Implementation and Analysis of the use of the Blockchain Transactions on the Workings of the Bitcoin

Muhammad Reza Rizky Fauzi, Surya Michrandi Nasution, Marisa W. Paryasto
Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

muhammadreza1801@gmail.com, surya.michrandi@gmail.com, marisa.paryasto@gmail.com

Abstract. The present study discusses the workings of blockchain bitcoin in the transactions sector, on the development of today's emerging computers in the financial sector of blockchain bitcoin traction. In this case the author analyzes how the transaction is running, as well as how blockchain bitcoin is doing work in transactions on the system to make transactions. Transaction is a data structure that encodes the transfer of values between users with in a bitcoin system. Every transaction is a public entry in this bitcoin blockchain. And become a large transaction bookkeeping global.

Keywords: Bitcoin, Blockchain, Transaction Bitcoin, Simulation, Blockchain Bitcoin Sandbox.

1. Introduction
The development of computers today is very fast and continues to grow rapidly. One of the current computer developments is in the world financial sector, The financial sector is called the digital currency in the presence of this digital currency makes it easier for users to make financial investments in the form of digital currency called bitcoin and security in investment in the financial sector. It is now very difficult for the user to invest and secure his finances because there are so many crimes and irresponsible people taking and financing. Then with the development of this computer in the financial sector is very important and in needed the present so that our finances are not taken and tapped by the irresponsible parties and finances that we have saved is under control. The development of computers in the financial sector is also in use to facilitate the user perform transactions send and receive digital currency bitcoin in a large scope is of the world in the form of digital currency is bitcoin. With the development of the computer helps users to send or receive bitcoin inside the country and abroad, And with the development of the computer today users can make financial investments in the form of digital currency called bitcoin, in the presence of this user do not have to worry about the crime because with the development of computers in the field of finance is the user feel safe with the user save money in the form of bitcoin investment.
In this study researchers discussed the workings of blockchain bitcoin in the transactions sector, on the development of the computer that is developing at this time in the financial sector in the blockchain transaction bitcoin. In this case the researchers make the implementation and analyze how the
transaction is running, and how blockchain bitcoin stores the transaction data that has been done and do work in transactions in bitcoin system to make transactions. Transaction is the most important part of a bitcoin system. Everything else in bitcoin is designed to be done, spread into the network, validated, and then added to a ledger (blockchain) called a ledger (bookkeeping). Transaction is a data structure that encodes the transfer of values between users within a bitcoin system. Each transaction is a public entry in blockchain bitcoin. And become a large transaction bookkeeping global.

2. Related work

Bitcoin is one of the first implementations of cryptocurrency or digital currency. Bitcoin is a unique currency in which there is no central body governing transactions or publications. Bitcoin is open source and peer-to-peer. Open source means the currency system is developed jointly by anyone who wants to contribute. Peer-to-peer means that each transaction is recorded by a network of computers directly connected like a torrent system, Not through a mediating party such as a bank or merchant as is the case with most existing online payment systems (paypal, credit card, etc.). In this paper we will discuss the security aspects underlying the operation of bitcoin. Starting from account security and privacy, how digital signature systems are on bitcoins, how bitcoin overcomes double spending issues, How bitcoin mining works, as well as how bitcoin overcomes fraud from users who want to cheat. Keyword bitcoin, cryptography, bitcoin mining, double spending. [1].

Bitcoin is widely used as a digital currency and is widely used by hundreds or even thousands of merchants worldwide online, as a recognized currency. The bitcoin system itself is based on cryptocurrency, regardless of government regulation and decentralized the technology used is peer-to-peer networking and cryptography to maintain data integrity. In this research will be studied on how to get bitcoin through one way that is mining. Keywords bitcoin, cryptography, merchant, mining, peer-to-peer networking. [2]. Recently many reported incidents of infringement, surveillance and security that compromised privacy on users by form or model Calls to questions where the third party controls and collects some personal data. With Bitcoin providing trustworthy financial credentials for administrative computing to be under control and the system uses a peer-to-peer network with a decentralized general ledger. In this paper, we describe a decentralized personal data management system that ensures users control their own data. We implemented a protocol that converts blockchain into automatic access control management that does not require a third party. Unlike bitcoins, transactions in our systems are not really financial, they are used to carry instructions, such as storing queries and data. [3]. In a technology-dependent world, privacy is now much sought after. The privacy required among others is desirable especially when wanting to make online payments. With this online payment it motivates users to switch to electronic money and not using normal money normally. The shape of electronic money is not like that of banknotes used every day. The most successful use of electronic money is a decentralized bitcoin with a peer-to-peer system. This paper provides a broad introduction to bitcoin, While analyzing the construction and investigating some benefits and shortcomings. In this case it can be seen that when compared to paper money and money electron called bitcoin, bitcoin has its own class that has its own system. [4].

