Journal of Engineering and Applied Sciences 13 (3): 696-699, 2018
ISSN: 1816-949X

The Study for Detection and Tracking Technology on Cyber-Vulnerable Area by Consortium Block Chain

[1]Cheol Hee Yoon and [2]Jang-Mook Kang
[1]Police Science Institute, Asan, Korea
[2]Namseoul University, Seoul, Korea

Abstract: The block chain technology started with security technology. But it will bring a revolution in every area of society. A block chain is a continuously growing list of records, called blocks which are linked and secured using cryptography. Each block typically contains a cryptographic hash pointer as a link to a previous block, a timestamp and transaction data. Information such as cyber gambling, suicide prevention and fake news which are cyber threats can be managed by the information sharing exchange algorithm and forgery prevention technology of the block chain. This technology cannot access and modify the final information written on the ledger as well as it provides a source technology that cannot be manipulated by any hacking, theoretically. This study is expected to contribute to the strengthening of the block chain technology to solve the validity of the consortium block chain and the cyber vulnerable area.

Key words: Consortium block chain, cyber vulnerable area, cryptographic hash pointer, cyber gambling, suicide prevention, security technology, Korea

INTRODUCTION

As the block chain consists of a set of technical combinations such as 'hash algorithm asymmetric key encryption', it utilizes a P2P-based exchange network, a decentralized operating system that does not require a 'third party accredited organization' (Arai *et al*., 2004).

The generated blocks are dispersed and stored, so, that theoretically, more than 51% of the network participants must be hacked and succeeded. In other words because of the 'physical, temporal, spatial' Impossibility of modulation there is a significant advantage in integrity management after detection of illegal cyber threats on cybercrime.

In the recently study, we attempt information such as cyber gambling, suicide prevention and fake news which are cyber threats can be managed by the information sharing exchange algorithm and forgery prevention technology of the block chain.

MATERIALS AND METHODS

Understanding block chain technology

Block chain type: Block chaining can be classified intothree types according to the nature of network participants and system access range, public block chain, private block chain, consortium block chain (Jung-Seok, 2016).

First, the 'Public Block Chain' which is a primitive initial model is an 'open type' technology in which all participants can freely share information and anyone can participate if they can use the computer interface.

It has a unique type of technology which is made by 'distributed type' structure with perfect decentralization characteristic and does not receive the centralized control of the central manager, although, it has the disadvantage of being relatively slow due to the need for verification of numerous connection points, it is a technology required for cyber-vulnerable area management and verification of information integrity (Kyeong-Su, 2018) (Table 1).

A technique of block chain generation: The method of generation is efficiently carried out in the following step in order to make a block chain. First, after encrypting the records produced by the information owner with the public key with a data 'input value' having an arbitrary length.

It generates a 'digital signature' of a mathematical algorithm representing a deterministic 'result value' of a fixed length. In this process, check whether the sender's 'Public key' matches the 'Private key'. Then, we do 'Mining (Hoon, 2016) 'which decrypt complex hashing ciphers. Mining is a process of "unlocking passwords" or "complex math problems" with mining.

Corresponding Author: Cheol Hee Yoon, Police Science Institute, Asan, Korea

Table 1: Key features of each type of block chain

Type classification	Concepts and features	Use case
Public block chain	First block chain use cases	Bitcoin, Ripple, Litecoin, Open Bazaar, DASH, Ethereum
	Open to everyone through the internet and operate	
	Anyone can participate in notarization through computing power	
Private block chain	Personalized block chain	NASDAQ, overstock, chain
	One object manages the internal network as a authority	
	Platform services emerging for development	
Consortium block chain	Semi-central type block chain	R3 CEV, HSBC, Varclays, Goldman Sachs, BoA
	Only a small Number of preselected (N) subjects can participate	
	Notarized participation through agreed rules among the subjects	
	Easy network expansion and fast transaction speed	

The encrypted block is composed of 6 pieces information. It consists of 'block headers' and 'block bodies' containing 'transactions' to form one block. Second, the block hash of the block header is created by twice-hashing the SHA-256 function.

Each of these blocks is connected to a chain by a linked list method in which a list is implemented using a link between an element and an element. Here, the element (or bit) is the minimum unit of information indicating either state of the pulse which is either "exist", "absent" or "binary. The previously generated block hash is stored in the 'previous block hash value' item of the next block header.

The block body stores transaction and other information not used in block hash calculations. From the most recently generated block (#N) to the first block (Genesis block, "#0") all are connected. In this way, a system in the form of a chain is constructed.

This means that a large amount of information held in each block is not utilized as independent data independently but is a vowel and data in which a valid block is successively connected as a whole.

This unique link structure scheme means that the entire block (#1) is affected when the record for the current block (#2) is to be modified. After the node receives the newly created blocks from the network, it connects the blocks to the existing block chain after validating the received block.

To connect the new block to the block chain, the node checks the newly created block header and finds the hash value of the previous block. This is because once registered data cannot be modified and continuous data cannot be manipulated. It does not allow to design arbitrary operation, technically (Bong-Jin, 2017).

RESULTS AND DISCUSSION

Application of block chain technology to solve cyber vulnerable area

Consortium block chain to solve cyber vulnerable area: A block chain is a technique whereby all participants in a network jointly validate, record and archive transaction information. It means, block chain is distributed transaction book that jointly manages cyber information (Tae-Hyung, 2017).

The main features of this block chain are: First, the block chain has the characteristic of 'P2P Base'. This is because only the data is used for data usage among the peers of each network and all transactions are permanently recorded (called 'History data') in established system.

It is a principle. By using 'distributed database' algorithm based on P2P network of block-chain, it is possible to share information that contains information of cyber-vulnerable shaded area and information ledger which contains hazard information.

