Realization and Addressing Analysis In Blockchain Bitcoin

Raja Sakti Arief Daulay, Surya Michrandi Nasution, Marisa W. Paryasto
Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia

rajasaktidaulay@gmail.com, michrandi@telkomuniversity.ac.id,
marisa.paryasto@telkomuniversity.ac.id

Abstract. The implementation research and analyze address blockchain on this bitcoin will have
the results that refers to making address bitcoin a safe and boost security of address the bitcoin.
The working mechanism of blockchain in making address bitcoin which is already in the
blockchain system.

Keywords : Address, Bitcoin, SHA-256, Base58Check, Blockchain, Simulation bitcoin sandbox.

1. Introduction
The development of computers on this day is growing rapidly and also affect the financial system in the
world. Example is bitcoin, which is an electronic money made by Satoshi Nakamoto in 2009. But bitcoin
also developed a system called blockchain. Blockchain is a publicly accessible financial bookkeeping
and blockchain can show all transaction data that has occurred in a bitcoin network.
This journal is implementation of blockchain in the addressing sector of bitcoin. Where the bitcoin
address on the blockchain is used to be able to receive payments from others. And we can tell your
bitcoin address to others. This bitcoin address consists of different byte versions and your public key
hash byte combines them which are then encoded into Base58Check.
In this case the study analyzes how to use of bitcoin addresses in securing the sender and recipient
address for transactions on bitcoin.

2. Related work
Reinhard [1], In this paper, the advantages of a bitcoin are defined as a digital signature chain. The
privacy or confidentiality of user data is done in a unique way on bitcoin, in example each address in
the form of hash value. By default bitcoins also replaces the user address with a new hash value that is
different from the previous address. That is, transactions occur by way of digital signature on the hash
of the previous transactions and the public key of the receiver of the coin and the receiver further verifies
the received digital signature to ensure the ownership of the coins. However the problem with the system
is that the coin recipient can not be sure that the sender is not sending the same coin more than once
(double-spend). Bitcoin stores all transaction data that ever happened. This then raise the question of
how space on a user’s computer is enough to hold all the bitcoin transaction data that has occurred.
Bitcoin solves this problem by using a data structure called Merkle Tree. The basic logic of using this
data structure is longer transaction data can be deleted and stored its hash only.
Danielle Drainville [2], In this research explains bitcoin using some type of cryptography for validation
and system security. Namely using the hash function used for transaction and block generation is SHA-
256. As well as signature algorithm such as elliptic curve digital signature algorithms such (ECDSA). The algorithm is used to prevent malicious users from destroying the system. The function of this hash is to prevent malicious users from stealing and creating their own bitcoins. The conclusion in this paper is that cryptography is very useful for bitcoin security as well as few cases of theft or cases caused by cracker to break down this system, as for cases that occur because in the resulting by users who are negligent in closing his account.

Nicolas Dorier 2015 [3], From this book explains the bitcoin address is used to be able to receive payments from others. That private key is used to be able to spend the bitcoin owned. These two keys are not stored into the network, they can also be generated without having to connect to the internet. To get the bitcoin address, you can get it easily with your public key in the network you use for that address. This bitcoin address consists of different byte versions (on both networks) and your public key hash byte combines them, then encoded into Base58Check. The Base58Check encoding has some neat features like checksums to prevent typos and also reduce ambiguous characters. Base58Check encoding of an address to ensure that bitcoin wallet users do not send bitcoins to an address that should be used on different networks.

Dody Dharma [6], This paper describes the hash function SHA-256 uses 6 logical functions, each of which operates on a 32-bit word represented as x, y, and z. Where on the functional will be a new 32 bit word. The hash function is most commonly used to speed up the process of reading data in a table or data comparison process such as data search in a database, detecting the duplication of records on a large file, and searching for sequence similarities. The hash algorithm recommended by Adobe to be utilized is SHA-256, as it is considered quite safe against cryptographic attacks.

3. System design and implementation

3.1. System design

The concept of making the design us to implement and analyze in blockchain bitcoin, but discussed in this concept only in addressing the bitcoin and analyzing the system is safe or not. What is needed in the research is a program in bitcoin using python programming language, as well as software to test and analyze how the system running and tested to the system is safe or not.