3. System design and implementation

3.1. System design

In this case the concept of making the design we made is implementing and analyzing how blockchain bitcoin works, and analyzing what is inside the blockchain bitcoin. But discussion in this concept is addressing on bitcoin, key on bitcoin, and transaction on bitcoin, and analyzing whether the system is safe or not for use in bitcoin transactions. The things needed for research to be made is a program on
bitcoin by using python programming language and java programming, as well as a simple software application to test and analyze the validity of how the system is running and to test whether the system is safe to use or not.

Below is the work of blockchain bitcoin transactions on an existing system:

**Figure 1. How Transaction Works** [5]

In the picture above transaction definition sender as a tool to make a transaction and transaction result into a network. The transaction message consists of the recipient’s public address details containing the value of the transaction and an exchange, and the address itself serves as a tool for conducting sales transactions between the sender and the recipient authenticating the transaction.

Transaction authentication nodes (computers or users) receive network messages and verify message validation by decrypting key exchanges between sender and receiver, as well as transactions confirmed and placed on databases that provide information about transaction delivery.

Block creation of pending transactions is put together in the latest version of the ledger or called the database (blockchain) by one of the nodes in the localhost network. at certain time intervals the node broadcasts the block into the localhost network to be validated.

Block validation node receives localhost network of proposals from blocks and works to validate it by going through repeated processes that require awareness of most networks. Different blockchain localhost networks use different techniques to validate them. Bitcoin in a simple localhost network block for storing transaction data. Various techniques have different pros and cons. The common denominator ensures that any transactions are in effect, and cannot create fake transactions.

Block chaining if all transactions have been validated, the new block is chained in blockchain, and the data base is broadcast to the localhost network, and the whole process can be completed in a few seconds.

Example illustration on key to be transactions on ECDSA algorithm:

**Figure 2. An illustrated example of how key works to transact** [8]
The picture above explains ECDSA is the result algorithm of DSA development. This algorithm uses elliptic curve over the prime finite field to specify the key. Stage at ECDSA is the stage of determining key, signing stage, and verification stage. In ECDSA, the party that will perform the digital signature, has an elliptic curve domain parameter of D = \{q, FR, a, b, G, n, h\} and the secret key pair dA and the QA public key. Then the party who will verify the signature has a copy of the authentic D document and the QA public key.

- **Key Generation**
  1. Selecting a random integer dA, whose value is between [1, n-1].
  2. Calculating QA = dA \cdot G = (x1, y1)
  3. Secret key = dA, and public key = QA [8]

Example illustration on address to be transactions Base58 on algorithm:

![Base58Check Encoding](image)

*Figure 3. Illustration of Base58 process Check encoding [9]*

Figure above explains that Base58 is a binary-encoded text format developed for use in bitcoins and is widely used in cryptocurrencies. Base58 also offers a balance on a compact, readable, and detect errors and prevention. Base58 is part of base64, which uses large and small types of letters and numbers, but can eliminate some of the characters that are often mistaken for each other. To add extra security to typos or transcription errors, Base58 Check is a Base58 encoding format, often used in bitcoins that has error-checking codes Built-in. The checksum is an additional four bytes added to the end of the data being encoded. Checksum is derived from data encoded hashes therefore can be used to detect and prevent transcription in typing errors. When presented with the Base58Check code, the decoding software will calculate the checksum of the data and compare it with the checksum already included in the code. If both do not match, it will indicate that the error is known and the Base58Check data is invalid. [9]

After learning about related topics, the next process is to design a system that includes the research flow, special flow, collecting the device used. The design of this system is done by creating a flowchart and use case diagram of how the system runs. Implementation in this research is how a blockchain system can create address on bitcoin and how Combining the bitcoin address of the sender and receiver, and whether the address is safe or not. Testing aims to test whether the bitcoin blockchain system is running well or not. Is the bitcoin blockchain address system secure.

