Journal of Engineering and Applied Sciences 13 (3): 686-690, 2018
ISSN: 1816-949X

A Case Study for Public Blockchain and Cryptocurrency Technology Focus on Authentication System

Nara Kim and Jang Mook Kang
Department of Big-Data Industrial Security, Namseoul University, 31020 Cheonan City, Korea

Abstract: An blockchains are secure by design and are an example of a distributed computing system and blockchain is suitable for the identity management transaction processing. In this study, we suggested a user authentication service based on blockchain. Blockchain technology enables entities independent of each other to rely on the same shared, secure and auditable source of information in a way that fits well with a system of widespread digital identity. The proposed model can be applied to various systems while guaranteeing secure authentication of users. Therefore, users can conveniently use various services without generating many accounts and passwords.

Key words: Blockchain, authentication, identity management, cryptocurrency, public blockchains, secure

INTRODUCTION

Bitcoin began operating in January 2009 and is the first decentralized cryptocurrency with the second cryptocurrency, Namecoin, not emerging until more than 2 years later in April 2011 (Hileman and Rauchs, 2017). Today, there are hundreds of cryptocurrencies with market value that are being traded and thousands of cryptocurrencies that have existed at some point (Taylor, 2013).

For example, Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy and speed of certain components of the internet infrastructure such as DNS and identities. For the technically minded, Namecoin is a key/value pair registration and transfer system based on the Bitcoin technology. Bitcoins and various Cryptocurrency have appeared. At the same time these Cryptocurrency have different technologies. Different technologies lead to different implementations and services.

In the present study, in this study we suggested a user authentication service based on blockchain. Blockchain technology enables entities independent of each other to rely on the same shared, secure and auditable source of information in a way that fits well with a system of widespread digital identity. The proposed model can be applied to various systems while guaranteeing secure authentication of users. Therefore, users can conveniently use various services without generating many accounts and passwords.

We focused on public block chains and cryptocurrency. In particular, we analyzed open blow chain technology and compensation cases through Cryptocurrency.

MATERIALS AND METHODS

Public blockchain and Cryptocurrency technology

Public blockchain: The following description is an excerpt from an IBM technical review. The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger (Jayachandran, 2017). A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today. One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of research to ensure all are in sync. Another disadvantage is the openness of public blockchain which implies little to no privacy for transactions and only supports a weak notion of security. Both of these are important considerations for enterprise use cases of blockchain (Jayachandran, 2017). In addition to IBM's

Corresponding Author: Department of Big-Data Industrial Security, Namseoul University, #13149 Design Information Bldg., 91 Deahakro, Seongjwan-eup, Seobuk-gu, Cheona City, 31020 Choongnam, Korea

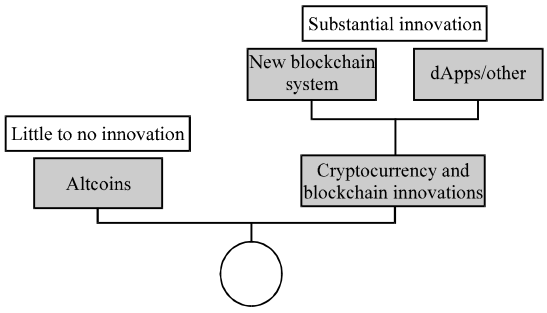

Fig. 1: The world of Cryptocurrencies beyond Bitcoin (Hileman and Rauchs, 2017)

technical reviews, the University of Cambridge study, supported by visa's credit card, describes the open blockchain technology as follows:

The common element of these different Cryptocurrency systems is the public ledger ('blockchain') that is shared between network participants and the use of native tokens as a way to incentives participants for running the network in the absence of a central authority. However, there are significant differences between some Cryptocurrencies with regards to the level of innovation displayed (Fig. 1).

Figure 1 shows, the blockchain technology is divided into public and private. A private blockchain is a technology that is advantageous for a country or a large company. Cryptocurrencies are not required for private blockchain services. On the other hand, a public blockchain requires Cryptocurrencies. Public blockchain service is suitable for venture companies. A venture company can issue cryptocurrencies to receive investment.

This study deals with public block chain technology and services. In the next study, we analyze the Cryptocurrencies that must be considered in the public blockchain service.

