Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Bitcoin Technology: A Peer-to-Peer Digital Cash Transaction

Madhumita Santra, Kanij Fatema Aleya, Supriya Maji, Asoke Nath
Department of Computer Science, St. Xavier's College (Autonomous)
Kolkata, India

Abstract: ***A worldwide decentralized digital currency system which is used to transfer funds online between parties. This online payment system is not controlled by government and any institutions. It sends values directly from one party to another. It is introduced as a peer to peer version of electronic currency system in 2009 by developer Satoshi Nakamoto. It is fast, safe and anonymous way to send money. This survey focuses on the technology used in Bitcoin. Here the author highlights the use of cryptography for the purpose of transaction security and distributed maintenance of a ledger in Bitcoin technology and also describe how Bitcoin technology works. In this document the author discuss some of the portion of bit coin technology which is used.***

Keywords: bitcoin, blockchain, digital signatures, bitcoin wallet.

I. INTRODUCTION

While traditional online payment system or transaction processes are dependent on financial institute as trusted third party to process electronic payments, Bitcoin is the first online payment system, held electronically, which is decentralized, that is, this system is not dependent on financial institution or any government. It is fast, safe and anonymous way to send money. This concept of peer to peer digital cash system was first mentioned in 2008 in a research paper published under the name Satoshi Nakamoto. It was first implemented in 2009. It uses peer to peer technology and transactions take place between users directly without any intermediary. In traditional online payment system transactions are verified by the financial institute but in bitcoin transactions are verified by the nodes and recorded in the public distributed ledger called block chain. Bitcoin is both a network protocol-Bitcoin and also a unit of account (digital asset)-bitcoin. Bitcoin is a network that enables a new payment system and a omplete digital money. It is a complex scheme whose implementation involves some cryptographic algorithms; this is why, it is also known as crypto-currency. Users can buy, send and receive bitcoins electronically for a normal fee using wallet software on a personal computer or mobile device. As a new user one can get started with Bitcoin without understanding the technical details. Once user installed a Bitcoin wallet in his/her computer or mobile phone, it will generate his/her first Bitcoin address and he/she can create mode when he/she need one. One can disclose his or her address to their friends for transactions. But Bitcoin addresses should only be used once.

II. BACKGROUND OF BITCOIN TECHNOLOGY

As a protocol Bitcoin is open for all to send values between any computers which are connected through the internet. Bit coin is called open tool for sending values because when a user wants to send or receive values via bit coin there is no need to get approval or access from an institution. To transfer bitcoins, the only requirement of the user is to download and run free software on the computer. Bitcoin protocol is accessed with the software like bitcoin wallets and bitcoin mining clients. Bitcoin software is not produced by a single institution. In Bitcoin technology, it maintains some rules which is known as consensus rules. It is a particular software rule which are used to reject attempt to create fraud on the Bitcoin network by either- (i) attempting to spend coins from an address whose key do not controlled by the user, and (ii) attempting to double spend coins i.e. send someone coins that the user have already spend elsewhere in previous transaction. If any client tries to commit fraud he is fail to achieve desired result because other nodes in the network would ignore any actions of the client which are violate the fraud preventing consensus rules. Bitcoin has its own metric for value called a bitcoin. There is no physical bitcoins and no any bitcoin software files. Instead of that a bitcoin is a chain of digital signatures stored in a public ledger called blockchain. In the following section there are some descriptions of some keywords related to the Bitcoin technology.

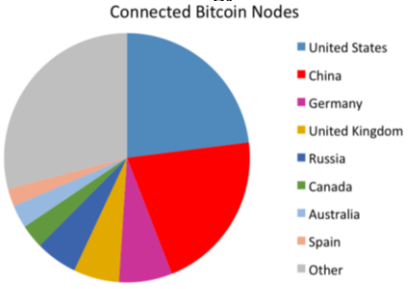

Fig 1: Pie chart of nodes that are connected to the Bitcoin network [7]

A. Blockchain

All Bitcoin transactions that have ever been executed are stored in a public ledger called blockchain. The size of the blockchain is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order. Each user who is connected to the Bitcoin network and performs the task of validating and relaying transactions gets the copy of the blockchain. It has complete information about the address and their balances right from the genesis block to the most recent completed block. Since it stands as proof of all the transactions on the network it is seen as a main technological innovation of Bitcoin. The blocks are not randomly placed in the blockchain, they are linked to each other like a chain with every block containing a hash of previous block. The final digital signature in a given chain will be that of the current holder of a bitcoin amount and the holder will be recognized by the network by a random but unique string of characters which is the user's public address.

B. Bitcoin Mining

It is the process by which verified the bitcoin transactions and information about those transactions is stored in the blockchain. It is also a process through which the new bitcoins are released. Anyone who can access through the internet and has suitable hardware can take part in the mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. . The participant who first solves the puzzle gets 25 BTC as reward. Bitcoin miners stored the information of the transactions in the block and verify them if the transaction is valid or not, if it is valid then select the header of the most recent block and insert it into the new block as a hash. After that solve the proof of work problem when the solution is found the new block is added to the local block chain and circulate to the network.

