International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Bitcoin and its Real Time Applications

Rishika Malli

Student, Department of ISE, BMSIT&M, Bangalore, India

Abstract: ***In this paper the working design of Bitcoin transaction in peer-to-peer network is explained, the security features of Bitcoin including circulation and alteration in the previous Bitcoin transaction is illustrated. Results on the future application of Bitcoin and the possibility of replacement of Bitcoin are discussed. The important factors that determine the future of Bitcoin circulation, price, and scope in future are analyzed which only prove that Bitcoins are here to stay. Applications of Bitcoin include Bitcoins as a transmission of renewable energy such as solar energy, Bitcoin Satellite which enable the latest transaction data processed by the Bitcoin network, and Kryptoradio that facilitates the broadcasting of the transaction data and provide updates using radio waves.***

Keywords: open source, peer-to-peer(P2P), cryptography, blockchain

1. Introduction

In the recent years, a deep relationship has been formed between computer science and banking systems. Some of the financial decisions taken by world powers has proven to be short sighted and has resulted in numerous recessions and financial meltdowns. This is the main reason for cryptography experts and programmers to design a new financial architecture and system, which is the beginning of digital cryptographic currency. Hence, new type of currency that would not be affected by governments' unprecedented decisions, politics and fraud was designed named Bitcoin.

The main differentiation of this new currency is being "virtual", which has empowered Bitcoin such that it is being considered an actual competitor for replacing strong currencies. Another aspect of Bitcoin is the wide range of its effects in the world and the rise in its popularity among the technical world.

Bitcoin provides anonymous, fast and secure transactions. One can transfer any amount from one point in the world to another without including a third party in between them or being forced to pay fees.

This 'open source' 'P2P' electronic-cash system was introduced in the year 2009 by Satoshi Nakamoto. It is completely 'decentralized' which essentially means that there exists no central server or trusted parties and everything is based on crypto proof instead of trusting the other person.

The key features of Bitcoin are:

Open Source: the algorithm to create and transfer Bitcoin is accessible to everyone and it is not a secret.

P2P and decentralized: the Bitcoin network does not have a central control point or trusted entity and is not controlled by an organization. Bitcoin is based upon a peer to peer network, which allows it's users to transfer money without involving a third party and in a non-reversible fashion. This protects the anonymity of each party and also foregoes any tax obligations or transfer fees.

Cryptography: Bitcoin transactions use cryptographic key pairs and hashing is used in processing transactions.

The presence of these features enables a large spectrum of applications of Bitcoin, some of which are discussed in further sections.

2. Background

Bitcoin is the first implementation of a concept named "crypto-currency", which was first described in 1998 on the cypherpunks mailing list, which essentially suggested the idea of a new form of money. Money that uses cryptography to control its creation and transactions, rather than a central authority.

The first Bitcoin specification and concept proof was published in 2009 in a cryptography mailing list by a person named Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about his own identity. The community has then grown exponentially with many developers currently working on Bitcoin.

The Bitcoin protocol and software are published openly and any developer or a person with interest around the world can review the code or even create their own customised version of the Bitcoin software.

The changes made by Satoshi have been adopted by others and therefore he doesn't control Bitcoin. The identity of Bitcoin's inventor is as relevant as the identity of the person who invented the paper and published the same.

3. Design

The Bitcoin technology primarily refers to two things: universal database and miners. One is a universal database that grows linearly in blocks and records transactions, forming a chain called as "blockchain." Second is a network of peers who are called as miners, these are the users that add the blocks to the blockchain which essentially helps in growing the blockchain.

If you own bitcoins, that means there is a record on the blockchain that contains a numerical value (coins) and one half of a digital signature. A digital signature is sort of a

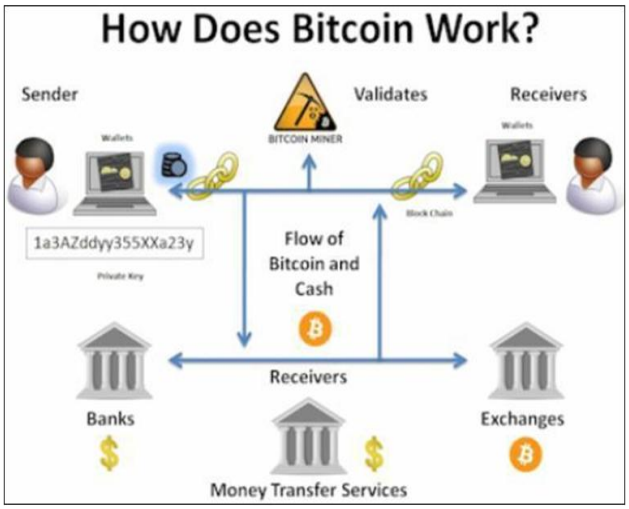
cryptographic puzzle that only you can solve, because only you hold the corresponding half. This is referred to as your "private key," and that is what is in your Bitcoin wallet.