Cryptocurrency technology: In public blockchain technology, the token is a Cryptocurrency. In private blockchain technology, tokens are only used for transactions. However, the public blockchain technology has been rewarded for participating in transactions and using someone else's computer resources. Cryptocurrencies is used as a method of this reward system (Fig. 2).

Cryptocurrencies takes up block chaining, protocols, tokens and a variety of applications. For example, the analysis of one of the public Cryptocurrencies, etherium is as follows. Ethereum is a public, open-source and block chain oriented distributed computing protocol that features smart contracts (scripting) functionality (Nielson, 2008).

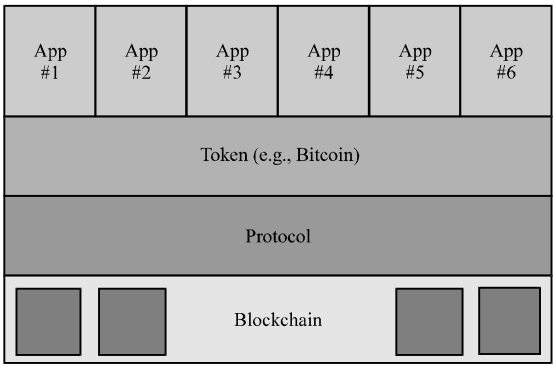

Fig. 2: The Cryptocurrency technology stack (Kasireddy, 2017)

There are many kinds of Cryptocurrency as follows: Cryptocurrency was traded as of August 2017. At the top of the list is of course, Bitcoin with a market cap of $55 billion. Ethereum is a distant second with a market cap of $25 billion but there are seven other cryptocurrencies with market caps over a billion. The currencies include Ripple ($6.8 billion), Bitcoin cash ($5.1 billion), Litecoin ($2.3 billion), NEM ($2.3 billion), Dash ($1.4 billion), Ethereum Classic ($1.4 billion) and IOTA ($1.3 billion) (Duggan, 2017; Hileman and Rauchs, 2017).

A virtuous circle structure of public blockchains and Cryptocurrency: We analyzed the virtuous cycle through the following scenarios. First, Cryptocurrency trading takes place. This transaction is known to the nodes participating in the Cryptocurrency network. Record and formalize known transactions on a network node of Cryptocurrency. This process is called mining in public blockchain services. This process is stored in blocks. Thus, the blockchain feather block is a collection of Bitcoin transactions in about 10 min. A blockchain is a book in which all the Bitcoin transactions that have taken place until now are recorded in chronological order.

Figure 3 shows a virtuous circle structure for Cryptocurrency. In the virtuous cycle process, new blocks are processed according to the rules. First, mining nodes are competing for processing. Second, submit the proof of research of the first mining operator. Third, the evidence tells neighboring miners that "this is the original". Fourth, the miners will go through the process of confirming and accepting them.

The block, thus, received is followed by an existing blockchain. This is the process of formulating blocks and blockchains. Bitcoin mining is specifically to find an arbitrary number X that makes the value of the hash of the block smaller than the given number (Nakamoto, 2008).

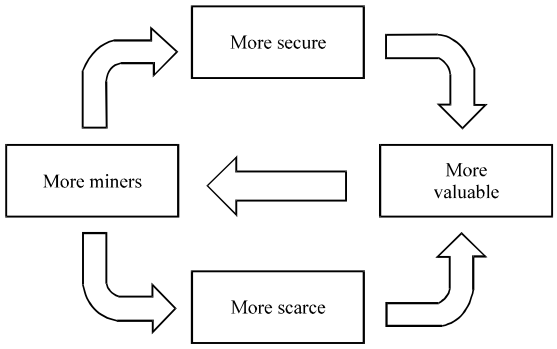

Fig. 3: The virtuous cycle of Cryptocurrency (Rho, 2014)

For example, a summary can be up to 99999 which is a random number that produces a summary that is less than or equal to the given number, 00099. Through the above process, a virtuous cycle of a public blockchain is achieved.

RESULTS AND DISCUSSION

Hashing function: The blockchain technique is used for authentication. One of the details of this authentication technique is a hash algorithm. The following paragraph cites an study by Rabbani (2017).

Hashing refers to the concept of taking an arbitrary amount of input data, applying some algorithm to it and generating a fixed-size output data called the Hash. The input can be any number of bits that could represent a single character an MP3 file an entire novel, a spreadsheet of your banking history or even the entire internet. The point is that the input can be infinitely big. The Hashing algorithm can be chosen depending on your needs and there are many publicly available Hashing algorithms.

