Application of Blockchain Technology to Guarantee the Integrity and Transparency of Documents

Khuat Thanh Son†, Nguyen Truong Thang†, Le Phe Do††, and Tran Manh Dong†

† Institution of Information Technology, Vietnam Academy of Science and Technology, Hanoi, Vietnam
†† University of Engineering and Technology, Vietnam National University, Hanoi, Vietnam

Summary
This paper studies blockchain technology - which is getting strong attention from the industry and also being applied in many fields. Based on the nature of blockchain's data security, we analyze the application of blockchain technology to deal with the problem of data integrity and transparency for text documents. Firstly, the paper presents an overview of some technology components constituting to blockchain and its relevance and optimization to the data authentication/protection problem. Next, an experimental application of blockchain to form a network which stores documents and maintains the integrity and transparency of documents stored in the network for external queries.

Keywords:
Blockchain, hash table, peer networks, game theory, digital signatures, cryptography, ECDSA, SHA-265, documentation.

1. Introduction

Blockchain technology currently has started its establishment in many areas such as government, banking and finance, supply chain, e-commerce, hi-tech agriculture to IoT. Similar issues with stakeholder trust and data integrity have been identified in many industries [1-4]. Blockchain, a distributed ledger technology, is a potential solution to the problem of trust in numerous use cases [5-6]. Several organizations, particularly in the financial industry, have started to explore whether blockchain technology can be successfully integrated into existing software to address the need for a more visible and immutable audit log [7]. More recently, the use of blockchain for applications outside of currency and financial services has also received significant attention. Within healthcare, blockchain has been proposed as a possible solution for managing patient and provider identity, permissions to healthcare data, and to manage participant consent [8-10]. Indeed, it is undeniable that blockchain is being used more and more in every aspect of life, especially in the field of data and document authentication because its nature is about information safety and network security.

The blockchain research article gives potential applications in protecting the integrity and transparency of data. The paper first briefs through its core component technologies, analyzes the outstanding features of the technology compared to the existing tools with respect to the authenticity and transparency of document content, especially the texts of legal documents.

The rest of the paper is structured as follows: Section 2 presents fundamental components and the nature of blockchain. Sections 3 and 4 give more details about its encryption mechanisms via digital signatures, hashing functions and cryptography techniques. Section 5 is the key contribution of this paper as it describes an experimental application which can securely store text documents in a blockchain network while maintaining the integrity and transparency of document contents. Section 6 concludes the paper and points out further development from this stage.

2. Component Technology and Blockchain nature

Blockchain's ideas stem from the Byzantine general problem in computer science and reliable data exchange in a distributed network [11]. This idea was first proposed by Satoshi Nakamoto [12] in a distributed peer-to-peer network form which was implemented as a core part of a cryptocurrency system known as “bitcoin” in the form of open source called blockchain technology. Blockchain technology acts as a ledger for all transactions.

Blockchain is a technology that allows secure data transmission based on an extremely complex coding system, similar to a company's accounting ledger, where cash is closely monitored. In this case, blockchain is an accounting ledger operating in the digital domain. Blockchain owns a very special feature that the transmission of data does not require any intermediary (or third party) to validate information. The blockchain peer-to-peer network has many independent nodes (aka. mining machines) that can authenticate information without requiring a "sign of trust". The data once stored in a blockchain can not be changed and only be added with the consent of all nodes in the system. This is a high security and fault-tolerance system against the possibility of data

Manuscript received December 5, 2018
Manuscript revised December 20, 2018

theft and network faults. Even if some part of the blockchain network collapses, the remaining computer nodes will continue to perform normally to protect the data integrity and transparency.
Blockchain is said to be the combination of the three component technologies. Those are:
- **Cryptography:** Using public key and hash function to ensure transparency, integrity and privacy.
- **Peer-to-Peer Network:** Each node in the network is considered as a client and a server for storing application replicas.
- **Game theory:** All nodes participating in the system must comply with the rules of consensus and be motivated by economic incentives.

3. Digital signature and Cryptographic technology

3.1 Digital signature

The specifically electronic signature is the electronic signature used in blockchain, which is built on public key cryptography [13-14], also known as asymmetric crytography.