If producers of cyber hazards put cyber threats and leak information, The other user can acquire source information that is monitored online and can be controlled by a regulatory agency such as the police.

Therefore, we have accumulated information resources for cyber vulnerable area. As well as the servers of a particular central organization, all the computers of the online network participants are equally distributed and stored by block chain.

A new type of security management, block-chain model can be provided that independently verifies the validity of the data. Second, integrity verification of data using 'Merkle Tree' an encryption technique used in the block chain and public key based asymmetric key cryptosystem can be applied.

The root node of the merkle tree consists of the hash values of the data of all the leaf nodes constituting the tree. The user has the advantage that it is possible to verify the stigmata of the data by merely verifying the hash of the root node.

The hash function algorithm functions as a digital fingerprint. Though it accepts input with an unspecified length but outputs have a fixed length. It is very difficult to infer the input value from the result of the hash function because the result is a completely different value even if the input value changes slightly with the one-way function (Geroge *et al*., 2001).

As mentioned before, the consortium block chain is more secure because it is based on the SHA-256 (256-bit SHA-2) function and can utilize the Mercle tree. So far, we have analyzed technologies that reduce the vulnerability of cyberspace using consortium block chain technology. The following paragraphs discuss the application of Consortia block chain technology.

Application of consortium block chain to solve cyber vulnerable area: In Korea, where block chaining is used most frequently is the financial industry sector, it is possible to safely and conveniently use data information by using 'transparency' and 'traceability' of transactions in the field.

If, we extend this function to the public service purpose to construct the element detection and management system for cyberspace, the cyber space can be provide e-Confidentiality' 'Integrity' and 'Non-repudiation' for solving the cyber vulnerable area among the information data generated in the cyber space (Bae Bong-Jin, 2017). Also, since, each information data is connected to a chain structure, it is very necessary as a cyber hazard detection and prevention technique.

Cyber vulnerable area detection and tracking technology by block chain: Due to the removal of cyber hazard items is achieved in detection and tracking technology by block chain. First, meta search information of major search engines can be managed through the Merkle tree hash of the block chain. This is because it is possible to manage the risk factors of cyber on a regular monitoring by the block chain ledger and to prevent the forgery from the source information about cyber vulnerable areas.

Step by step as news reports from various media companies on the portal site, news accounts on Twitter, RSS monitoring provided by media companies share the consortium block chain ledger to provide users with quick and accurate information which the integrity of the information flow channel can be guaranteed.

Second, cyber vulnerable areas are based on jargon, so data collection and automatic analysis functions must be implemented through the block chain, the analyzed jargon is used to calculate the number of postings, posting frequencies and statistics for each term.

The calculated statistics are used in the analysis of the importance of cyber Jargon, recent cyber risk factors and criminal transaction trends. The search results managed by the block chain technology are extracted with new and new terms and can be utilized for the latest cyber Jargon collection and trend analysis. Identification of initiators and vulnerable factor writers of cyber risk and division of organizational sharing power (identification of bot networks) in the case of large-scale re-distribution without using the normal sharing function, similarity analysis can be performed and managed by the block chain technique using the message retrieval.

Ultimately, the risk factors to be analyzed are plotted according to the time sequence through the time series analysis engine. It is possible to analyze the usage patterns over time by analyzing the risk factor distribution and risk factor log history.

As outputting all the risk factors corresponding to the search condition to the timeline, we check the time sequence between each risk factor. This time order is again applied to the block chain which is used to prevent forgery of facts that is for integrity verification.

CONCLUSION

The cyber vulnerable area reducing system that incorporates the block chain technology cannot access and modify the final information written on the ledger as well as it provides a source technology that cannot be manipulated by any hacking.

Though the traditional forgery hacking technique before the block chain technology was introduced was simply altered by those who attempted malicious tampering but using a block chain is not possible in a completely different way. Note that using block-chain technology.

It is the fact that all those who are trying to solve the cyber-vulnerable area are majorities, not minority of them. The ability to monitor and manage normal multi-users is a major milestone.

A huge ledger with all of the risk elements of the cyber vulnerable area is shared with the public which is managed using block chain technology. This study is expected to contribute to the strengthening of the block chain technology to solve the validity of the consortium block chain and the cyber vulnerable area.

ACKNOWLEDGEMENTS

This research was Supported by a Korea University Grant for 'Derivation of Educational Information Metaphor and Semantically Assigned Weights of Multiple Modality using Semi-formal/Irregular Data Values Applicable to Smart e-Learning' from Korea.

REFERENCES

Arai, M., K. Okumura, M. Satake and T. Shimizu, 2004. Proteome-wide functional classification and identification of prokaryotic transmembrane proteins by transmembrane topology similarity comparison. Protein Sci., 13: 2170-2183.

Bong-Jin, B., 2017. A Hash-Based Signature Scheme for Block Chain. Pusan National University, Busan, South Korea.

Geroge, C., J. Dollimore and T. Kindberg, 2001. Distributed System: Concepts and Design. 3rd Edn., Addison-Wesley, Boston, Massachusetts, USA., ISBN-13:9780201619188,.

Hoon, K.J., 2016. A study on the efficiency improvement of virtual money and block chain system. Master Thesis, Korea University, Seoul, South Korea.

Jung-Seok, K., 2016. A study on the factors affecting the intention of block chain technology acceptance. Ph.D Thesis, Soongsil University, Seoul, South Korea.

Kyeong-Su, S., 2018. A study on cyber threats from North Korea and counterstrategies. Ph.D Thesis, Faculty of Political Science and Diplomacy, Chungnam University, Daejeon, South Korea.

Tae-Hyung, K., 2017. Block Chain Concept and Case Analysis by Field. Ji-Jong, China, Pages: 487.