2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India

Blockchain – Literature Survey

Akanksha Kaushik
Dept of CSE,
BMS College of Engineering,
akankshak1506@gmail.com

Archana Choudhary
Dept of CSE,
BMS College of Engineering,
choudharyarchu@gmail.com

ChinmayEktare
Dept of CSE,
BMS College of Engineering,
chinmayektare@gmail.com

Deepti Thomas
Dept of CSE,
BMS College of Engineering,
deeptithomas94@gmail.com

Syed Akram,
Asst. Professor, Dept of CSE,
BMS College of Engineering,
syedakram.cse@bmsce.ac.in

***Abstract*— In the modern world that we live in everything is gradually shifting towards a more digitized outlook. From teaching methods to online transactions, every small aspect of our life is given a more technological touch. In such a case "money" is not left behind either. An approach towards digitizing money led to the creation of "bitcoin". Bitcoin is the most efficient crypto-currency so far in the history of digital currency. Ruling out the interference of any third party which monitors the cash flow, Bitcoin is a decentralized form of online currency and is widely accepted for internet transactions all over the world. The need for digital money would be extensive in the near future.**

***Keywords*— Bitcoin, Blockchain, Decentralised Currency, Transaction, Mining**

I. Introduction

The concept of bit coin is in a way difficult to theorize but can be implemented in practice[1].Though it has not been extensively researched and documented it still can prove to be a very strong form of online currency.Bitcoin has its own perks when it comes in comparison to the traditional old bank transactions. It is a decentralized form of currency, in simple terms it means that nobody rules over it. The presence of many redundant copies of the transaction database eliminates any third party rule over the money you own and lets you exercise total control over it, the government can't freeze your money[3].

Transactions are practically untraceable back to the user and also taxation cannot be imposed on this process since the ownership address can be changed only by the owner it is impossible to steal bitcoins[3].Counterfeiting of crypto currency is almost impossible because of the efforts of cryptography and encryption algorithms[10]. Thus bitcoin can pave to be a breakout in the field of digital currency further it is simple to use a bitcoin wallet is similar to the wallet in the back of our pockets. It generates a bitcoin address which can be shared so that others can deposit cash to that address. Their usage is restricted to one time which makes them secure [11]. A certain secret key is owned by the bit coin wallets and is used to sign the transactions. The transactions are digitally signed which make minimal to no room for any alterations to be made, thus security plays its role again [11].The transactions are broadcasted among all the users and get confirmed by a process called mining [11].

The block chain is a shared public ledger [11]. The complete bit coin network depends on the block chain. The block chain includes all confirmed transactions. The bit coin transaction process extensively makes use of some of the cryptography techniques such as elliptic curve cryptosystem (ECC). The encryption techniques used in this algorithm make use of public and private keys and are proved to provide security during the entire transaction process. Now coming back to the process of mining, it is a distributed consensus system. The pending transactions in the block chain are confirmed through this process. We would read in detail all about the different bitcoin ideologies in the coming sections.

II. Comparison of Centralization/Decentralization

Centralization is a process where the authority to make decision lies in the hands of only a few, in other words, "Centralization" is the consistent and systematic way of entrusting authority to people who are in the centre of the organization. The world's financial system that uses national fiat currencies which are created and managed by government sponsored central banks is a centralized way of dealing with currency [13].

Whereas a decentralized structure is independent of any centralized authority and therefore eliminates the need for a central bank. In the case of bitcoin, every user in the network has a copy of a record/ledger that keeps track of all transactions happening in the bitcoin network and their ownerships. As every user in the network has a copy, it is considered to be a distributed ledger and in bitcoin network, this is achieved using blockchain [13].

The traditional banking system is based on the concept of coercive centralization. This is because the entities with the authority over money's creation, regulation, and transfer have the will and the power to hurt you if you disobey and transfer of money takes place only with the permission of those who are in control. Whereas decentralization is based on Market-based centralization whose main feature is the ability to opt out. Fiat user is always forced to utilize a centralized service, unlike bitcoin user. This is the key difference between centralization found in Bitcoin and centralization found in the traditional banking industry [13].