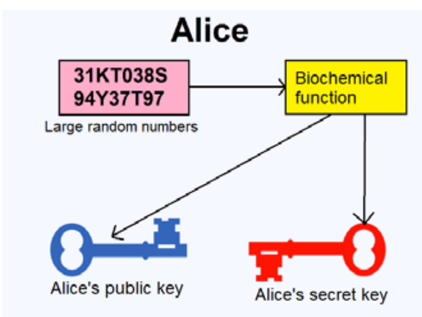

Fig. 1 Public encryption

The digital signature scheme includes the following components:
1. Set of clear texts M
2. Set of signatures S
3. Set of keys K for signature generation, set of keys K' for signature verification
4. Effective procedures for generating keys: $N \rightarrow K \times K'$, where K and K' correspond to sets of private keys and public keys respectively.
5. Procedures for generating signature: $M \times K \rightarrow S$
6. Procedures for verifying signature: $M \times K \times K' \rightarrow \{True, False\}$

Specifically, an electronic signature system consists of three algorithms:
- (sk,pk) := G(keysize) where G is a key generation algorithm.
- sig: =sign(sk,m) where sign is the signing algorithm. The function sign accepts a message m and a secret key sk input, then creates signature sg for message m under private key sk.
- verify (pk, m, sig) is the signature verification algorithm. This function takes a message m, a signature sg, and a public key pk as inputs. The algorithm returns true if sg is the signature of message m under the public-key cryptography pk, and false otherwise.

Our electronic signature system must meet the following two characteristics:
- The correct signature must be checked for the correct result: verify (pk, m, sign (sk, m)) = true
- The signature can not be forged.

In this paper, Python library is used to simulate the electronic signature scheme [15].

3.2 Cryptography techniques in Blockchain

Modern blockchain uses optimized cryptographic technology such as Elliptic Curve Cryptography (ECC) to ensure integrity for its components. Elliptic Curve Digital Signature Algorithm (ECDSA) was first introduced in 1991 from independent works by Neals Koblitz and Victor Miller [16]. Since the 2000s, the United States, Russia, Japan, South Korea and several European countries have researched intensively this area and made some standardizing efforts via international bodies such as ISO, ANSI, IEEE, SECG, FIPS. Among those, Russies is thought to be the most active country utitlizing ECDSA. In 2001, Russia introduced the GOST R34-10-2001 digital signature standard using the Elliptic cryptography with 256-bit key length. The latest Russian version of the digital signature is GOST R3410 in 2012 with a key length of 512 bits.

4. Hash function Sha-256, Role of the Hash Code in Blockchain

4.1 Hash function SHA [17]

SHA (Secure Hash Algorithm) [18] has been recognized among US standards in 1992 and is applied in conjunction with the DSS digital signature algorithm. This algorithm accepts a message M of any length as the input and delivers 160-bit long output. Blockchain uses SHA-256 hash function with the following characteristics:
- One-way function: That is, from the initial message, it is easy to create a hash value. However, from the hash value, there is no way to restore the original

message. The one-way function can be constructed on the basis of block cipher, e.g. F can be constructed according to the following formula:

$$F(X) = X \oplus E_K(X),$$

Here K is a fixed key number already known. For a lasting EK algorithm, the function is assumed to be a one-way function, because we do not know the vector formed by the output of EK.

- Collision resistance. It is difficult to find two different messages that yield the same hash results.

If either of these properties is violated, the hash function is no longer usable.

4.2 Role of the Hash code

SHA-256 hash function is developed by NSA and it is irreversible. This is actually used in BTC (bitcoin) [19] exploits as proof of the work algorithm and in the creation of BTC addresses thanks to its security. This paper mentions about the role of the hash in the blockchain network built in Section 5.

In blockchain, the current state-of-the-art hash function is considered to be safe due to the following analysis.

- Suppose a hacker wants to crack a private key of 256-bit length. That is, it must exhaust 2256 the possible cases of the key. A typical modern super-computers can perform 1018 key tests per second. So the hacking system must take 3x1051 year so that it can exhaust the searching space of the key.

