International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Peer To Peer Electronic Cash Transaction System

Chetan Panchal[1], Omprakash Mandge[2]

[1]Student, Dept. of Institute of Computer Science, MET College, Maharashtra, India
[2]Assistant Professor, Dept. of Institute of Computer Science, MET College, Maharashtra, India

---

Abstract: *There are many P2P electronic cash transaction systems exist; Bitcoin in vary short span of time has been able to attract millions of users. Bitcoin is not sole entity and is depend on community of Bitcoin users to perform the transaction. The peer to peer network is close to purely decentralized since anybody can run a Bitcoin code and there's fairly low barrier to entry. Bitcoin, the primary and hottest cryptocurrency, is paving the way as a disruptive technology to long standing and unchanged financial payment systems that are in situ for several decades. Bitcoin may be a highly sophisticated decentralized trust network which will support myriad financial processes. The interaction between many nodes is what results in the emergence of the subtle behavior, not any inherent complexity or trust in any single node. In this paper we carry out the study of Bitcoin in which we would also understand the working of a P2P electronic cash transaction system and also have a deep insight into the Legal & Security issues related to the use of Bitcoin*

1. INTRODUCTION

Bitcoin may be a collection of concepts and technologies that form the idea of a digital money ecosystem. Units of cash called bitcoin are utilized to store and transmit esteem among members within the bitcoin network. Bitcoin is a network of consensus that allows for a modern financial system and complete digital currency. It is the primary decentralized peer-to - peer payment network with no central authority or intermediaries powered by its users. From a user perspective, Bitcoin is just about like cash for the web.

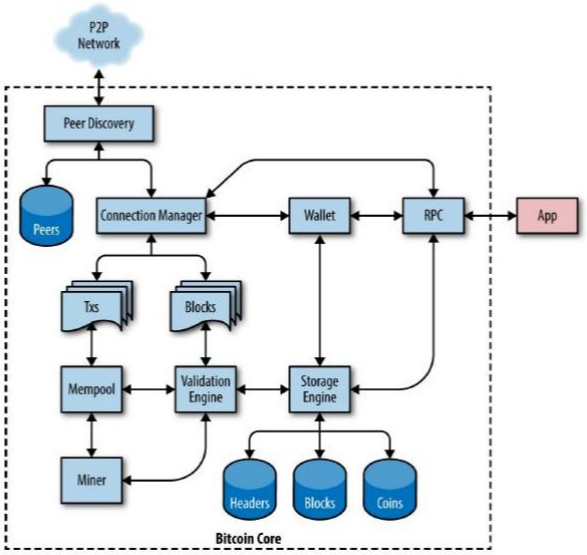

Fig-1: Bitcoin Core Architecture(Source: Eric Lombrozo)

2. HOW BITCOIN WORK

From a user point of view, Bitcoin is nothing more than a versatile app or computer program that gives a individual Bitcoin wallet and permits a user to send and get bitcoins with them. Without others knowing, the Bitcoin network is sharing a public ledger called the "Blockchain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of every transaction. Digital signatures a bit like the sending addresses protect the authenticity of each transaction, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. Furthermore, Anyone can use specialized hardware's computing power to process transactions and earn a bitcoin gift for this service, often called "mining".

3. HOW BITCOIN PRICE DETERMINE

Bitcoin, like most other currencies, features a floating rate of exchange. That means that the value of bitcoin visa-vis any other currency fluctuates according to supply and demand in the various markets where it is traded. For example, the "price" of bitcoin in US dollars is calculated in each market supported the foremost recent trade of bitcoin and US dollars. As such, the price tends to fluctuate minutely several times per second. A pricing service will aggregate the

prices from several markets and calculate a volume weighted average representing the broad market exchange rate of a currency pair.

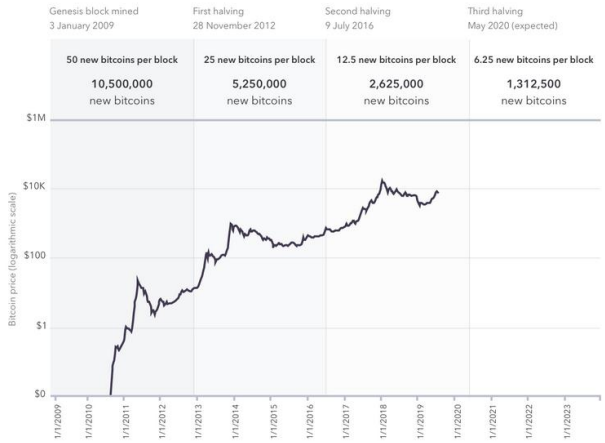

Fig-2: Halving process of Bitcoin

Bitcoin is never traded in one place. Instead, it is traded on multiple exchanges, all of which set their own average prices, based on the trades being made by the exchanges at a given time. If you would like to shop for and sell bitcoin, you've got to settle on a specific exchange which can have its average price. The price of bitcoin fluctuates at any given moment, counting on which exchange the knowledge comes from.

