RESEARCH ARTICLE OPEN ACCESS

Blockchain Insight

Azhar Ushmani
Senior Software Engineer
AdvancedMD Inc
USA

ABSTRACT
The modern economy has recently been presented with the blockchain technology which is considered to be the most perspective and effective system. It is designated to solve various problems associated with security and reliability of data processing. Theoretically, the technology demonstrates positive and reliable results but there are certain advantages and disadvantages. The purpose of the assay is to discover the phenomena of blockchain and to analyze the structure of this newest technology which is so popular nowadays.
Keywords:- *Block Chain*

I. BLOCKCHAIN AND ITS ARCHITECTURE IN DETAILS

There are a lot of hopes associated with the blockchain technology and they are not only associated with the financial sphere including cryptocurrency. Such spheres as business, logistics and government systems can implement the technology making them more reliable, safety, and trusty. The reason why the technology is becoming so popular is that it has strong benefits but there are also certain disadvantages. Among them the most obvious is the implementation costs and process. One of the greatest advantages of the technology is that it provides an opportunity to transfer your financial assets without using and spending money on an intermediary.

The realization of the blockchain technology is based on creating data blocks. The data is different in each of the blocks. Moreover, the blocks in the chain are interrelated with each other. When a new data block is connected to the blockchain, it becomes impossible to delete or change the data block. Another advantage of the blockchain is that hackers need to have a great processing power to be able to hack one of the data blocks. The hash value of each block is calculated by miners separately and that is one of the reasons why hacking a blockchain is not an easy thing to do (Golosova, and Romanovs).

One of the most popular definitions of a blockchain is that it is considered to be a digital ledger that contains information on transactions and can also be used to record everything that represents certain virtual value. Now, it is time to discover the structure of the blockchain technology. It is represented as a sequence of blocks and every new block is added within a certain time interval. The data which is kept within block can be different but, at the same time, the hash, transaction and timestamp can be reached and visible in all the versions of the Blockchain networks. It is obvious that each block contains the cryptographic hash of the later data block. Moreover, the information on the hash is generated automatically. Thus, it becomes really impossible to do anything with the data in the hash. The verification of the next joint block strengthens the security of the previous one in the blockchain. As a result, the more blocks are in a chain, the more secure and reliable the blockchain is.

Concerning the use of the technology in the sphere of cryptocurrency, blocks are called transactions. Each of these transactions contains the information on a value, recipient's address as well as sender's address. Besides, it does look like an ordinary transaction we used to see in our bank account. If one person transfers a Bitcoin to another, the value of this Bitcoin moves from one address to another. As a result, the transaction alters the structure of the correlated blockchain. In other words, the technology presented is shared and decentralized. All the users of the blockchain have the copy of the blockchain. Each of the transactions is processed in the same order it is presented in the blockchain. Transactions are tied together and transferred from one user to another as blocks. Each user can also process each of the transactions but the verification process is done independently. The data contained in the blocks is associated with the movement of the cryptocurrency from one

owner to another. Besides, the information on verification and handling of the transactions depends on the ways of implementing the technology (Guo, and Liang).

There are two types of the blockchain structure. The first one is presented in the form of a block sequence and includes all the data on transactions. The data is collected into a public ledger. Hash is contained in the block header and a block has just one parent block. The initial block of a blockchain is named a genesis block and it does not have any parent one.

The block structure is presented by the block header as well as block body. Considering the block structure, it indicates which of the validation rules to follow. Moreover, the hash value of the transactions in the block is called merkle tree root hash. Timestamp is referred to the current time since January 1, 1970. It is usually displayed in seconds. There is also one more term to consider which is nBits and it shows the target limit that is referred to a valid block hash. Another term that will be used in the paper is nonce which means a 4-byte field which is generally starts with zero and is supposed to increase when calculation of every hash is done. The parent block in the block of a structured blockchain has 256-bit hash value and is connected with the previous block.

To make a certain transaction any user needs to have a public and private key. The private key is of a great importance and it is needed to be kept confidentially. The transactions that are digitally signed can be transmitted throughout the whole network. It is also important to understand that the digital signature is composed of two stages. The first one includes the process of signing and the other is related to the process of verification. To send some money, a person needs to encrypt the information with the private key. The receiver needs to complete the process of validation with the help of the public key of the sender.