In the picture below Specific Design above explains that after the user has obtained the key and address bitcoin, it will enter into the transaction phase, the transaction phase here is a public exchange Key and address of the sender so that the sender can send the bitcoin which is then validated by the sender and the receiver so that the transaction is valid or invalid key and address. Once the transaction is valid then the transaction will be sent into the blockchain ledger, the blockchain is a database that stores transaction data, after transaction is completed then there is a transaction confirmation that tells the sender that the
bitcoin that has been sent to the recipient has arrived at the recipient and the contents of the transaction confirmation itself in the form of transaction code, data sender, receiver data, the number of bitcoin, and time stamp.

This flowchart explains how the research is done as follows:

![Flowchart]

**Figure 4. Specific Design**

3.2. Implementation

This stage discusses about the design of system implementation, the program that has been made is in the form of an application system to implement transaction experiments on bitcoin with a simple method in the form of GUI applications.

After that stage of the application is used to determine the identity data of bitcoin users in the form of bitcoin wallet. The definition of bitcoin wallet itself is a place (wallet) as a storage bitcoin. Users will not be able to have bitcoins without having bitcoin storage. This wallet also serves to do bitcoin transactions on blockchain bitcoin. And this wallet application also serves as a tool for storing bitcoin user data such as balance, address, private key, public key of a user, as well as a transaction tool on blockchain bitcoin you want to do.

This application is designed in a simple form by using GUI method in java, because this application is just an example and a replica of the wallet application on the real bitcoin.

The design of this application system is used to perform a transaction on bitcoin. The application of this wallet makes it easier for users to transact both send and receive bitcoin with other users.

In this design we use several applications to do the making. Things needed to do Making this program is a program on bitcoin by using python programming language, as well as a simple software application that is GUI application to do testing. As well as analyzing the validity of how the system works with what it wants, Such as the transaction program is running and the application for testing was running...
well in order to make the transaction process to be done. And to test whether the system is safe to use or not in transacting on bitcoin.

3.3. Program Structure
Stage explains how the parameter system in a simple application software that has been created that is with programming algorithms that use python language that raised from a transaction work on bitcoin, then after generating transaction data on the bitcoin, the next experiment is to combine an address and key on the bitcoin into the transaction to be performed.

What is required at this stage is to work on raising an address and key on bitcoin to perform transactions on bitcoins. Because if you do not do that stage to bring up an address and user key then the transaction will not be done.

Design of the transactions that liaises between the user address and user key to do the transaction work on bitcoin. After getting the address and key users of the next stage is to unite the program into the transaction program for the transaction can run, After the program has been integrated and running well then input the program into a simple GUI application that has been created, the application is a wallet of bitcoin is a bitcoin user data storage. With the wallet users can do bitcoin transactions, without the wallet then the user cannot use bitcoin.

The result of the planning that has been achieved is the program can transact with what has been desired, this is the result of testing of how transactions work on blockchain bitcoin:

**Figure 5.** Bitcoin Wallet App

Bitcoin Wallet application that shows the contents of the bitcoin wallet, the wallet contents of the wallet contains several pieces of data are: Address or user id, private key as a tool to verify transaction results and as a bitcoin address backup tool, public key as a tool for selling transactions, and balances on bitcoins from coin ID users owned by bitcoin users.

**Figure 6.** Sending Transaction Process
In Sending Transaction Process transaction process to be performed, in this process the sender sells its bitcoin to the recipient. The sender needs the address of the recipient to do delivery. If the recipient does not provide the address then the sender will not be able to send the bitcoin to the recipient because what is needed to transact on the bitcoin is the recipient and the sender must do that step first ie the exchange of address and the public key to conduct the transaction and verify it.

**Figure 7. Transaction Status Process**

Process of transaction status, with the transaction status on a bitcoin wallet makes it easy for the sender to see if the bitcoin is already sent or not sent. If successful in sending the balance of the sender bitcoin will decrease and if unsuccessful then the sender bitcoin balance will not decrease.

**Figure 8. Transaction Record Process**

The figure above explain Transaction Record Process, once the transaction is received the data sent to the recipient and to the database Changed data contained in it contains public key hash, the amount Bitcoin sent and transaction status that has been sent to the recipient.