What can this Hash be used for? A common usage for Hashes today is to fingerprint files, also known as check zones. This means that a Hash is used to verify that a file has not been tampered with or modified in any way not intended by the researcher. If WikiLeaks, for example, publishes a set of files along with their MD5 Hashes, whoever downloads those files can verify that they are actually from WikiLeaks by calculating the MD5 hash of the downloaded files and if the Hash doesn't match what was published by WikiLeaks then you know that the file has been modified in some way.

Hash functions are used in Hash tables (Konheim, 2010) to quickly locate a data record (e.g., a dictionary definition) given its search key (the headword). Specifically, the Hash function is used to map the search key to a list, the index gives the place in the Hash table

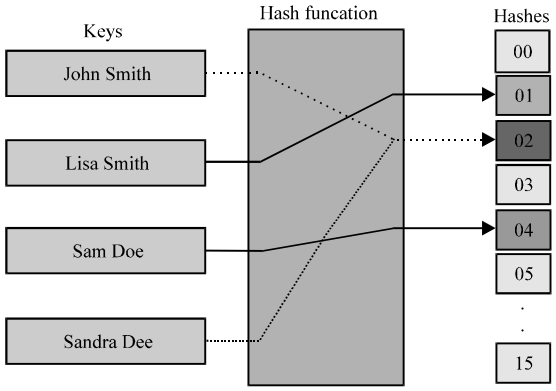

Fig. 4: The Hash function (Menezes *et al*., 1996; Anonymous, 2018a, b)

where the corresponding record should be stored. Hash tables, also are used to implement associative arrays and dynamic sets (Menezes *et al*., 1996) (Fig. 4).

How does the blockchain make use of Hashes? A Hash function that maps names to integers from 0-15. There is a collision between keys "John Smith" and "Sandra Dee".

A perfect Hash function for n keys is said to be minimal if its range consists of n consecutive integers, usually from 0-n-1. Besides providing single-step lookup, a minimal perfect hash function also yields a compact hash table without any vacant slots. Minimal perfect Hash functions are much harder to find than perfect ones with a wider range (Menezes *et al*., 1996).

The Hash function is used for digital signatures. Digital signatures are used today all over the internet. Therefore, the Hash function used in public blockchain technology can be utilized for digital signing.

Digital signature: Rosargia analyzed digital signatures as follows (Anonymous, 2018a, b). A digital signature is supposed to be just like a signature on study only in digital form. And there are mainly two things that, we want from signatures: only the owner can make the signature but everyone seeing it can verify its validity the signature must be tied to a particular document. So that, anyone can copy it and sign another document. In fact, a signature is not just a signature but certifies your agreement or endorsement of a particular document.

Digital signatures can be used for authentication. Certification is used in many areas. For example, it is necessary when purchasing goods electronically or when purchasing real estate. On the other hand, hackers want to hack the digital certification process. Therefore, digital authentication requires thorough security. If the wrong information is transmitted during the authentication

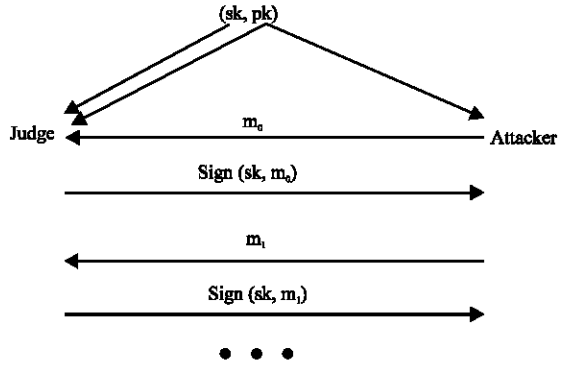

Fig. 5: Authentication system to use blockchain tech

process, the user is in danger of fraud or the like. Public blockchain technology can secure the digital authentication process. Especially by using distributed book technology of public blockchain service, security can be maintained at low cost. The next study is an explanation for this.