With centralized currency, since the authority lies in the hands of a single entity they can set the rules and can change them at their will, adjust inflation like it is needed and even access client money if necessary. With Bitcoin, the each and every client knows rules by which the system operates, the way it works and the amount of money that can be created. Hence rules cannot be changed without the approval of the clients, every single one and not just the miners [14].

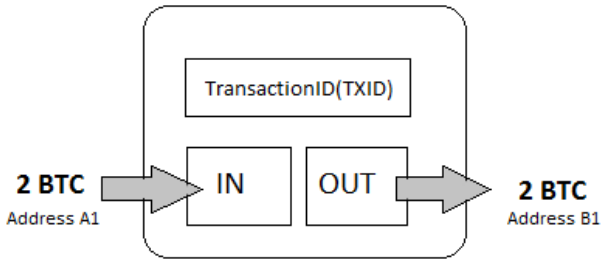
978-1-5090-3704-9/17/$31.00 © 2017 IEEE

Funds required maintaining the servers that run the banks, as well to maintain physical security and manpower is too high in the centralized banking system. The funds needed to maintain all of the bank's personnel, technology, weaponry stuff, and vehicles that make up our legacy banking systems are extreme compared to the amount required for generating the bitcoins and mining them [14].

Decentralization has its own set of disadvantages over centralized banking systems. Decentralized currency might cease to exist. There is no way to finding out if it will persist in future or not. There are people who have loaded up the bitcoins in hope of profiting in future, but if people eventually start to get bored of it and find it inconvenient, all the investors will face heavy losses [15].

Since decentralized currency allows parties involved in

Fig 2. Private Keys in Wallet



transactions to be anonymous, there is always a chance that government might intervene in this world to get hidden information [15].

Other risks include security. To deal with decentralized currency it is a necessary that we have a wallet. If we lose even the minute details there is a chance that we might lose all our investment as well and since it is virtual investment all our money literally disappears into cyberspace. In addition, we might have to deal with the problem of hacking. If we are sloppy with the way we deal with our wallet the hacker gains control of our account and misuse it [15].

III. Components of Bitcoin

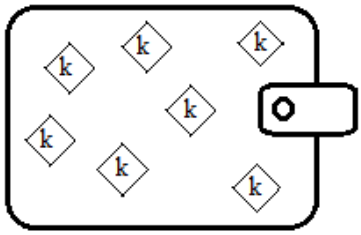


Fig 1. Blockchain

A. Block chain

The block chain is a shared public ledger that records all confirmed transactions. It consists of blocks that hold batches of valid transactions[7]. Each block includes the hash of the previous block,

linking the two. Thus, the linked blocks form a chain. Blockchain eliminates the risk of data being held centrally. The use of public and private keys is the basis for decentralization. The user's address is a public key and users get access to their Bitcoin or other digital assets through the private key which is like a password. Massive database replication maintains data quality.

Cryptography enforces the integrity and chronological order of the blockchain. Blockchains are made secure through cryptographic technology[5].

B.Bitcoin Walle

A user needs a wallet in order to use a Bitcoin. The wallet holds a public key pair that represents the user's account. There is a private key for every Bitcoin address that is saved in the Bitcoin wallet of the person who owns the wallet. A wallet allows you to receive bitcoins, store them, and then send them to others [8]. There are different types of wallets such as software, hardware, paper, brain and online wallets. One of the most common ways to use Bitcoin is through a Software Wallet.