**Table 1. Process From Database**

| Kode_Transaction | Sender          | Receiver          | Bitcoin value | Time_stamp           |
|------------------|-----------------|-------------------|---------------|----------------------|
| 53bf2502         | 16ByDscY2dMnCtwM | 1PoDhtBLLHbx5tZXTc1 | 5             | 2017-06-03 14:09:59,27481 |
Above describes the table process of the database, the database itself here is as a replica tool of a data blockchain (ledger). This database serves as a notice to the seller and the buyer that the transaction process is done and as a mean of data transaction, transaction that has been going on or have done the transaction process before. The database also serves as a large storage tool to store some data that transacts from the number of users who do bitcoin transactions.

**Figure 9. Transaction Confirmation Process**

Figure this explain the Transaction confirmation process. This process is a confirmation tool to notify the sender and the recipient that the bitcoin has been already sent by the sender has been sent and received by the receiver. With the confirmation of the transaction itself provides convenience and security to the sender that the bitcoin delivery transaction is already in progress and has been sent to the recipient.

4. **Analysis**

At this stage, the test results that have been done are to find out whether the bitcoin system is safe when it wants to transact on bitcoin. The bitcoin system is the transaction security system, in the bitcoin itself the security lies in the key (public key and private key) and address. When you want to trade on bitcoin itself, you requires a key and an address to check the validity and validity of a transaction on bitcoin to know how transaction works on bitcoin, if the transaction does not have or have key and address then the transaction will not run and can not be used To conduct a transaction. Because key and address is needed by transaction to do bitcoin sale, and with key and address make sense of security and sense of comfort of bitcoin user to do bitcoin trading transaction, key exchange and address itself serves as a tool to conduct sales transaction Between sender and receiver.

The bitcoin transaction system itself lies in the exchange of the user's key and address, when transacting the sender and the recipient must first perform the key and address exchange in order to make the transaction process, if there is no exchange first then the transaction will not run. With the key and address exchange system on the transaction itself provides a sense of security to the user when they want to do bitcoin transactions.

So with this security the transaction on the bitcoin lies in key and address on bitcoin. By exchanging legitimate keys and validity that has been run between the sender and the recipient then the transaction goes well.

5. **Conclusion**

The result of the hypothesis that the researcher wants is a safe transaction to use when transacting bitcoin between sender and receiver after transaction, transaction data is stored on blockchain bitcoin so that user feel secure in transaction bitcoin blockchain own also as tool of storage of transaction data which
have been going on and know that the transaction is done. The test expected by the researcher is a test for safety in the transaction on blockchain bitcoin. the transaction security system on the bitcoin itself lies in the key and address then in the test this time is to analyse whether the system is safe to transactions on bitcoin as well as to implement how the transaction is running. By performing a valid key exchange and validity that has been running between the sender and The recipient then the transaction goes well.

References

[1] Reinhard Denis Najogie, mei 2013, “Analisis Keamanan Bitcoin”.
[2] Ferry Mulyanto, M Tirta Mulia, “Analisis Mining System pada Bitcoin”.
[3] Guy Zyskind, Oz Nathan, dan Alex 'Sandy' Pentland, 2015 IEEE. “ Decentralizing Privacy : Using Blockchain to Protect Personal Data”. MIT Media Lab. Tel-Aniv University, MIT Media Lab. Cambridge,Massachusetts. Tel-Aniv, Israel. Cambridge,Massachusetts.
[4] Danielle Drainville, Desember 2012.” An Analysis of The Bitcoin Electronic Cash System”. University of Waterloo.
[5] Peter Froystad, Jarle Holm, 2015 “Whitepaper Blockchain : Powering the internet of Value”. EVRY Financial Service
[6] Michael Crosby, Nachippan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, October 2016 “Sutardja Center for Entrepreneurship and Technology (Blockchain Technology)”. Barkeley Enggneering.
[7] Richard Caetano, 2015 “Learning Bitcoin Embrace teh new word of finance by leveraging the power of crypto-currencies using Bitcoin and the Blockchain”. Packt publishing open source, www. It-ebooks.info
[8] Rama Febriyan, 2014/2015 “Perbandingan Digital Signature Algorithm dan Elliptic Curve Digital Signature Algorithm”.
[9] Andreas M. Antonopoulos, 2015 “Bitcoin & the Blockchain”. O’Reilly Ebook Advantage.