Message Authentication Code

Chang Liu[1], Liyan Jiang[1], and Yiwen Yang[1]

[1]Group 4, VE475, UM-JI

July 31, 2022

Abstract

Bitcoin system, as a totally digital payment system, possesses many advantages over cash payment and traditional digital currency system. These advantages are the result of its subtle construction based on a combination of many advanced cryptographic algorithms. To investigate how those cryptosystems are involved, and how they result in the advantages, the payment transaction cycle, address generation and weakness of the current setting are closely analyzed from cryptographic perspective. This report more focuses on high-level structure of bitcoin system and shows the reasons for both of its advantages and weaknesses.

Contents

1 Introduction

Cash payment is instantaneous, meaning merchant receives the money at the moment when consumer pays it. It's also somehow anonymous because no information of owner of the money involved in payment is recorded. Besides, it also "cheap", meaning no third-party institution is needed to complete the payment. On the contrary, normal digital currency based on cash is more reliable because transaction is conducted by authorized institutions, which avoids fake money in payment. It's also more convenient because no physical contact is needed to complete payment.

However, Bitcoin system, as a totally digital payment system, inherits all the advantages of these traditional payment system while getting rid of their disadvantages. Bitcoin payment is instantaneous, anonymous and "cheap" as cash, while reliable and convenient as traditional digital currency. Moreover, without relation to cash, issuing currency is also done without any financial institution.

To achieve these goals, many advanced crypto algorithms are taken advantage of. For example, each transaction is based on public key cryptography and digital signature technology, assuring the reliable validity of transaction while preserving anonymity. Besides, bitcoins are essentially solutions to a problem based on hash function, whose difficulties assure the value of bitcoins. Blockchain is subtly constructed on these algorithms, making it possible that all the computation, verification and information storage is achieved together by all the participants.

Though many special designed are applied to increase the security and stability of bitcoin system, due to its great complexity, it still has weaknesses. People are able to conduct attack as regular users, miners or hackers.

2 Anonymity of Users and Transactions

2.1 Generation of Keys and Address

Bitcoin system use public key cryptography to encrypt transactions. To do this, each user has a unique pair of secret key and public key. Because asymmetric encryption algorithm *ECDSA-SECP256k1* is used to encrypt transactions, the private key is a random 256-bit number. Unlike encryption algorithms based on finite field, no primality of secret key is required here. Therefore, key generation is much easier, especially when the number of users is large. Then based on this secret key, the following steps are taken to generate public key and finally the address.

1. The public key $(x, y) = [x]G$ is calculated, where s is the secret key and G is a universally agreed element in the elliptic curve group. Then $0x04$, x and y are concatenated together. Because x and y are also 256-bit numbers, this step gives a 520-bit long output.

2. The *SHA-256* result of the output of the last step is calculated.

3. The *RIPEMD-160* result of the last output is calculated.

4. A 8-bit number indicating version is attached to the beginning of the last output.

5. *SHA-256* is applied the output of last step, whose output is applied with *SHA-256* again.

6. The result of step 4 is concatenated with the first 32 bits of the output of step 5, which is the address of a user in bitcoin system.

7. For convenience, the address given by step 6 is usually expressed in *Base58* form.

2.2 Anonymity of Users and Transactions

First, because public key cryptography is used, the public key can be exposed to everyone. Therefore, every user has a public static address for receiving bitcoins, bringing great convenience to payments. Besides, in the procedure of generating an address, hash functions are heavily used, so the probability of leaking information is eliminated as much as possible.

Second, because all the information about the bitcoins involved in transactions are encrypted with receivers' public key, only expected receivers can decrypt transactions, obtain information about those bitcoins and then use them.

Third, as is shown in the generation process of keys and addresses, the only thing needed is a 256-bit number, meaning no personal information is bound with the address at all. In this way, bitcoin system assure users' anonymity. Consequently, transactions, which only rely on bitcoin system addresses, are also anonymous.