B. Bitcoin Transactions

Participants in a Bitcoin network engage in transactions

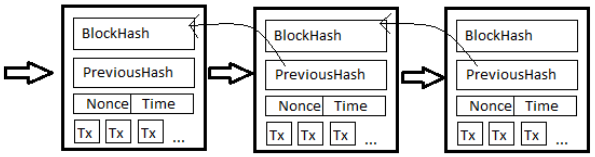


Fig. 3 Bitcoin Transaction

through a collection of Bitcoin addresses (called the wallet). The most detailed level of reporting recorded on a Blockchain is a transaction. Thus a transaction is an atomic record in the ledger. One or more sending addresses and one or more receiving addresses along with how much is sent and received by these addresses are involved in each transaction record. The transaction process in the Bitcoin network guarantees that each transaction verification is distributed among multiple participants in the network, each transaction record is cross-checked by multiple nodes and that transactions are ordered consecutively with linearly ordered timestamps[9].

A hash value as the transaction identifier (TXID) and a list of inputs and outputs constitute the key elements of a transaction. In a transaction, the hashes and references to previous block hashes take on the role of serial numbers. This eliminates the need for serial numbers as are used in other digital cash systems [4].

IV. Security Analysis

Motives to exploit the weaknesses of Bitcoin always exist as it is a digital currency with a notable market value. Apart from double spending there also exists among the attack vectors key recovery and transaction malleability. However, the most feared attack is the so-called 51% attack. Some of the fundamental properties of Bitcoin can be explored while discussing these attacks[4].

Bitcoin is a decentralized cryptocurrency which has seen a massive growth in popularity and volume of transactions[16]. This growth underpins increased risk with this currency. To alleviate this risk, cryptocurrencies require an in-depth security analysis of the various components that interact with their financial networks. Side channels are often overlooked when designing systems. Side channel risks can be exposed through security analysis. [16]

A. Double Spending Attack

Cheating in a transaction can be done through double spending. Double spending is the result of successfully spending some money more than once. Transferring a certain number of Bitcoins to one person and transferring the same exact Bitcoins to another person, simultaneously, by a user is known as double spending [17]. The existing solution for this attack is blockchain which lets the users know what transactions count and can be trusted. Having a timestamp server is a better solution for preventing this type of attack. A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash. The timestamp proves that the data must have existed at the time.

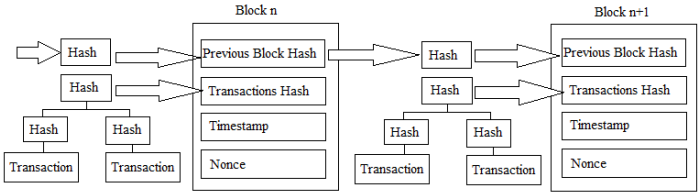


Fig.4 Blockchain structure with timestamp

B. Brute Force Attack

Brute-force attack can be used to attack keys generated by improperly-configured random number generators and can also be chosen to attack poorly-chosen brain wallets. Brute Force Attack is nothing but an exhaustive key search [16]. Every Bitcoin public address has a Bitcoin private key meant for it. The algorithm used for the computation of the private and public (which is the associated address) keys is ECDSA (Elliptic Curve Digital Signature Algorithm). Theoretically, a brute force attack should work. We have to brute force the ECDSA, which requires solving 2^256 (as the private key is 256 bits) operations to find the private key and this is computationally unfeasible [18].

C. Finney Attack

The Finney attack is named after Hal Finney. It is a double spending attack with the following features: It only works if the merchant accepts unconfirmed transactions. It still works, however, if the merchant waits a few seconds to verify that everyone in the network agrees he was paid. It requires the attacker to be mining and controlling the content of his blocks; however, he can, in theory, do this with any hash rate, in particular significantly less than 50% of the network hash rate. The only way to protect oneself against such an attack is to make at least one conformation per transaction before sending out the purchased goods and repeating this process for every transaction [18].