Authentication system to use blockchain technique: Information protection is a digital fraud activity that takes place during business or processing. The hacker analyzes the process as a module and finds vulnerabilities. For example, suppose you have a service that "A" purchases an item and delivers the purchase price to "B". Breaking down this process can lead to the following vulnerabilities: there is a process in which "A" delivers the purchased item information to "B" in plain text. The hacker can intervene in the process of notifying "B" that the "A" has purchased a "$5" item in plain text over the internet. The hacker takes the commodity price "5 $" from the internet. Then modulate this "$5"-"$5000". And then pass this to "B". "B" is deceived as "A" purchases a "5000$" merchandise. This process is due to the transmission of important information about the product in plain text. So far, information security has focused on encryption. It is to convert plain text into a cipher text. However, the Blockchain technology informs all participants that "A" has purchased a "$5" item for a multi-stakeholder. Therefore, there is a problem that a hacker should not hack everyone's information. This distributed library technology is more secure than existing systems.

Figure 5 illustrates technically what has been described so far. The information protection process is as follows (Rosargia *et al*., 2014). As a first step, the attacker sends a message m_0, the judge signs it and sends it back. As a second step then he sends another message m1, the judge signs it and sends it back. As a third step, the previous steps can be repeated over and over, until the attacker is satisfied. After that, the attacker picks a new message m and tries to forge a signature. As a final step, the judge will run the verification algorithm to check whether it verifies or not. The above process is technically a way to prevent forgery and tampering by hackers. Technically, digital signage can be replaced by blowchain technology. And if you use it well, you can get low cost protection effect.

CONCLUSION

This study analyzed blockchaining technology and digital authentication technology. A digital authentication system is proposed to solve the high cost of existing digital authentication technology. In particular, the public Blockchain technology is expected to replace the existing digital authentication service. This study was limited by the recent emergence of blockchain technology. There was not enough technical content to examine. In particular, we have not been able to analyze how distributed server technology works with existing authentication systems. However, this research is expected to contribute to the public blockchain technology and Cryptography to provide insights into igital authentication systems.

ACKNOWLEDGEMENT

Funding for this study was provided by Namseoul University.

REFERENCES

Anonymous, 2018a. Blockchain and cryptocurrency #3: Digital signatures. Steemit, Inc., New York, Virginia, USA. https://steemit.com/blockchain-crypto/@rosargia/blockchain-and-cryptocurrency-3-digital-signatures.

Anonymous, 2018b. Hash function. Wikimedia Foundation, California, USA. https://en. wikipedia. org/wiki/ Hash_function.

Duggan, W., 2017. On the breadth of cryptocurrency: How many different kinds of digital currencies are there?. Benzinga, Detroit, Michigan. https: //www.benzinga.com/general/education/17/08/9893336/on-the-breadth-of-cryptocurrency-how-many-different-kinds-of-digital.

Hileman, G. and M. Rauchs, 2017. Global cryptocurrency benchmarking study. Msc Thesis, Cambridge Centre for Alternative Finance, University of Cambridge, Cambridge, England, UK.

Jayachandran, P., 2017. The difference between public and private blockchain. Blockchain Unleashed: IBM Blockchain Blog. https://www. ibm. com/blogs/ blockchain/2017/05/the-difference-between-public-and-private-blockchain/.

Kasireddy, P., 2017. Bitcoin, ethereum, blockchain, tokens, ICOs: Why should anyone care?. Hacker Noon. https://hackernoon.com/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care-890b868cec06.

Konheim, A.G., 2010. Hashing in Computer Science: Fifty Years of Slicing and Dicing. John Wiley & Sons, Hoboken, New Jersey, USA.

Menezes, A.J., P.C.V. Oorschot and S.A. Vanstone, 1996. Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida, USA., ISBN-13:978-0-84-938523-0, Pages: 780.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. J. Netw. Comput., 1: 1-9.

Nielson, B., 2008. Review of the 6 major blockchain protocols. Richtopia Ltd., London, England, UK. https://richtopia.com/emerging-technologies/review-6-major-blockchain-protocols.

Rabbani, H., 2017. What is hashing and digital signature in the blockchain?. Blockgeeks, Ontario, Canada. https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/.

Rho, S., 2014. [Virtuous cycle of bit coin mining]. Organic Media Lab lnc., Korea. (In Korean) https: //organicmedialab.com/2014/01/11/virtuous-cycle-of-bitcoin-mining/.

Taylor, M.B., 2013. Bitcoin and the age of bespoke silicon. Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems, September 29-October 04, 2013, IEEE Press, Piscataway, New Jersey, ISBN:978-1-4799-1400-5, pp: 16:1-16:10.