3 Bitcoin Payment Transaction Cycle

3.1 Bitcoin Address

3.1.1 Generation

Every user, in the Bitcoin system, must generate his/her Bitcoin address, in order to do the following:

- receive and make bitcoin payments
- keep the balance of unspent bitcoins

The Bitcoin system is based on public key cryptography, and specifically, Bitcoin uses ECDSA, which guarantees each user two keys, the public one derives the payment address while the private key decrypts the balance.

In principle and disregarding the details, incoming transactions to some user's Bitcoin account:

- are first encrypted by the sender using recipient's public key
- are sent to the sender encrypted
- are received and stored in sender's wallet encrypted
- the corresponding private key is used before each outgoing payment

In other words, the private key is the signature of ownership of the bitcoin in the wallet, and thus private keys are the target for illegal attacks.

3.1.2 Distribution

After completion of all communications that precede a payment transaction, the last step is for passing the address of one's Bitcoin account to the sender. Since the address is originally in the form of incomprehensible strings, the address is usually translated into QR code or E-mail (or some other remote communication protocol).

One thing should be emphasized is that the Bitcoin address must be correct **AND** legitimate, otherwise corrupted address may result in the irrecoverable loss of Bitcoin. However, currently Bitcoin schematic does not have a solution to this problem, especially when the corruption is caused by meet-in-the-middle attack.

3.2 Opening Wallet and making Payment

The encrypted transaction is first sent to the bitcoin network, then distributed. More precisely, it does the following:

- Collect individual transactions for ten minutes
- Each ten minutes, package them, adjust the target parameter based on timing.
- Send them to mining servers.

3.3 Validation of Blocks by Miners

Mining servers distribute blocks prepared by the Bitcoin network to their clients with special software modules, called miners.

After receiving the current block, all miners perform the following procedure iteratively:

- generate random number
- add it to the block
- calculate the hash of such block

For a block to be validated, the produced hash must be in a form such that certain number of its leading bit positions equal to zero.

Another thing to say is that, the process of collecting new transactions and mining or validation of the current block are synchronized.

3.4 Return of Validated Blocks to the Bitcoin Network

When some miner succeeds in creating correct hash for the current block, he/she returns such new block to the Mining Server and further returns it to the Bitcoin network. Usually, when one member of the pool creates the target hash, all members share the reward.

3.5 Distribution of the New Block to all Users

When each node in the Bitcoin network receives new validated block, all Bitcoin wallets of users linked to that network node receive the distributed portion of bitcoin. Each wallet is linked to several of the Bitcoin network nodes for redundancy and availability reasons.

However, after receiving the latest block, the transaction is not 100% validated, as it may be included in the branch of the blockchain that is going to be discarded. This inconvenience cannot be resolved by simple modification of the Bitcoin protocol, due to the inherit properties that root inside the schematic of Bitcoin system.

4 Double Spending Attack

As Bitcoin is becoming popular and attractive for legal transactions by honest miners, there are also several known vulnerabilities of the Bitcoin system, which are causing an increasing amount of illegal transactions. One of the biggest challenges is that these vulnerabilities cannot be solved by simply releasing such small security patches [1], but instead the whole Bitcoin protocol may need to be modified. Since Bitcoin system is working based on the entire Bitcoin community, then everyone in the community should adopt the modifications, which is considered to be very difficult.

Double spending attack is the most famous attack working on *fast* payments [2]. During the execution time between that the sender (attacker) submits the transaction into the Bitcoin network and that the recipient confirms the transaction, the attacker can attempt to spend the same Bitcoin for twice, given that the time interval is short (a few seconds). The attacker achieves this by generating different outputs of the same unspent transaction outputs (UTXO) input, and sending the copies to multiple users. Since there is no trusted entity that verifies the legitimacy of UTXO used as input in a transaction, it is hard for users in a decentralized system to tell the duplicated copies from the original one [3]. The Bitcoin system prevents double spending problems by making users able to validate UTXO, but it does not work when transaction time difference is shorter than the transaction cycle time.