4. GROWING ATTRACTION TOWARDS THE USE OF BITCOIN

4.1 User Anonymity

- The system is meant to publicly record Bitcoin transactions and other relevant data without revealing the identity of the individuals or groups involved.
- Instead, Bitcoin users are identified by public keys, or numerical codes that identify them to other users, and sometimes pseudonymous handles or usernames.
- special computer programs available to all Bitcoin users, called mixing services, privately swap a selected Bitcoin unit for an additional Bitcoin unit of identical value, and thereby obscure the source of the owner's holdings.

4.2 Bitcoin Exchanges

- Bitcoin exchanges allow users to exchange Bitcoin units for fiat currencies, Just like U.S.A. Dollar and euro, at variable exchange rates. Many Bitcoin exchanges also exchange Bitcoin units for other cryptocurrencies, including less popular alternatives which can not be exchanged directly for fiat currency.
- **Most Bitcoin exchanges take a cut, typically but 1%, of every transaction's value.**

4.3 Block Chain

- The block chain may be a public, distributed ledger of all prior Bitcoin transactions, which are stored in groups referred to as blocks. Every node of Bitcoin's software network – the server farms and terminals, travel by individuals or groups referred to as miners, whose efforts to provide new Bitcoin units end within the recording and authentication of Bitcoin transactions, and thus the periodic creation of latest blocks – contains a consistent record of Bitcoin's block chain.
- New Bitcoin transactions are constantly taking place, however finite the Bitcoin block chain grows over time. As long as miners continue their work and record recent transactions, the Bitcoin block chain will always be a bit ongoing .
- A Bitcoin transaction hasn't occurred technically until it's added to the block chain, where it becomes irreversible – unlike traditional payment processors, Bitcoin doesn't have any standardized fee or refund facilities.

4.4 Private Keys

- Every Bitcoin user has a minimum of one private key (basically, a password), which may be a integer between 1 and 78 digits long . Individual users have several anonymous handles, each with their own private key.
- Users either create their own private keys manually, or use a random number generator to do the same thing. Keys can be stored online (either privately cloud storage or on public Bitcoin exchanges), on physical storage media (e.g thumb drives), or on paper, and only entered online during transactions

4.5 Wallets

- Though wallets like Coinbase theoretically protect against the theft of Bitcoin units that aren't currently being used, they're vulnerable to hacking – particularly public wallets used by Bitcoin exchanges, online marketplaces, and specialized websites that exist solely to store Bitcoin wallets known as "wallet services."
- Hackers often target the public wallets that store private keys for users, allowing them to spend the Bitcoin stolen.

- Like keys, copies of wallets can be stored on the cloud, an internal hard drive, or an external storage device. Unlike keys, they can't be stored on paper.As with keys, it's strongly advised that users have a minimum of one wallet backup. Backup of a wallet doesn't duplicate the Bitcoin units stored, just their ownership record and transaction history.

4.6 Miners

- Miners are individuals or cooperative organizations with access to powerful computers, often stored at remote, privately owned "farms." In an attempt to mine new Bitcoin they conduct extremely complex mathematical tasks, which they then hold or sell for fiat currency.
- Miners are "rewarded" these Bitcoin for their effort and often also receive transaction fees paid by buyers.

4.7 Finite Supply

- Bitcoin's own source code places a strict limit on the amount of Bitcoin units which will ever exist: 21 million.
- The last Bitcoin is projected to spring into being sometime around 2140 – that's , if the currency still exists and other people still care enough to mine it. After that, Bitcoin transaction fees will be the sole compensation for the miners.

5. RISK & SECURITY ISSUES THE BITCOIN

5.1 Vulnerable Wallets

- Bitcoin wallets do have a real vulnerability when it comes to hacking attacks and theft. A report by a team of researchers from Edinburgh University said they have found weak spots that can be exploited in hardware wallets. The same research shows that even the heavily encrypted hardware wallets were still vulnerable due to this loophole
- The scientists managed to intercept communication between the wallet and PCs using malware. This lack of security affects Bitcoin users' anonymity, as their funds can be easily transferred to other accounts.