IV. Wallet and Cryptography

The first thing a user needs in order to use a Bitcoin is a wallet. The best approximation of a user's the account is a public key pair that is held in the wallet. It is therefore very essential to secure the wallet [12].According to common Bitcoin terminology; there are a variety of wallet types such as software, hardware, paper, brain and online wallets. The most common ways to use Bitcoin is through software wallets. A locally running Bitcoin instance is necessary for a software wallet. In the case of online wallets, a hybrid approach is followed where most operations are performed on the client side and the wallet is encrypted. If an attacker gains access to a targeted machine he can also access the user's wallet and thus this makes online and software wallets prone to security concerns [4].Another class of wallets is hardware wallets which follow the concept of using a separate device that operates offline. It is much harder for an attacker to access this wallet because it is not directly connected to the network [4]. Brain and paper wallets are more secure. The former requires the user to store the keys in their mind by memorizing a passphrase while the latter stores key holding the coins as a physical document [4].The Bitcoin protocol makes great use of the elliptic curve cryptography (ECC), in order to secure transactions.

V. Implementation Parameters and Constraints of Bitcoin

The following are the implementation parameters and constraints of Bitcoin:

A. Peer to Peer Network

Basically, bitcoin is implemented as a peer-to-peer network (P2P) architecture on top of internet layer. By peer-to-peer, we mean that no client in the network is superior to other and that all share burden of providing network services. Nodes in the network are interconnected by a flat topology i.e. there is no server, no centralized service and no hierarchy in the network. Hence bitcoin network is inherently flexible and decentralized. Nodes in a peer-to-peer network (P2P) does both that is provided as well as consumer services at the same time. This reciprocity acts as the incentive for participation [20].The concept of a P2P network is similar to how the information is shared among friends. If data is shared with one client of the network, eventually this will reach every other member of the network without being altered in any way [19].

B. Security Constraints

a) Hashing

Understanding how cryptographic hashing works is necessary in order to understand digital identities. The process of mapping digital data of any arbitrary size to data of a fixed size is known as hashing. An important feature of a hash value is that it is very difficult to derive the original input number without knowing the data used to create the hash value [19].

A good hashing algorithm needs a few requirements such as:

i. The hashing algorithm must have a fixed output length(256 is a good value for this)
ii. The smallest change in input data must produce a notable difference in output
iii. Same input will always produce same output
iv. There must be no way to reverse the output value to calculate the input
v. Calculating the HASH value should not compute intensive and should be fast

Hence it can be seen that hashing ensures a good level of security.

b) Digital Signature

For a digital signature, all you need to do is append your personal data to the document you are signing. Hashing algorithms comply with the rule that even the smallest

change in input data produces a significant difference in output, therefore it is obvious that the HASH value created for the original document will be different from the HASH value created for the document with the appended signature. A digitally signed document is the combination of the original document and the HASH value produced for the document with your personal data appended [19].

You need to make sure that your signature cannot be copied, and no one can perform any transaction on your behalf. The best way to make sure that your signature is secured is to keep it yourself and provide a different method for someone else to validate the signed document. Public-key cryptography also known as asymmetric cryptography is what is needed to be used to ensure security. For this to work, a private key and a public key has to be created. These two keys will depend on each other and be in some kind of mathematical correlation. The assurance that each private key will have a different public key is guaranteed by the algorithm that you will use to make these keys. A public key is an information that you will share while a private key is an information that you will keep to yourself. You can be sure that no one else can produce the same HASH value for a particular document if you use your private key (your identity) and original document as input values for the signing algorithm to create a HASH value, assuming you kept your key secret. If anyone needs to validate your signature, he or she will use the original document, the HASH value you produced, and your public key as inputs for the signature verifying algorithm to verify that these values match [19].