Even in the worse case when the hacker is equipped with an extremely powerful super-computer which can handle the above searching space in only a day instead of 3x1051 years, blockchain network can withstand the attack by linking blocks together using a cryptographic hash function:

- Suppose the current block is A and its hash value "H_A".
- When a new block B is added to blockchain network, the miner's task is to calculate the hash value of the new block. This process is the solution to the PoW problem.
- To realize a link between A and B, the hash value H_A of block A is will be involved in the computation of the hash value for block B. The formula for computing the hash value of block B is as simple as: "H_B = hash (H_A + info_block_B + nonce) < target". Here, info_block_B is the transaction information in block B, nonce is the value to look for to solve the PoW problem, and target is the threshold to find the nonce value to satisfy the current difficulty.
- Because "H_A" joins the hash function to find "H_B", this is the link that constitutes the string in the blockchain structure. Therefore, if the hacker tries to change a transaction in block A, then he has to solve the PoW problem at block A, and find one or more new blocks with a valid hash value to replace block B. Obviously, it is a double-spending attack. By statistical analysis, the probability of this attack is arbitrarily small as the number of nodes in the blockchain network grows.

In the next section, the paper presents the application of blockchain to a specific problem, namely the integrity and transparency of text documents.

5. Experimental Application of Blockchain to Guarantee Document Integrity and Transparency

As Sections 3 and 4 mention, blockchain is based on the combination of 3 fundamental technologies, the use of the hash code [20] to link to the original data can be further extended. In a hostile environment, storing and linking large amounts of data enhance document and data security againts potential changes.

Blockchain data structure in each computer node in this experiment is implemented as a chain or linked list. The link between a block and its immediate predecessor is implemented by simultaneously storing a hash value of the previous block. If there is a change in the previous data structure, the hash value will be changed and the link will be broken. Such a structure is suitable for storing and linking data blocks that do not appear concurrently, which occurs in turn from time to time. Combined with the Merkle tree model, a sequence of data units can be linked together in chronological order. Thus a blockchain data structure always starts with an initial block called the genesis block. The data structure of each block contains the following fields:

- Index is used to store address of block based on type of input text. Different types of text will have different index codes. For example, a type of legal document will be indexed from PL01.1 to PL01.20, which will be indexed differently for search and retrieval
- Timestamp:
- Data:
- Nonce: 32 bits ensure that each block is used only once
- Previous hash value
- Hash code

For illustration purppose, Javascript is used as the programming language to simulate blockchain network. In the following case, the Nonce case will be removed because this paper does not deploy the mining algorithm. The hash array of the block selected by us is the SHA-256 hash function [21] created by combining the above domains. Firstly, a Structor Block with the above attributes is created. ClassBlock includes a constructor which is the block's property in the network and calculates the hash code for the block in the network.

The hash calculation formula for the next block is based on the hash function imported from the crypto-js library and uses the SHA-256 hash function. We also create a function calculateHash() which return the associated hash value of a input block. In terms of programming language Javascript, the hash function takes in each part of the block object, putting it into the SHA-256 function and converting it into a chain. In this part, we convert SHA-256 results into chains which are easier to deal with.

The calculateHash function takes every element in a block's data. As a result, if any piece of data is modified, the block's hash function will change the value immediately. This is a great feature to ensure data security in blockchain. Below is the code of the functions to build the next block and link ito a network of blocks.

Here is a block installed in the same way as the blockchain principle:

```
"chain": [
{
    "index": 0,
    "timestamp": "01/01/2018",
    "data": "KTS Blockchain demo",
    "previousHash": "0",
    "hash":
"4ef45213194435504cfb43d10eaec97edff57bb2353376d71ab
4f3bfcd09a4c9",
    "nonce": 0 },]
```

In the next part, we will conduct to test the use of that network for ensuring the integrity and transparency of a document. As a result of the above part, we can see that the blocks created are linked together according to the principle: the following block will connect to the previous block through PreviousHash. However, the important part is the data (where the data is stored without being encrypted). In this experiment, we conduct the data encryption with signatures based on the elliptic curve.

According to the Weierstrass formula [22], the elliptic curve E in the domain K is the set of points (x, y) $\in K_x K$ satisfying the equation:

$$y2 + a1xy + a3xy = x3 + a2x2 + a4x + a6$$
$$(a_i \in K \text{ và } 4a_4^3 + 27a_6^2 \neq 0)$$

Where an O point called point at infinity [23].

To set up the ECDSA signature scheme, we choose the elliptic curve E on the domain Fq with O being the infinity point, the base point G □ E and n is the degree of G (nG = O).