The author analyzes how blockchain creates addresses on bitcoins, the concept being made this time is to see how the public key creates the address, and how to transfer the bitcoin from sender and the transacted receiver bitcoin. Bitcoin is not also used in terms of sale and purchase transactions but is also used as a mining, so research aims to determine the security of bitcoin[1].

The addresses on the bitcoin is like a key for the bitcoin to be known and usable, bitcoin addressing is designed so that bitcoin can not be known by others[3]. The bitcoin address is unique, the address is created using cryptography type Base58Check and SHA-256[3].

A bitcoin address is the same as an email address that serves to receive and store bitcoins. If an email user has only one email addresses while bitcoin users have multiple addresses. Bitcoin addresses usually have 26-35 characters and it’s made very unique.

1MgErLiH1DuGMrd58fuL4CLQHe4VSboqKn

Figure 1. Example of bitcoin address

The address contains several numbers and letters. The bitcoin address has an error-checking code called checksum. The computations on the checksum will detect addresses that have one faulty nature. This process helps to prevent errors when sharing our address. Usually wallets do validation and reject if address is wrong.
Figure 2. Example of address validation

From both instances the address resembles a valid address but the second address is invalid at checksum. Both have the same resemblance except for the letter N that is at the end of the second address[5].

Table 2

| Input                     | Hash sum       |
|---------------------------|---------------|
| Fox                       | DFCD3454      |
| The red fox runs across the ice | 52ED879E      |
| The red fox walks across the ice | 46042841      |

Figure 3. Illustration of hash function[8]

Base58 is a binary-encoded text format developed for use in bitcoins and is widely used in cryptocurrencies. Base58 also offers a balance of compact, readable, and error detection 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, Base58Check is a Base58 encoding format, often used in bitcoins that have built-in error checking codes. 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[7].

Figure 4. Illustration of Base58Check encoding process[7]

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 to combine address bitcoin from public key sender, and whether
the address is including safe or not[4]. Testing aims to test whether the bitcoin blockchain system is running well or not. Is the bitcoin blockchain address system secure. This flowchart explains how the research is done as follows.

![Flowchart](image)

**Figure 5. Flowchart**

In the flowchart above the first step is to process the SHA-256 and Base58Check algorithm after which the processing that occurs that the address will be combined with the public key will be in hash with SHA-256 algorithm, then after the address has been in the hash with SHA-256 will checksum with Base58 encoding. Then after the new Base58 encoding will be formed onto the final format of the address that is Base58Check.

### 3.2. Implementation

Implementation of address at this stage is that transactions can be done and address serves as a tool to deliver transaction results. Address is made by using public key and then in hashing to be the correct address format.
Figure 6. Generate address results

Figure 6. shows that the bitcoin address has been created, basically the address has several stages to be formed into the address with the correct format. Format for the correct address is Base58Check, whereas to make the address required public key that has hexadecimal format, it needs hashing for the address can be converted to SHA-256 code. From the result of hashing that becomes SHA-256 code will be checksum 32 bytes, after the result obtained then will be checksum again with 4 bytes. From the results in checksum 4 bytes, then will be generated by using the library of Base58Check format. Then the address will be generated which can be seen in Figure 6.

Verification Key : 002053060e600097fead4f753b5ca845e371ac5284
dcc9bfc03bd004808ca615ff059722e632baeeec44c69536b5d016130853f6599
dcc9bfc0
this is your full checksum 32 bytes
this is your checksum 4 bytes : 002053060e600097fead4f753b5ca845e371ac5284dce9bfc0

Hashed public key : 002053060e600097fead4f753b5ca845e371ac5284
dcc9bfc03bd004808ca615ff059722e632baeeec44c69536b5d016130853f6599
this is your full checksum 32 bytes
this is your checksum 4 bytes : 002053060e600097fead4f753b5ca845e371ac5284dce9bfc0

Figure 7. Address creation process

In the application design result created for the transaction, then the address is inserted into a wallet application to know the identify of bitcoin user.
If the user wants to make a transaction then the user must fill the account box with the recipient address so that the bitcoin sent is successful. Here the sender must also know the address of the recipient.

If the transaction is successful it will be displayed as shown in Figure 10. and the balance of the bitcoin of the user will be reduced. If the recipient’s address is invalid, then the transaction status column will show “Transaction Failed”. 
After the transaction is successful then the data will be sent to the database in the form of record results from transactions containing information in the form of bitcoin sent, byte on the public key, and public key hash that contains the address of the recipient.

