the blockchain network, thereby ensuring both the transparency of the investigation and the integrity of the digital evidence.

The blockchain creates blocks in which all transaction information generated during a certain period of time is stored and propagates the created blocks to members' computers connected to the network rather than to the central server, which makes it practically impossible to forge and alter the data.

The investigation agency extracts the transaction of evidence information and make a request for transactions such as the submission of the evidence information to the enforcement authority. The block is propagated through the steps of transaction definition, transaction authentication, block creation, block validation and block chaining to setup the blokchain. The investigation agency submits the evidence, and the enforcement authority requests the blockchain network to verify integrity and adopts the evidence if the integrity is verified.

The framework for ensuring the integrity of digital evidence proposed in this paper is composed of key generation and distribution, evidence collection, evidence registration and evidence adoption decision procedures, and the symbols and notations used are shown in <Table 1>.

Table 1. Notation.

Notation	Description
IA	Investigative agency
JA	Judicial authority
ID_{IA}	Investigative agency(Investigator) ID
CN	Case number
TS	Target(suspicious) system
SI	Suspicious system information
DI	Digital evidence profile
TS	Time stamp
PI	Digital evidence profile
H()	Hash

1)Key generation step

For private key generation, a random number generator is used to generate pairs of 256 random numbers. The each random value becomes the user's private key and has a length of 256 bits per key. The user obtains the hash value of the user's private key to make a public key. The hash values of 512 generated by the hash function become the user's public key.

2)Evidence collection step

The investigation agency confiscates a digital data source which is suspected of being involved in a criminal offense from the suspicious system, when an investigator should use a certified forensics tool as shown in the process of ①~③in <Figure 2>.

Using the forensics tool, the investigator analyzes digital data involved in the suspicious system and collects digital evidence. In order to guarantee the integrity of the digital evidence, he or she generates an identifier, extracts the system information, creates the profile of digital evidence to which the collected identifier is applied, and uses it as a transaction of the digital evidence.

First, the transaction for the extracted evidence is defined. The definition of a transaction is the transaction model pre-defined by the blockchain network, and the sender's digital signatures, transaction payload and receiver's public key are encrypted with the sender's digital key.

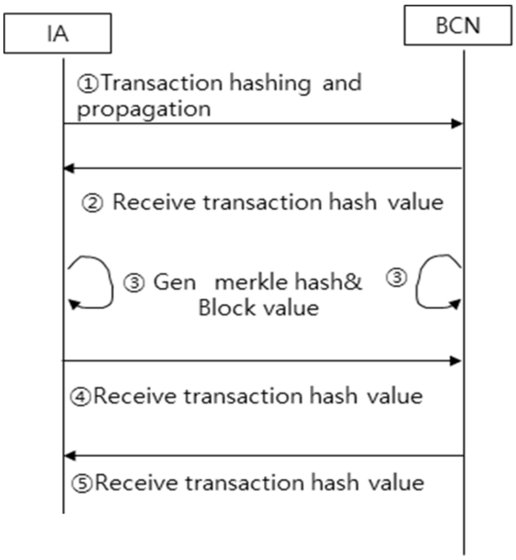
The investigator logs onto the suspicious system(TS) through a forensic program and collects system information(SI), when the collected information uses H/W and S/W eigenvalues that can identify the suspicious system. The investigator then uses the SI to generate case number(CN). He or she also generates Timestamp used as the digital evidence collection point and the standard time of the current forensics system.

The investigator collects the digital data from the TS and generates the DI. Then, he or she creates the PI using the collected DI and the stored CN and uses the SHA-256 hash algorithm to create a hash value, when the PI records the profile information of the digital evidence.

3)Evidence information registration step

The step of evidence information registration corresponds to the process of ④~⑥ in <Figure 2>. In this process, the transaction for the extracted evidence information is propagated, verified and added to the blockchain <Figure 3> shows the procedure for this step.

Figure 3. Evidence information registration step.


IA
BCN
①Transaction hashing and propagation
② Receive transaction hash value
③ Gen merkle hash& Block value
③
④Receive transaction hash value
⑤Receive transaction hash value

- The investigation agency transmit the transaction extracted from the digital evidence in the previous step to each node connected to the blockchain network.

- The transaction is broadcasted to blockchain network.

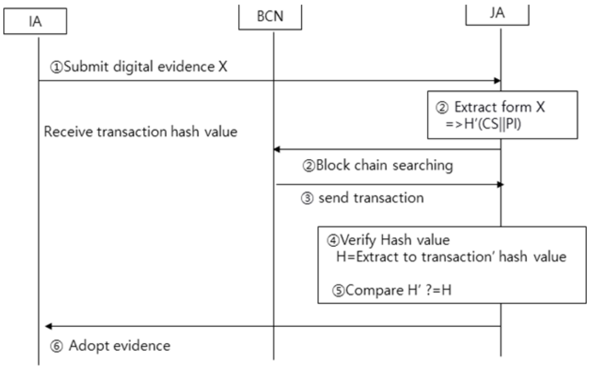
- The nodes of the blockchain network receive the transaction value of evidence in formation.

- The nodes generate the root hash value by creating the Merkle tree with the hash value of the transmitted transaction. The completed hash value is used in the header for block creation. The block is created by performing the proof-of-work until the desired range of hash values is obtained using the SHA-256 hash algorithm.

- If the node completes the block creation first, it informs the other node that the block creation is completed. If another node completes the block creation first, it receives nonce and timestamp value when the block is generated from another node.

- Each node verifies the hash value of the block by using nonce and timestamp value received from the node that generated the first block. If the first generated block is not a normal block, it is not registered. In this case, the block creation is performed again.