Possible attacks on ECDSA are classified as follows:

- An attack on discrete logarithm problem on an elliptic curve: this is a successful calculation way for opponent to calculate A’s private key from the parameters and Q’s public key. Then the opponent can forge A's signature on any selected message.
- Attack on the hash function. Ideal security: A t-bit hash function is considered to be ideal security if two conditions are satisfied simultaneously:
  - o Give a hash output, generate a reverse mapping (i)
  - o Create the conflict (ii)

SHA-1 is a 160-bit hash function and believed to have ideal security. The known method of the fastest attack is to exploit the properties of SHA-1 to find the conflict of SHA-1. So this takes 280 steps, attacking ECDSA in this way is calculated to be impossible. However, this attack imposes an upper bound of 280 on the security level of ECDSA, regardless of the size of the primary safety parameter n. Of course, this is also the case for all signature schemes with an existing appendix because only SHA-1 and RIPEMD-160 hash functions widely accepted are secure and practical. These are both 160-bit hash functions.

Because the documents needed to sign are usually long. One way for signing is to divide the documents into small chunks. Each chunk is then separately signed and those signed are reassembled into blockchain. However, the disadvantage of this method is that the signature is large. Furthermore, the signing speed is slow because the signing function is based on public key cryptography. In addition, the signature may not consider the page number within the document that may effect the integrity of the document. Therefore, the blockchain protocol need to sign to the hash value of the documents, because the value of the hash function always provides the specified length.

Based on the above mechanism, the following advantages are observed:

- Authenticity (Ability to identify the origin of digital signatures) (1)
- Anti- denial (No deny for responsibility) (2)
- Integrity (3)

→ The safety of the ECDSA signature scheme corresponds to the complexity of the discrete logarithm problem on the elliptic curve.

We now incorporate the encryption of SHA-256 into this data through library import:

```
const SHA256 = require('crypto-js/sha256')
const HASH256 = require('js-sha256/src/sha256')
```

The obtained result is a network of new blocks generated with the input data encoded in the HASH256 (index input) function and digitally signed in this data. In the next section, we will experiment with any input text data, use the SHA-256 hash function according to the formula proposed by this paper to calculate the number of blocks associated with each document. The output is then inserted into the blockchain network through the index attribute of Block Struct. The number of blocks will depend on the size of the input document.

6. Experiment and Evaluation

After establishing a blockchain, we will build up a blockchain network and a block struct is defined as in Section 5. Next, we will introduce the construction procedure of blockchain and the principle to validate the integrity and transparency of a data in the network.
According to Section 5, after a block has been created, we construct a set of structs in the block and each struct stores a page of text as shown in the following figure:

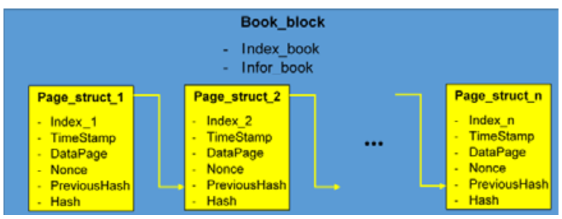

Fig. 2 Structure of a block

A Page_struct consists of the same components as those of a complete block, connected together through previousHash and a dimensional page_struct:

- Index: document page code with 8-bit length
- Timestamp: 18 bits
- Data: 256 bits (the contents of the page are encrypted, using the SHA-256 hash function)
- Nonce: 32 bits
- Hash value of previous block (PreviousHash) 256 bits
- Hash code: 256 bits

A book_block block is a set of multiple page_struct. To distinguish between different documents, we design two more elements index_book in the book_block in order to store the document code. We define this document code according to each different type of document (refer to classification in the National Library of Vietnam).

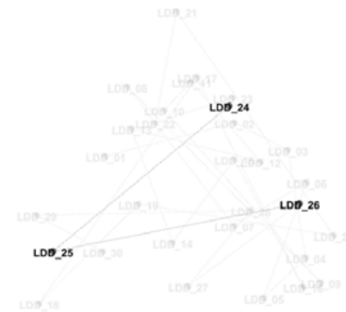

Fig. 3 Simulation of a book_block

As such, after having an input data, we encode and initialize a block with a size that depends on the number of pages and an average block of 500 pages has the size of about 20,121 kB.
After having created interconnected structs, we created a network of different struct strings connected through the previewHash code. As shown in Figure 4, one node is a page_struct with the full fields defined by us.