![Transaction BitCoin](image)

**Figure 10.** Transaction delivery succeeded

Once the record is sent to the database, the database will contain information such as the table containing the delivery record that has been done before. In the database is also known in the form of a note about the address used during the transaction process. Such a process is called blockchain where the delivery process will be related to the previous one, the security gained in the blockchain is also very useful because all the shipping process will be recorded in full.

**Table 1.** Blockchain Database

| Kode_Transaction | Sender  | Receiver | Bitcoin value | Time_stamp        |
|------------------|---------|----------|---------------|-------------------|
| 53bf2502         | 16ByDscY2dMnCfwMdJviV2CBcbauHqaZJ3 | 1PoDhtBLLLHbx5rhZXTc1DapsqA3dkAwCjK | 5              | 2017-06-03 14:09:59.27481 |
| 6d71fa0a         | 16ByDscY2dMnCfwMdJviV2CBcbauHqaZJ3 | 19sacEBHM2HxC2iB9uVFXjzMe4Yjm1Smih | 3              | 2017-06-04 11:21:40.40417 |
4. Analysis
In this section the test results that have been done is to find out whether the address bitcoin is safe for delivery bitcoin. In bitcoin security system is located on private and public key as well as the address. To generate the address required public key, while the path to send bitcoin is required also address so that bitcoin will be sent right to the receiver.
Address is made using public key for the security of user data is maintained, the format of the address has also been encrypted. Address encryption begins with the public key format which then in hashing first, after in hashing then the format will change to SHA-256. Then SHA-256 will be checksum 2 times, the first with a 32 byte checksum and then followed by a 4 byte checksum. Then the result of the 4 byte checksum will be encrypted into Base58Check code.
The security of the address is also aimed at the ability of Base58 to use large and small fonts and numbers, to add extra security to typos or transcription errors. The Base58 encoding also has a built-in error checking code, when presented with Base58Check code, the decoding software will calculate the checksum of the data and compare it with the checksum already included in the code. So if both do not match, will indicate that the error is known and the Base58Check data is invalid.
So with this security address on bitcoin is located on the public key and checksum process that can make into Base58Check code. By encrypting the public key that is converted into the address then the transaction will be safe and run well.

5. Conclusion
The conclusion that can be in this research is that way to get address that is by using public key and then used hashing method to make public key to SHA-256 code, after in hashing become SHA-256 then checksum will be 32 byte and 4 byte. Once encoded into the checksum the result becomes a valid Base58Check code used for an address in bitcoin.
In performing address transactions are also required for successful transactions. The process in the blockchain output also show the Pubkey Hash in the contents of the address of the recipient and after arriving at the database all the delivery results that occur also indicate the address of the sender and receiver are also recorded well without any changes made, which where the address is safe and encrypted with good.
The security of the address is also indicated by the encoding of Base58 which has a built-in error code, that is, when presented with Base58Check code, the decoding software will calculate the checksum of the data and compare it with the checksum already included in the code.

References
[1] Reinhard Denis Najogie, mei 2013, “Analisa Keamanan Bitcoin”. Program Studi Teknik Informatika. Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.
[2] Danielle Drainville, 21 Desember 2012, “An Analysis of the Bitcoin Electronic Cash System”. University of Waterloo
[3] Nicolas Dorier, Will Bill Strait, 10 Januari 2015, “Blockchain Programming in C#”
[4] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.
[5] Richard Caetano, 2015, “Learning Bitcoin: Embrace the new world of finance by leveraging the power of crypto-currencies using Bitcoin and the Blockchain”.
[6] Dody Dharma, “Studi Perbandingan Penggunaan Algoritma Hash SHA-256 dengan Simetrik dan Asimetrik Chipers dalam Perancangan Secure SWF Rich Internet Application (RIA)
[7] Andreas M. Antonopoulos, 2015, “Mastering Bitcoin”
[8] Rama Febriyan, “Perbandingan Digital Signature Algorithm dan Elliptic Curve Digital Signature Algorithm”. Institut Teknologi Bandung.

[9] Andreas M. Antonopoulos, 2015 “Bitcoin & The Blockchain”. O’Reilly E-Book Advantage.