C. Bitcoin Wallet

Bitcoins are stored in the Bitcoin wallet. A wallet is a randomly generated string of numbers which consists two parts: the public key and private key. The first half of the Bitcoin wallet is known as public key and the second half of the Bitcoin wallet is known as privet key. The public key of the wallet is known to all. But the private key is intended only to the wallet owner. Only the wallet owner can access the private key. If anyone gets a hold of private key of any other user's, they will have access to all their bitcoins. There are three different types of Wallets.

Online Wallet: It is used to store the digital keys on the Web. It means that Bitcoin wallet is stored not on the computer, but on some faraway server of service provider. There are different online wallet providers. And depending on the provider, features of Bitcoin wallet can vary. The main advantage of online wallet is that it enables the users to enter the wallet in any place of the world. Online wallets are very easy to start using and have simple interface. Considered safe, but still susceptible to network failures and hacking. Someone can take measures to increase security.

Local Wallets or Offline Wallets: A local wallet is an application that can be downloaded to the personal computer. Private Keys are stored locally on the hard drive. Considered safe, yet is important to make backups of the private keys in case that hard drive fails. Also carries a risk of hacking or physical theft. There are safeguards to make this method more secure.

Paper Wallets: A paper wallet is a public/private key that is generated offline and printed on a physical piece of paper and then stored in a safe location. Arguably the most secure way to store your BTC. No record of the private key online or your hard drive. It is impossible to be hacked. They are still susceptible to theft, fire and water damage.

III. CRYPTOGRAPHIC METHODS USED IN BITCOIN

Bitcoin is also called as crypto-currency system because its implementation involves some encryption methods of cryptography to regulate the generation of units of currency and verify during the transfer of funds. To protect Bitcoin transaction process from intentional threats or fraud it uses two cryptographic schemes: digital signatures and cryptographic hash function. Digital signature is used to exchange the values between parties and the cryptographic hash function is used while writing transaction records in the public ledger (blockchain). Below the author discuss about these two cryptographic methods.

A. Digital Signature

This asymmetric key or public key cryptographic algorithm ensures integrity, authentication, and non-repudiation between senders and receivers. The implementation of digital signature involves pair of keys i.e. public key and private key. In digital signature when the sender wants to send some message to someone he/she encrypt the message using its own private key and sending the encrypted message. After receiving the message receiver first verify the authenticity of the message and open the message using sender's public key.

The Bitcoin protocol used the above scheme to sign and verify the transaction messages. In particular, transaction message (m) is signed with the private key (P_a) and then broadcast to the bitcoin network. All members of the Bitcoin system can verify that this transaction came from the owner of public key (P_k) by taking the message (m), signature (c), and public key (P_k) and running the verification algorithm.

When a user said A wants to send bitcoins to B using the Bitcoin network they must have Bitcoin addresses. Each Bitcoin address has its own public key and it is identified by its public key. When A sends bitcoins to B, first A signs the transaction using its own private key and send it. Now the message is broadcasted in the Bitcoin network. Every node (users) present in the Bitoin network can see the transaction and verify that is it A who sends the message or not and it also check that there is enough fund to complete the transaction. The users verify the transaction using A's public key

and the signed message and depend on that the transaction is accepted or rejected. After verifying the transaction, all the information about the transactions is stored in the public ledger using another cryptographic method called hash function.

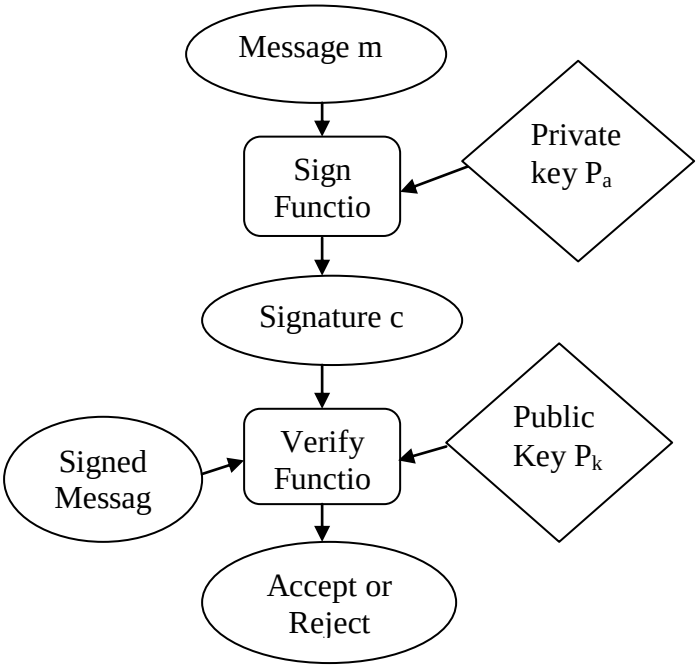

Fig 2: Digital Signature technique.

According to the features of Digital signature, after issuing a message the users cannot deny it and no one could pamper the message. It does not provide confidentiality but it provide authentication. In Bitcoin a specific class of digital signature algorithm used to sign transaction, is called Elliptical Curve Digital Signature.