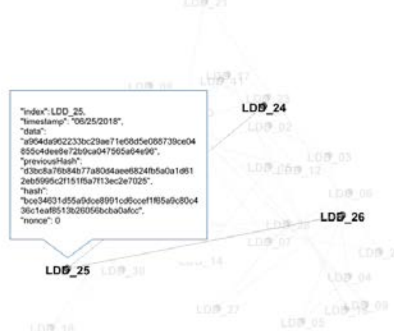

Fig. 4 Information about a node (page_struct)

As shown in Figure 5, when looking at the index, we identify that it is the page 25 of the LDD document, in which an initial date is 06/25/2018 and the data is encoded by the render_data function, preview_hash is the hash code of page 24, and the hash code is generated via the calculateHash function as we have stated in Section V.
After building the book_block, we created a network of book_blocks connected together. And the blocks are connected together into a chain of blocks called chains.

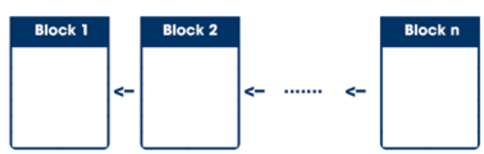

Fig. 5 Block chain

Based on the combined characteristics of the three technologies, Blockchain uses game theory to create equal credibility within the network, requesting the consensus of all the members in the network when making any change or modification to the Blockchain. Therefore, the information in Blockchain can not be changed. And if you want to add information, the consensus of all the nodes is requested. Even if a part of the new technology system falls, the remaining computers and nodes will still work to protect the information.

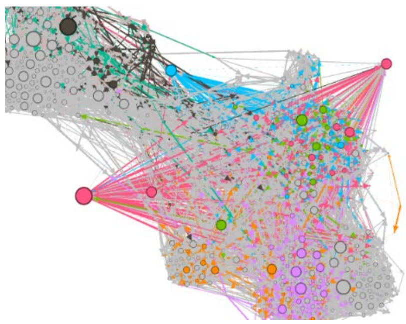

Fig. 6 Block network

More specifically, the transmission of data in Blockchain does not require intermediaries to confirm the information. This system consists of many independent nodes and has capability of high information authentication. Owning P2P technology [24], the communications within the Blockchain network does not pass through a particular server placed on a particular server; they are communicated across all network nodes in the network, which allows Blockchain to play a critical role in cloud data permission application as it allows anyone that work together save data in a equal and secure manner, even when they do not know each other. Then, instead of just saving files on a single internal traditional server, the data will be able to naturally saved to thousands and millions of devices in the world. Based on peer-to-peer computing [25], not depending on the credibility of anyone, but on the majority, along with encryption capability, Blockchain becomes a highly secure technology in many fields and particularly in ensuring the integrity and transparency of data.

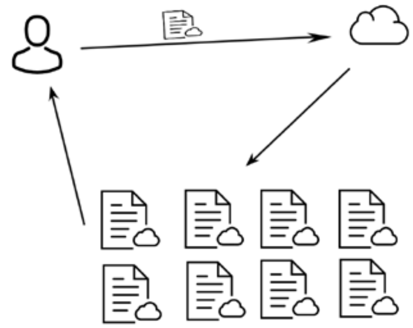

Fig. 7 Store data

The users use the system for two tasks:

- Importing original document
- Checking the integrity and transparency of any document

The user will import the original document. The user will push the document and the system will calculate the page number of the document and return the user full block sequence information including information as we have described.

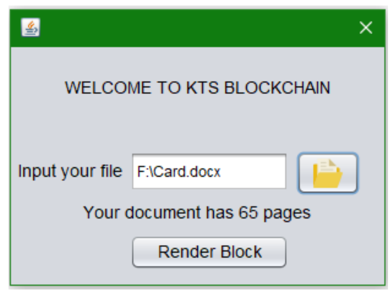

Fig. 8 Importing original document

Then the user will take the chain received on the Blockchain network, here we use the demo similar to the site https://blockchaindemo.io/. In addition to the information described, there will also be an index located at the block location on the block network.

Next, to authenticate any document, the user will perform the following steps to authenticate a document on the Blockchain network. The first step, the user will put the document to check integrity and transparency on the system, the system will hash data then check the index and check on the block sequence. The second step, the system will use the index of the hash document to check out the document on the block sequence. If the hash code of the user's document wants to be checked after the block network check that is 43.6% of the network nodes on the network, the user's text is acceptable.