Figure 4. Evidence adoption decision step.


IA
BCN
JA
①Submit digital evidence X
② Extract form X =>H'(CS||PI)
Receive transaction hash value
②Block chain searching
③ send transaction
④Verify Hash value H=Extract to transaction' hash value
⑤Compare H' ?=H
⑥ Adopt evidence

- If the validation is successful, pending transactions in the transaction pool are grouped together, and blocks are created, propagated to other nodes, and added to the blockchain for storage and management.

4)Evidence adoption decision step

The process of ⑦~⑫in <Figure 2> is the step to decide whether to adopt the evidence submitted by the investigation agency. The investigation agency stores the transaction of the evidence information in the blockchain and then submits the evidence to the Judicial authority.

The Judicial authority extracts the hash value H'from the evidence submitted by the investigation agency and requests the blockchain network to verify the integrity. The node of the blockchain network retrieves the block in the blockchain and then extracts hash value H from the transaction. Later, the two values are compared and verified to confirm the integrity of the submitted digital information. If the verification is successful, the evidence submitted by the investigation agency is adopted, and if the verification fails, the integrity of digital evidence can be considered to be damaged. <Figure 4> shows the procedure for this step.

4. Evaluation of the Proposed System

The proposed system using blockchain has characteristics that propagate data such as the transaction value of digital evidence to all nodes connected to the blockchain network for storing and sharing them and thus prevents the forgery and falsification of the data. This gives a high degree of credibility to the proposed system. In addition, the proposed technique can reduce the risk of system hacking or server operating costs because it requires no separate cental server, unlike the conventional public key-based method which stores all data in the authentication system. In addition, it is possible to prevent the denial of nodes that register evidence information due to the characteristics of blockchain. In the previous systems, one hash value is used to prove one original data. However, in the proposed blockchain-based system, as authentication is done through a hash value corresponding to a plurality of hash values, not a one-to-one correspondence, security for digital evidence verification can be improved.

5. Conclusion

With the advent of the Fourth Industrial Revolution, the use of digital devices is further increased, and the phenomenon of information digitalization is being intensified. In addition, the amount of evidence confiscated in a digital form at the crime scene is increasing dramatically, and digital evidence is becoming a very important key to proving criminal allegations.

In this regard, this study proposed a method to ensure the integrity of digital evidence without the intervention of a central authentication server by using blockchain. The blockchain is a technology that creates a block that records all transactions that occur during a certain period of time, propagates the created block to all computers connected to the blockchain network instead of the central server, and thus can prevent the forgery and falsification of data. Therefore, the proposed technique using the blockchain guarantees a relatively higher level of performance compared to the previous techniques in terms of the possibility of hash value forgery and falsification of digital evidence, system hacking risk, operating costs and credibility. Therefore, it is expected that the use of the proposed technique can further strengthen the integrity of digital evidence, and digital evidence obtained through the improved procedures will bring about positive results in terms of integrity assurance, and the reliability and cost of investigation. In addition, the court is expected to make a more fair judgment through the digital evidence obtained in this way.

For the future research, there is a need to develop more practical systems that can verify the effectiveness of technical aspects through practical cases and allow investigators to use them with ease, and to outline the detailed directions of supporting policies.

6. References

6.1. Journal articles

[1] Kim JH & Jeong DW & Lee KH. A Study on the Integrity Assurance Process of Reliable Digital Evidence. *Journal of Security Engineering*, 10(5), 527-538 (2013).

[2] Gil YH & Un SK & Hong DW. How to Correct and Reliable Digital Evidence. *Digital Forensics Society of Korea*, 1(1), 147-161(2007).

[3] Seo KM & Chang KS & Kim GB. Integrity of Digital Evidence: Can We Prove Whether Its Integrity is Preserved?. *Journal of Digital Forensics Security and Law*, 7, 1-16 (2010).

[4] Jo SS & Shin YT. An Improvement on Integrity Assurance Processes for Digital Evidence. *Korean Institute of Information Scientists and Engineers*, 39(2), 184-191 (2012).

[5] Kim BS. Digital Evidence and Forensics. *Korea Association for Telecommunications Policies*, 21(6), 37-54 (2009).
[6] Lee IS. Digital Evidence Acquisition System. *Review of Kiisc*, 26(5), 37-43 (2016).
[7] Kwon OG. The Digital Evidence and Admissibility of Evidence. *IT & Law Review*, 5, 291-318 (2011).
[8] Kang JH. Preventing the Technology Leakage while Utilizing Digital Research Note Based on Blockchain & Showing the Remedy of How to Prove the Information of the Technology. *The Korean Journal of Security Affairs*, 7(1), 7-29 (2017).

6.2. Thesis degree

[9] Lee JJ. A Multi-signature Scheme for Security Enhancement of Blockchain-based loT System. Ajou University, Master's Thesis (2018).
[10] Thakur M. Authentication Authorization and Accounting with Ethereum Blockchain. University of Helsinki, Master's Thesis (2017).

6.3. Additional references

[11] www.bitcoin.org (2008).
[12] www.evry.com (2015).

Author
Lee Ae-ri / Catholic Kwandong University Assistant Professor
B.A. Semyung University
M.A. Semyung University
Ph.D. Myungji University

Research field
- Authentication Scheme for Smart Learning System in the Cloud Computing Environment, Journal of Computer Virology and Hacking Techniques, 11(3) (2015).
- Intelligent Digital Forensic Analysis Method for Cyber Crime Investigation, International Journal of Police and Policing, 1(2) (2016).

Major career
- 2014~present. Catholic Kwandong University, Assistant Professor.
- 2018~present. The Korea Society of Digital Industry and Information Management, Director.