When you want to spend your Bitcoins, you need to make a request for the addition of a new record to the blockchain. The new record refers to the Bitcoins you want to spend that is- it points to the previous transaction in which you received those coins which only proves that you own them, because your other half-signature solves the cryptographic puzzle. Additional it adds a new digital signature to the Bitcoins, which can be completed only by the Bitcoins' next new owner. When that owner wants to spend these bitcoins, he repeats the same process.

Hence the blockchain is just a long chain of transactions. Each of these transaction refers to an earlier record or a transaction in the chain. But Bitcoin users do not directly make the updates to the blockchain. To transfer coins to someone else (another person), the sender has to create a request and broadcast it over the Bitcoin P2P network. After which it is in the hands of miners. The miners grab the requests and do an additional few checks to ensure that the signature is correct and that there are enough number of Bitcoins to make the transaction valid. Further, they bundle or group the new records into a block and add it to the end of the blockchain as shown in the figure.

All miners hence work independently upon their own versions of blockchain. When the miners finish a new block, all they do is to broadcast it to the rest of their peers, who check it, accept, and add it to the end of the chain, and start up their work from this very new starting point.

Each time a block gets solved, a virgin transaction is created with few new minted Bitcoin that are signed over to the first miner who completed the work



4. Application

4.1 Solar Coin

The SolarCoin Foundation launched a digital asset known as the 'SolarCoin'. The SolarCoin uses a blockchain called ElectriCChain. The ElectriCChain collects the non-confidential data related to the solar owners. The goal of ElectriCChain is to essentially grow a network of seven million plus solar installations worldwide. The SolarCoin working can be demonstrated as if one has a solar panel, one will be eligible to download a SolarCoin wallet. Then he/she receives a SolarCoin for each megawatt-hour of power his solar installation produces. The foundation holds 99.4 percent of all the coins that exists/will exist while the rest will be mined by the public and now being provided to anyone who can prove they have added solar electricity to the grid.

4.2 Bitcoin Satellite

Without the peer-to-peer payment network, Bitcoin does not operate today. A denial-of-service attack which is coordinated and distributive in nature, on all peer-to-peer nodes would halt all payments or transactions across the network, and this is the disadvantage or a threat that needs to be addresses leading to the invention of Bitcoin Satellite.

The Bitcoin would survive if means to distribute Bitcoin data exists such as satellite or flash drive through the postal service.

Satellite distribution of public block-chain data facilitates resilience, enabling use in geographic areas where Internet connectivity is unavailable or inconsistent.

It additionally provides a facility of track able donation address and purchases and real time feed are broadcasted to the audience.
A well oriented network of grounded stations is significant to account for multiple orbits. These stations are responsible for transmitting the data precisely the block-chain transaction updates to the satellite.

4.3 Kryptoradio

The project called Kryptoradio is the result of a partnership between Koodilehto, a Finnish co-op specializing in open technology development, and another group who is responsible for development of an alternative digital currency called FIMKrypto. They also encourage the public upon adoption of the same. United they have acquired the rights to transmit the transaction updates to the Bitcoin blockchain across digital terrestrial television in Europe precisely Finland.

Apart from broadcasting transaction data from the Bitcoin blockchain, Kryptoradio also provides updates from the Bitcoin currency exchanges. The service additionally also transmits updates to the blockchain of the FIMKrypto currency.

Turning the drawback into an advantage and Application:
Receiving blockchain information, that is one way transmission through radio waves. The radio waves is useful for services like parking meters, cash registries, and vending machines which all work on one way transaction principle.

Example: A parking meter needs to know only if the payment has been done. It does not require us to send back anything. When the payment has been processed by any

means, the parking meter receives a Bitcoin transaction which is targeted to itself and end with providing the user with a ticket for the parking.

5. Conclusion

Bitcoin is essentially an digital coin. Bitcoin was created in 2009 and is operated by a decentralized authority, since the system works without a central control point or single administrator and it is based upon peer-to-peer network.

Bitcoin network depends upon the blockchain system – a shared public ledger. All transactions that are confirmed are included into the blockchain. All transactions between users begin to be confirmed through a process which is called as mining of Bitcoins.

Mining is a distributed agreement that confirms the waiting transactions by adding them in the blockchain. To get confirmations, the transactions must be packed in a block that obeys the cryptographic rules. The cryptographic rules will be verified by the network of peers called miners and their main role of miners is to prevent previous blocks from being changed or modified and building up of the block-chain.

Hence, hacking into a Bitcoin system, altering a previous Bitcoin transaction is a challenging task, next to impossible, which makes it secure, reliable and popular.

Bitcoin mechanism can be implemented in a wide range of applications such as SolarCoin, Bitcoin Satellite, Bitcoin vending machine, or Kryptoradio.

Developers in this space may predict regarding how the future of Bitcoin looks like and where the next generation of Bitcoin applications will emerge, but there's one thing all can agree upon: The future will not be centralized.

References

[1] Sahar Mirzayi, Mohammad Mehrzad, "Bitcoin, An SWOT Analysis", 7th International Conference on Computer and Knowledge Engineering (ICCKE 2017), IEEE, 2017.
[2] Satoshi Nakamoto, "Bitcoin, A Peer-to-Peer Electronic Cash System", www.bitcoin.org, 2008. (Original document)
[3] Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin", IEEE, 2013.