CIK : A minimalistic wallet implementation for BITCOIN

Computer Engineering Department, METU

Ozlem Ceren Sahin(1746668), Ibrahim Sagiroglu(1819531), Kamyar Ghasemlou(1786896)

Abstract—During recent years cryptocurrency and especially bitcoin(BTC) has been a hot topic with its impact on politics, economics, cryptography and of course the way we perceive the internet. This report is intended to make the reader familiar with the concepts of cryptocurrency and its origins then dive into the bitcoin implementation and provide some key information about the security and the approaches in its design. Finally CIK, a minimalistic wallet implementation by the authors of the report has been discussed briefly.

Index Terms—Cryptocurrency, bitcoin.

1 Introduction

BITCOIN is a peer-to-peer payment system which allows sending electronic cash from one party to another directly without going through a financial institution. The concept of this system was first announced in a self-published white paper by Satoshi Nakamoto in October, 2008 [1] and the code for Bitcoin (BTC) variant was released by Nakamoto as open-source software in 2009. Satoshi Nakamoto is believed to be a pseudonym for an individual or a group of individuals with strong background in economics, cryptography, P2P networks and a world class knowledge of C++ [2] [3].

1.1 Cryptocurrency

A cryptocurrency is a medium of exchange like normal currencies such as USD which uses cryptography for security on transactions, control over the creation of new units (coins) and anti-counterfeiting measures. The security is provided by both using public and private keys when there is a cryptocurrency tranfer between individuals.

Cryptocurrencies are fully decentralized which means government has no control over them. In contrast, in centralized banking such as Federal Reserve System, government controls the value of a currency through the process of printing fiat money.

The first fully implemented decentralized cryptocurrency is bitcoin by Satoshi Nakamoto.

By using timestamping schemes, the need for a trusted third party who timestamps transactions to the blockchain ledger is avoided. The mostly used timestamping scheme is based on SHA-256 and introduced by bitcoin [5].

1.2 Bitcoin

Bitcoin uses blockchain as ledger and , private keys for signing of transactions and mining for processing.

1.2.1 Balance

The purpose of a block is to prevent the same money spent twice by authenticating the timestamps. By observing a block, it is possible to get the information of all transactions. It is compulsory to include the previous timestamps in its hash information for each time stamp. By doing this, the block chains are created.

1.2.2 Transactions

Each transactions consist of 3 important information signed by the sender, for a sender to send bitcoins to a receiver, she must provide that she owns some, for this the sender references unspent past transactions that she has

received an amount greater that or equal to the amount is to be sent, then distributes the total bitcoins she has mentioned between the receiver and herself. e.g. Alice has received 25 BTC from Mary and 25 BTC from John, she mentions these transactions and states that she is interested in sending 30 BTC to Bob and 20 BTC to herself. Then she signs the transaction and sends it to a known miner node. In this instance she has placed the transaction request, and the transaction is not complete. First of all the network should verify that She truely has received 50 bitcoins and has not spent them, then the network should process her transaction to blockchain. It is advised to wait atleast 6 blocks to be processed after the verification of transaction, to prevent double-spending the same transactions. It is important to mention that if any user fails to spend all of the BTCs she has mentioned, the remaining amount will be lost in the blockchain and it is not possible to retrieve lost bitcoins. It is of importance to emphasis that blockchain does not store the balance of account. It uses 'unspent' received bitcoins as balance. This is a measure taken so that generation of blocks with invalid transaction if not impossible, would be almost impossible. In order to verify that a reference transaction is spentable, the node should check blockchain up-until that transaction, and make sure it has not been spent before [7].