Some features of Elliptical Curve Digital Signature Algorithm are-

1. Private Key: A secret number, known only to the person that generated it. A private key is essentially a randomly generated number. In Bitcoin, someone with the private key that corresponds to funds on the public ledger can spend the funds. In Bitcoin, a private key is a single unsigned 256 bit integer (32 bytes).

2. Public Key: A number that corresponds to a private key, but does not need to be kept secret. A public key can be calculated from a private key, but not vice versa. A public key can be used to determine if a signature is genuine without requiring the private key to be revealed. In Bitcoin, public key are either compressed or uncompressed. In Bitcoin, public key are either compressed or uncompressed. Compressed public keys are 33 bytes, consisting of a prefix either and a 256-bit integer called *x*. The older uncompressed keys are 65 bytes, consisting of constant prefix followed by two 256-bit integers called *x* and *y* .The prefix of a compressed key allows for the *y* value to be derived from the *x* value.

3. Signature: A number that proves that a signing operation took place. A signature is mathematically generated from a hash of something to be signed, plus a private key. The signature itself is two numbers known as *r* and *s*. With the public key, a mathematical algorithm can be used on the signature to determine that it was originally produced from the hash and the private key, without needing to know the private key.

B. Cryptographic Hash Function

In general, a cryptographic hash function takes as input a string of arbitrary length and returns a string with predetermined length. Users will refer to the input as message m and the output as hash h. The function is deterministic, meaning that the same input m will always give the same output h. Some features of hash function is stated below-

1. Pre-image resistance: Given a hash h it is difficult to find a message m such that hash(m) = $h^{.20}$

2. Second pre-image resistance: Given message m1 it is difficult to find a different message m2 such that hash(m1) = hash(m2). In other words changing the message leads to changing the hash.

3. Collision resistance: It is difficult to find two different messages m1 and m2 such that hash(m1) = hash(m2).

Another desirable property of the hash function is that even small changes in message m are likely to change hash h=hash(m) significantly. This makes it very unlikely for someone to be able to infer the content of the message from the hash. In summary, the output of hash functions is very much unpredictable (looks random) although it is deterministic. [1]

In Bitcoin technology, after verifying the transaction the block chain is updated. The hash function is used to update the public ledger called block chain after each transaction. Hash function is used in Bitcoin technology as following way-

When a transaction is made a block of newly broadcast transactions is used as an input into the cryptographic hash function to obtain a hash or digest then group the transactions which have been broadcast in the last record on the block chain. After that, the digest, with a nonce and the hash of the previous block used as the input of another hash function that produce a new block in the blockchain. In Bitcoin network the users compete to each other to record the transaction in the blockchain. Whoever first complete the task and solve the proof of work got a reward of 25BTC. This information of that transaction stored in the next block of the blockchain. Bitcoin mainly uses SHA-256, a type of Secure Hash

Algorithm (SHA-2) designed by the National Security Agency and published by the National Institute of Standards and Technology.

IV. CONCLUSION AND FUTURE SCOPE

Bitcoin could play an important role in transforming financial services and other industries. From the survey about Bitcoin technology, conclude that it is a new technology and there is a lot more to bitcoin. In this documentation some of those are highlighted. . It is a decentralized system and fast way to sent money but there is some risk with Bitcoin. There are also some risks on particular servers, protocol and the ledger. Quantifying risk is difficult within the Bitcoin industry. On an average, every 10 minutes, a new block is appended to the block chain through mining. The ever-growing size of the blockchain is considered by some to be a problem due to issues like storage and synchronization.

ACKNOWLEDGMENT

I am very grateful to Prof. Shalabh Agarwal and Dr Asoke Nath of the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India, for their help and guidance in while preparing the write up of this seminar. I am also very grateful to all the professors for helping us to their utmost. The write up of this seminar wouldn't have been possible without their guidance.

REFERENCES

[1] Anton Badev, Matthew Chen "Bitcoin: Technical Background and Data Analysis", In Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C, October 7, 2014, pages-01-15.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" satoshin@gmx.com,www.bitcoin.org, 2008. Pages- 01-08.

[3] Jonathan Levin, University of Oxford, Department of Economics, "Introduction to Bitcoin: Unique features and data availability", jonathan.levin@economics.ox.ac.uk, Nov 21, 2013. Pages- 01-07.

[4] Johann Palychata, Research Analyst at BNP Paribas Securities Services, "Bitcoin and blockchain,What you didn't know but always want to ask". BNP Paribas Securities Services. Pages-02-03.

[5] Antony Lewis, "A Gentle Introduction to Bitcoin", Brave new coin, antony@bitsonblocks.net. Sep21 2015. Pages-04-13.

[6] Jerry Brito, Peter Van Valkenburgh, "Operational risks faced by Bitcoin companies ",Lloyds Emerging risk report-2015. Pages- 06-14.

[7] www.google.co.in/search?q=diagrams+on+bit+coin+technology+growth+around+the+globe,date-11th may,2016,