The programmers can define certain characteristics of a blockchain. One of the key ones is considered to be decentralization. There is no need in any central trusted agency that could approve or disapprove transactions. Another characteristic is associated with persistency which means that all the transactions can be validated in a quick and easy way. Invalid transactions will not be approved by miners. And, if a transaction is invalid, it is rather easy to see it in a blockchain. There is one more characteristic that is lacked by the current financial system and it is related to anonymity. The sense of anonymity is that any user can deal with a blockchain with the help of a generated address. Here, the real identity is not disclosed and a person can feel rather confident. Besides, any person who will interact with the blockchain can consider the auditability characteristic. For example, a Bitcoin blockchain preserves all the information on users' balances using a UTX-O model. It means any transaction has a relation to other unspent transactions and when a transaction is made, the condition of those related unspent transactions change from unspent to spent. As a result, any transaction can be found and verified.

Now, it makes sense to talk about the existing types of blockchain systems. They can be also divided into three groups: consortium, private and public (Kakavand et al.). Considering the public type, all the information is transparent and everyone can participate in the consensus process. If there is a consortium blockchain, then just users or nodes from a group of organizations can take part in the process of consensus. Regarding the private type of the blockchain, it is vivid that only a group of people from a certain organization will be able to take part in the consensus process. If talking about a private blockchain, it must be noticed that it looks like a strongly centralized one as just selected nodes have the consensus privilege. There are also certain terms to consider and explain their meaning. The determination on consensus is different from one type of a blockchain to another. The same thing happens when talking about read permissions. Those transactions that are presented in a public blockchain can be viewed by anybody but the approach can be different if talking about private and consortium types. These three types differ in the level of transaction immutability as well. The transactions made within a public blockchain cannot be changed at all while transactions in any consortium and private blockchains can be easily changed as the number of users is rather limited. Another difference between the mentioned types is associated with efficiency of a certain blockchain. There are a lot of transactions in a public blockchain. As a result, it takes a lot of time to multiply transactions and form blocks. Consortium and private blockchains can operate more efficiently as a number of transactions are limited and the latency is rather low. The level of centralization of these blockchains is different as

well. Public blockchains are completely decentralized. Consortium ones tend to be more centralized while private blockchains is under control of a certain group of users. The same thing happens in relation of a consensus process. It is logic that anybody can take part in a consensus processes when a public blockchain is addressed. But, the other blockchains use certain permissions (Gramoli).

There are also certain issues that are faced by blockchains and, considering them, it is easy to conclude which of them have to be solved within the shortest time possible. The first issue is associated with scalability. The number of transactions is increased daily and every node has to validate them and check if the initial transaction is changed into spent or not. Moreover, there are limits concerning a block size and time interval. Additionally, block capacity is not that huge and small transactions are frequently delayed as miners are waiting for huge transactions (Kareem et al.).

Another issue is associated with privacy leakage. Users make their transactions with the help of their private and public keys. Their real names stay anonymous but the data on transactions and balances for each public key remain visible. That is a problem that needs to be solved.

Mining is a sphere which needs improvement as well and a specific blockchain frequently appears to be attacked by selfish miners. So, selfish miners usually keep their transactions without transmitting them and the private one will be disclosed if several requirements are satisfied. The private chain is longer and miners are always ready to accept it. As a result, honest miners use their possibilities to save a useless chain built by selfish miners while the later mine the chains without any visible competition. Finally, they get more profits.

II. CONCLUSION

There is no doubt that the introduction of the blockchain technology has changed the attitude to the traditional industry and has shown its unconditional potential. With the technology and its main characteristics such as anonymity, auditability, persistency and decentralization, companies start considering the implementation of it into different spheres of business not just financial ones. Analyzing the architecture of the system, it has become possible to define its positive and negative sides. Moreover, there are also some issues and changes that are faced by the new technology. These problems need to be solved to develop the improved blockchain system.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [13].

Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature

REFERENCE

[1] Golosova, Julija, and Andrejs Romanovs. "Overview Of The Blockchain Technology Cases". *2018 59Th International Scientific Conference On Information Technology And Management Science Of Riga Technical University (ITMS), 2018. IEEE*, doi:10.1109/itms.2018.8552978.

[2] Gramoli, Vincent. "From Blockchain Consensus Back To Byzantine Consensus". *Future Generation Computer Systems*, 2017. *Elsevier BV*, doi:10.1016/j.future.2017.09.023.

[3] Guo, Ye, and Chen Liang. "Blockchain Application And Outlook In The Banking Industry". *Financial Innovation*, vol 2, no. 1, 2016. *Springer Nature*, doi:10.1186/s40854-016-0034-9.

[4] Kakavand, Hossein et al. "The Blockchain Revolution: An Analysis Of Regulation And Technology Related To Distributed Ledger Technologies". *SSRN Electronic Journal*, 2017. *Elsevier BV*, doi:10.2139/ssrn.2849251.

[5] Kareem, Amer et al. "Algorithms And Security Concern In Blockchain Technology: A Brief Review". *SSRN Electronic Journal*, 2018. *Elsevier BV*, doi:10.2139/ssrn.3234933.