A straight-forward solution to double spending attacks is to announce the transaction immediately to the Bitcoin network after it takes place instead of after ten minutes. However, this solution is considered to be impractical because it will make great modifications to the current version of Bitcoin and the implementation is very complicated to realize [1].

Next, we will describe several conventional attack methods.

4.1 Race Attack

To construct a Race Attack, the attacker needs to create two transactions Tx-A and Tx-R. The two transactions have the same input yet different outputs, and are sent simultaneously to the Bitcoin network. Then they will have the equal probability to be verified in the next block. Since the transactions have the same input, then it is impossible for users to accept both outputs at the same time, so either Tx-A or Tx-R will be stored in the network before the other one. If the majority of users receive the block with Tx-A first, then Tx-A is more likely to be verified first. Race Attack works when the recipient receives Tx-R before Tx-A, which means that the recipient accepts

Tx-R before Tx-A is stored, otherwise the transaction will be rejected. Then the attack is success, and the recipient will find the transaction invalid after Tx-A arrives.

To double the Bitcoin, the attacker should be able to reverse a transaction that already has been stored in the Bitcoin network. To achieve this, the attacker needs a significant share of computational power. While if the number of subsequent blocks that use Tx-A as inputs increases, it becomes extremely hard for the attackers to reverse the transaction, so the recipient should wait until at least six blocks are produce in the network for confirmation [3].

4.2 51% Attack

51% Attack is the largest threat to the Bitcoin system. The attack takes place when the attacker or the pool of users control over half of the total computational power of the system, then it is possible to reverse any blocks of transactions [4]. For instance, suppose the attacker owns 51% of the total computational power, he first releases a transaction into the network, then starts mining fraudulent transaction blocks secretly (not releasing to the network). The merchant waits for a number of confirmations and accepts the transaction, and at the same time the transaction is accepted, the attacker releases the secret blocks to the network. Since the attacker computes much more faster than all other users, then the fraudulent block chain is very likely to be longer than the original chain, which means that the fraudulent chain becomes dominant, while the original one with the transaction disappears, thus achieving the 51% attack.

This kind of attack is not occurring at present, but it is potentially dangerous due to selfish mining. In Bitcoin system, the more computational power the user owns, the stronger he is to solve the hash problem. If users share their computing resources in a mining pool and form a group, then it is selfish mining. Bitcoin system greatly relies on decentralized users, while users in reality prone to enter dominant mining pools so that they have larger chance to receive better rewards, and this violates the Bitcoin concepts. As long as some dominant mining pools form, the Bitcoin system is no longer a completely decentralized system, and 51% attacks can be applied to control the whole transaction system.

5 Conclusion

In this project, we studied the mechanism of Bitcoin and analyzed its advantages as well as weaknesses. We learnt how cryptographic algorithms are used in Bitcoin and why Bitcoin system is better than cash payment and traditional digital currency system. The transaction cycle of Bitcoin is explicitly explained, and double spending attacks against Bitcoin are researched. Through this work, we are able to further expand our knowledge in the vast cryptography area and improve major researching skills.

References

[1] Muftic S, Sanchez Martin JI, and Beslay L. "Overview and Analysis of the Concept and Applications of Virtual Currencies". In: LB-NA-28386-EN-C (print),LB-NA-28386-EN-N (online) (2016). ISSN: 1018-5593 (print),1831-9424 (online). DOI: 10.2788/242242(print),10.2788/16688(online).

[2] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin". In: *IACR Cryptol. ePrint Arch.* 2012 (2012), p. 248.

[3] Ehab Zaghloul, Tongtong Li, Matt W. Mutka, et al. "Bitcoin and Blockchain: Security and Privacy". In: *IEEE Internet of Things Journal* 7.10 (2020), pp. 10288–10313. DOI: 10.1109/JIOT.2020.3004273.

[4] Fredy Andres Aponte-Novoa, Ana Lucila Sandoval Orozco, Ricardo Villanueva-Polanco, et al. "The 51% Attack on Blockchains: A Mining Behavior Study". In: *IEEE Access* 9 (2021), pp. 140549–140564. DOI: 10.1109/ACCESS.2021.3119291.