1.2.3 Mining

Mining is the process of both the verification of payments and generation of bitcoins. Mining is the component that provides complex mathematical base for the network and makes it decentralized. Mining is aimed to find a hash value to a block of transactions that meets a specific criteria. Set of transactions in the block contains transactions pending approval by the bitcoin network. Miners, try to find a hash for the block containing a nonce and set of pending transactions that meets the criteria that the it starts with a predetermined number of zeros. This pretermined number is knows as difficulty, and larger it is, harder it gets to find such a hash. Currently SHA256 is used as the hash function, but it is possible to change it some time in the future as this algorithm becomes weaker. As stated above, the challenge in bitcoin mining is that the number of the zeroes in the beginning of the hash is increasing at regular intervals, this increase is intended to keep up with phenomenon moore's law describes, that is, as miners with better equipments join the network, it gets harder to compute a valid hash. In bitcoin implementation, in order to ensure that enough computing power is present at any instance for the network to work, each block rewards its 'miner' with agreed number of bitcoins, currently this number is 25, but it decreases by half every 52500 block to prevent inflation. It is worthwhile to mention that in total, there will only exist 21 million bitcoins and after sometime, miners would rely on 'transaction fees' they get from the transactions. In practice, higher the 'transaction fee' gets, the probbility of such a transaction being approved in the first block gets higher. When a solution of a block is found, the client sends the solution to each 'neighboring' node. Each receiver verifies the solution and reflects it to its neighbors [6].

One in a while, two miners come up with different blocks and different solutions for the same block number, in such a case network splits in to two different blockchains, the branch in which the next block number is computed first, prevails. At such a point, any node working on the 'invalid' chain, migrates to the longer one[4].

2 CIK IMPLEMENTATION

In the CIK wallet, we have chosen to use testnet rather than mainnet. Testnet is a network for developing and testing purpose, bitcoin in this network does not have value and network provides free coins for test purpose. Advantage of this network is the fact that bugs would not result.

2.1 Why use an API: chain.com?

In the implementation of CIK, chain.com API is preferred to be used because [9],

- It is the easiest and most cost-effective way to build applications on Bitcoin.
- It offers Test Networks for developers to get started in a sandbox environment.

- For the implementation phase, node with +20 gb of blockchain database is needed.
- Massive overhead hosting a node.
- Many similar services require a minimum fee per transaction.

2.2 Why testnet?

- Free coins for test purposes is preferred.
- By using free coins, there is no financial lose in case of a serious bug.
- It provides faster block generation, thus faster testing.

2.3 Why no mining application?

- It is too complex for the scope of the project.
- With current difficulty of the blockchain, it would be highly unlikely to be able to generate a block with a mainstream computing systems.
- It is not possible to implement an efficient miner without an adequate hardware equipment.
- Miners and nodes have to store the entire blockchain of +20 gb of data. Which is a huge overhead for small project.

3 Conclusion

CIK, which stands for the initial letters of the project members, is a minimalistic command-line wallet for Bitcoin. We have developed CIK, our bitcoin wallet, using an API called chain.com, testnet to obtain free coins and python as a programming language. This project is intended to be as a proof of concept and a really simple implementation to learn from. Some of the decisions were made to make it simple rather than safe, a third-party service is used for the broadcast of transaction.

But why Bitcoin?

The money used today is first come up as paper certificates that prove the gold, silver or any other acceptable commodity in the bank is deposited. The reason of every banknote has a statement ”I promise to pay the bearer on demand” is that anytime the paper can be exchanged with the real gold or silver.

As time goes, central banks with government began printing money which are not in return of any physical commodities like gold or silver, called ”Fiat Money” which have no equivalent of the productivity of economies and that was result in inflation. Many people starts yearning for another currency free from government manipulation and this is how Bitcoin and other digital currencies were born.

Aside from being ”inflation proof”, bitcoin allows you to send money directly to another person without involving any third party, the transaction costs are far less than the traditional systems and people can complete the transfer in minutes. Additionally bitcoins are anonymous which means your identity does not exist anywhere in the system.

The bitcoin and other currencies reach their goal very succesfully because the system is not under control of any third parties, it is under control of the community and protected by cryptography consepts; ”In cryptography We Trust” [8].

References

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*
[2] http://en.wikipedia.org/wiki/Bitcoin
[3] http://en.wikipedia.org/wiki/Bitcoin_network
[4] http://bitcoin-tr.com/bitcoin-madenciligi-mining/
[5] https://bitcoin.org/en/how-it-works
[6] http://dl.frz.ir/FREE/papers-we-love/digital_currency/primecoin.pdf
[7] http://www.coindesk.com/information/how-do-bitcoin-transactions-work/
[8] http://www.zambian-economist.com/2014/02/in-cryptography-we-trust-short-guide-to.html
[9] https://chain.com/docs