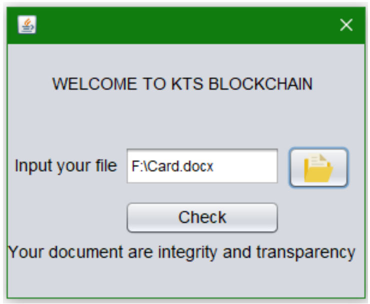

Fig. 9 Checking the integrity and transparency

Is Blockchain valid? true
"6b61c1a0f8f7ddee2c63bf47e6ae625d168a23c810fcfe40d31d9390011533dc"
Last hash of Blockchain:
6b61c1a0f8f7ddee2c63bf47e6ae625d168a23c810fcfe40d31d9390011533dc

And if there is a difference, i.e. the same percentage is less than 43.6%, the system will determine the deviation coming from which block. In this paper, we also use a function to check the accuracy of blocks in a chain (checkBlockchain), the system browses from the first hash value to the end of the chain and gives the index of the first difference block. This helps check the data change. If changing the text being only a space, the generated hash code will be different from the previously saved hash code. Here we use more a changed position check statement to give the exact position of the change.

If the text is modified, e.g. a space insertion on page 18 of a text, after re-running, we have the result that the user's chain is not the same as the original text originally uploaded and sends the message to the user:

Blockchain valid? true
"498ab519ed901d6c0df31496b31821b3c2650a78e25fb9c496d00a6910250e27"
Last hash of Blockchain:
6b61c1a0f8f7ddee2c63bf47e6ae625d168a23c810fcfe40d31d9390011533dc
Blockchain has been changed!
Document has changed at: Page 18

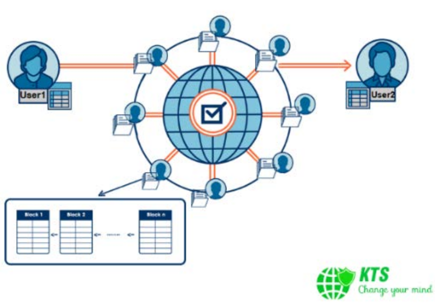

Fig. 10 Simulation of block network

Thus, according to the results obtained, we have created a network block. In particular, each different type of text will be attached to a different index based on the type of document, the number of years to release so that it can be easily retrieved later. This block network is used to authenticate one or more documents to verify that the text is accurate according to the original or modified text and, if so, providing a warning when the data change and showing where the change is located. The exact authentication is evaluated in the environment: a block network with 1326 blocks, archiving 101 documents with 08 different domains being about 97%. In this paper, we mention that there are many legal documents (decisions, circulars, etc.) currently being published on the Internet, but it is not possible to identify which type of documents is intact and not modified by even a space, and through the network block paper stated, we can indicate the authentication of the document to be examined.

In combination with hashing twice, we calculate and give the result if the attack occurs, the small ratio will go to about 0.00003136, combined with the signing of a number in the data stored in the block, the safety of each block decreases by the logarithm on the elliptic curve.

Combining with the peer-to-peer network and game theory that blockchain possesses, changing one part of the content is difficult and changing the whole document is harder, the probability to break the structure blockchain is 0.00002158.

According to the blockchain presentation, the blockchain network must be stored in different machines in accordance with the peer-to-peer network principle and there is the modification only when it is agreed upon in game theory, this change will be made. However, in this paper, we assume the formation of a network of computers that own blockchain technology as in Section VI.

7. Conclusion

In this paper, we presented the content relating to the blockchain: Analyzing the technologies that Blockchain uses, analyzing in depth the issue ensuring transparency and integrity of the data. We rely on the knowledge of technology in blockchain to create a simple block network, testing into an input data ientered through any file. However, in this paper, the application of blockchain is simply to ensure the integrity and transparency of document data and the blockchain network is still simple with a few computers, this makes the elimination of text can still be done without being detected. The development relating to blockchain technology is extensive, such as the construction of a system applicable to agencies and organizations in issues ensuring that the agency's materials are intact and used on the entire computer network to jointly participate on the network to increase the integrity and transparency for documentation. This is a direction we will continue to study in the coming time to further develop our research.

ACKNOWLEDGEMENTS

We would like to thank CS'18.17 topic: "Application of Blockchain technology in legal document security", Institute of Information Technology, Vietnam Academy of Science and Technology that has provided funding for the study. We would also like to thank the support of FIRST Central Project Management Unit, Ministry of Science and Technology, Vietnam under Grant Agreement number 12/FIRST/2a/IoIT.