C. Bitcoin Constraints

a) Transactions

To start sending information to the peers in the bitcoin network it is necessary that we have P2P communication, mechanisms for creating digital identities (private and public keys), and ways for users to sign documents using their private keys. And because there is no central authority to validate the user and his balance the system asks user details every time to check if you have lied or not. The transaction record has an entry of sender, receiver, no of bitcoins sent, timestamp etc. Next thing to do is to digitally sign the transaction record with your private key and transmit the transaction record to your peers in the network. At that point, everyone will receive the information that a particular peer (sender node) is sending money to someone other peer (destination node). The transaction is validated before the funds are sent to destination node[19].

b) Miners

Miners are core components of bitcoin network system .Validation of a transaction is done by miners. Also, they are responsible for mining node transactions, competing in the mining process, validating transactions, and creating new blocks. To validate transaction miner does two things. They rely on the fact that every transaction executed in the system is duplicated and made available to any peer in the network. They also check if the sender client has enough amount to initiate the transaction. Once your account balance is confirmed, a specific hash value will be generated by the miners. This hash value must have a specific format and it must start with a certain number of zeros.

The two inputs for calculating HASH value are:

i. Transaction record data
ii. Miner's proof-of-work

When the proper value for proof-of-work is found by the miner, he or she has rewarded a transaction fee, and this can be added as part of the validated transaction. Blockchain, a specific database format, has in it stored every validated transaction that has been transmitted to peers [19].

VI. Conclusion and Future work/scope

With the world becoming more and more digitalized by the day, the concept of digital currency is gaining momentum. Bitcoin is a decentralized form of online currency and is widely accepted for internet transactions all over the world. And these transactions are stored in a distributed database called Blockchain that keeps a permanent and tamper-proof ledger of transaction data. It makes creating and sharing of a digital ledger of transactions similar to bank ledgers. Unlike bank ledgers, blockchain records are not controlled by any central authority. The ledger file is shared among all the participants on the network called miners. Trust is achieved by using cryptography and with a large number of users. It enables borderless, permission free, fast and cheap access to the world of finance. Bitcoin provides the vision of a new era in the financial world.

References

[1] *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies* Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten Princeton University, Stanford University, Electronic Frontier Foundation, University of Maryland, Concordia University

[2] Bitcoin:Network Based Currency and its Self-Organizing Emergency

Michael PAETAU, Center for Sociocybernetics Studies, Bonn, Germany

[3]http://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/DigitalCurrencies/advantages/index.html

[4]Florian Tschorsch and BjörnScheuermann: "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies"https://eprint.iacr.org/2015/464.pdf

[5]https://en.wikipedia.org/wiki/Blockchain(database)

[6]http://bitcoin.stackexchange.com/questions/4974/what-is-a-double-spend

[7]https://bitcoin.org/en/how-it-works

[8]http://bitcoinsimplified.org/get-started/how-to-set-up-a-wallet/

[9]Anton Badev and Matthew Chen: "Bitcoin: Technical Background and Data Analysis"https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf

[10]http://idiotsguidetobitcoin.com/images/Idiots_Guide_to_Bitcoin_v1.0.pdf

[11]https://bitcoin.org/en/how-it-works

[12]https://en.bitcoin.it/wiki/Securing_your_wallet#Introduction

[13]https://bitcoinmagazine.com/articles/bitcoin-truly-decentralized-yes-important-1421967133/

[14]https://www.quora.com/What-are-the-practical-advantages-of-the-decentralization-feature-of-Bitcoin

[15]http://liquidthink.net/pros-cons-decentralized-currency

[16]https://static1.squarespace.com/static/53168f6ce4b0ee73efea0c2a/t/53c5cc86e4b0cf6b53648339/1405471878208/Bitcoin+Mining+Security-+Deja+vu+Security+-+2014.pdf

[17]http://ece.gmu.edu/coursewebpages/ECE/ECE646/F15/project/F15_Project_Resources/F14_Bitcoin_report.pdf

[18]http://ece.gmu.edu/coursewebpages/ECE/ECE646/F14/project/F14_presentations/Session_I_Electronic_Payments/1_Bitcoin.pdf

[19]https://www.toptal.com/bitcoin/cryptocurrency-for-dummies-bitcoin-and-beyond

[20]http://chimera.labs.oreilly.com/books/1234000001802/ch06.html#_peer_to_peer_network_architecture