References

[1] Riera A, Brown P. Bringing confidence to electronic voting. Electronic Journal of e-Government 2003;1(1):43-50.

[2] Kirkos E, Spathis C, Manolopoulos Y. Data mining techniques for the detection of fraudulent financial statements. Expert systems with applications 2007;32(4):995-1003.

[3] Server O. Corruption: A major problem for urban management: Some evidence from Indonesia. Habitat International 1996;20(1):23-41.

[4] Hofmann H, Schleper MC, Blome C. Conflict minerals and supply chain due diligence: an exploratory study of multi-tier supply chains. Journal of business ethics 2018;147(1):115-41.

[5] Crosby M, Pattanayak P, Verma S. Blockchain technology: Beyond Bitcoin. 2016.

[6] [6] Davidson S, De Filippi P, Potts J. Economics of blockchain. 2016.

[7] Khan C, Lewis A, Rutland E, Wan C, Rutter K, Thompson C. A Distributed-Ledger Consortium Model for Collaborative Innovation. Computer 2017;50(9):29-37.

[8] Benchoufi M, Porcher R, Ravaud P. Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research 2017;6:66.

[9] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. Open and Big Data (OBD), IEEE International Conference on; 2016.

[10] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society 2018;39:283-97.

[11] Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem". ACM Transactions on Programming Languages and Systems.

[12] Satoshi Nakamoto, The book of Satoshi (2014).

[13] Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques".

[14] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. “Handbook of Applied Cryptography”.

[15] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone (October 1996). "11: Digital Signatures". Handbook of Applied Cryptography.

[16] V. Miller, "Uses of elliptic curves in cryptography" in Advances in Cryptology Crypto 85, Springer Verlag, vol. 218, pp. 417-426, 1986.

[17] Stevens, Marc; Bursztein, Elie; Karpman, Pierre; Albertini, Ange; Markov, Yarik. "The first collision for full SHA-1" (PDF). Shattered IO. Retrieved 23 February 2017.

[18] Stevens, Marc; Bursztein, Elie; Karpman, Pierre; Albertini, Ange; Markov, Yarik. "The first collision for full SHA-1" (PDF). Shattered IO. Retrieved 23 February 2017.

[19] "Bitcoin". U.S. Commodity Futures Trading Commission. Archived from the original on 1 July 2018. Retrieved 17 July 2018.

[20] An Illustrated Guide to Cryptographic Hashes. (2015, May 9). Retrieved from http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

[21] Veness, Chris. “SHA-256.” SHA-256 Cryptographic Hash Algorithm Implemented in JavaScript | Movable Type Scripts, 2015, www.movable-type.co.uk/scripts/sha256.html.

[22] O'Connor, J. J.; Robertson, E. F. (October 1998). "Karl Theodor Wilhelm Weierstrass". School of Mathematics and Statistics, University of St Andrews, Scotland. Retrieved 7 September 2014

[23] W. Stallings, Cryptography and Network Security 5th Edition, Prentice Hall Pearson Education, Inc, 2011.

[24] Marling Engle. Vulnerabilities of P2P systems and a critical look at their solutions, May, 2006

[25] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

Thanh- Son Khuat received the B.S. degrees in Information Technology from University of Engeneering and Technology, Vietnam National University in 2016, respectively. During 2016-2017, he stayed in Samsung Vietnam Mobile R&D Centre, Samsung Electronic Vietnam, to study mobile and application for samsung mobile. Currently working at the Institute of Information and Technology, VietNam Academy of Science and Technology. Research fields: software quality assurance, software verification, program analysis.

Truong- Thang Nguyen received a Ph.D. in 2005 at the Japan Advanced Institute of Science and Technology (JAIST), Japan. Currently working at the Institute of Information Technology, Vietnam Academy of Science and Technology. Research fields: software quality assurance, software verification, program analysis.

Manh-Dong Tran received a M.S. degree in 2013 at the University of Engineering and Technology, Vietnam National University, Hanoi. Currently working at the Institute of Information Technology, Vietnam Academy of Science and Technology. Research fields: software quality assurance, software verification, program analysis.

Phe- Do Le received a Ph.D. Currently working at the University of Engineering and Technology, Vietnam National University, Hanoi, Vietnam. Research fields: Information security in electronic transactions, Math methods in technology