5.2 Hackers and Cyber-Attacks

- Mt. Gox was quite an enormous player within the cryptocurrency world. The exchange managed a whopping 70 per cent of all bitcoin transactions worldwide at its peak in 2013. This dipped a touch to 70% by the start of 2014, but the corporate was still going strong.
- Mt. Gox took a devastating hit within the largest bitcoin hack so far. Hackers accessed and stole 740,000 bitcoin from Mt. Gox customers and 100,000 from the corporate itself, roughly the equivalent of $460 million at the time. At today's value, that would be $7.2 billion.

5.3 Selfish Mining

- Selfish mining is a bitcoin mining strategy in which groups of miners collude in order to increase their revenue. Bitcoin was invented to decentralize production and distribution of money. But selfish mining can lead to Bitcoin mining operations being centralized.

5.4 Double Spending

- This allows an attacker to make more than one transaction successfully using a single coin which invalidates the "honest" transaction.

6. LEGAL ISSUES WITH BITCOIN

6.1 Fraud and Money Laundering

- the cryptocurrency starts in a legitimate wallet on the clearnet. It is transferred to a wallet within the dark web making multiple hops before landing during a second dark web wallet.
- It's at this point that the currency is clean enough to bring back up to the clearnet and traded on a legitimate cryptocurrency exchange or sold for fiat.

6.2 Business Registrations and Licensing

- A growing number of businesses are taking advantage of digital currencies as a form of payment. As in other financial areas, businesses may be required to register and obtain licensure for particular jurisdictions and activities. Owing to the complex and evolving legal status of digital currencies, this area is significantly less clear for businesses operating in the crypto market.
- Companies which only accept cryptocurrencies, for example, may not need to register or obtain licenses at all i.e. As far as cryptocurrency scams go, OneCoin is perhaps the one that rules all of them. US prosecutors alleged that the Ponzi scheme raked in around $4 billion, defrauding investors around the globe.

7. CONCLUSIONS

- Unless a user voluntarily publishes his Bitcoin transactions, his purchases are never related to his identity, very similar to cash-only purchases, and can't easily be traced back to him.

- This isn't to mention that bitcoin transactions are truly anonymous or entirely untraceable, but they're much less readily linked to non-public identity than some traditional sorts of payment
- The bitcoin payment system is only peer-to-peer, meaning that users are ready to send and receive payments to or from anyone on the network round the world without requiring approval from any external source or authority.
- This means no account maintenance or minimum balance fees, no overdraft charges and no returned deposit fees, among many others.
- Since bitcoin transactions haven't any intermediary institutions or government involvement, the prices of transacting are kept very low.
- This can be a major advantage for travelers. In addition, any transfer in bitcoins occurs very quickly, eliminating the inconvenience of typical requirements for authorization and waiting periods.
- Because users are ready to send and receive bitcoins with only a smartphone or computer, bitcoin is theoretically available to populations of users without access to traditional banking systems, credit cards and other methods of payment.
- In 2013, Bitcoin's market value exceeded $10 billion for the first time. That year, the first Bitcoin-dispensing "ATM" (more accurately, an automated currency exchange machine) appeared in Vancouver, British Columbia, and their number exploded in the subsequent years.
- In 2013, Bitcoin's market value exceeded $10 billion for the first time. That year, the first Bitcoin-dispensing "ATM" (more accurately, an automated currency exchange machine) appeared in Vancouver, British Columbia, and their number exploded in the subsequent years. If the digital assets aren't exempted from GST, the digital currency exchanges in India are getting to have a standoff with the tax authority
- When it comes to your bitcoin trading strategy, you should exercise caution. Bitcoin is a particularly high-risk asset, and even the foremost experienced traders can lose money during a highly unpredictable, volatile market. This is not a reliable method for boosting your pension's earnings potential.
- The price of Bitcoin is very volatile, partly due to the liquidity (the ability to quickly buy and sell) of the currency. The amount of bitcoins flowing through the market at any point in time gives investors the ability to enter and exit positions quickly.
- While the amount of merchants who accept cryptocurrencies has steadily increased, they're still considerably within the minority. For cryptocurrencies to become more widely used, they need to first gain widespread acceptance among consumers. However, their relative complexity compared to standard currencies will likely deter most of the people , apart from the technologically adept.
- A cryptocurrency that aspires to become a part of the mainstream economic system may need to satisfy widely divergent criteria. it might got to be mathematically but easy for consumers to know

REFERENCES

[1] Mastering Bitcoin Book by Andreas M. Antonopoulos
[2] Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
[3] Bitcoin and Beyond Book by Malcolm Campbell – Verd
[4] https://www.bitdegree.org/tutorials/how-does-bitcoin-work/
[5] https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work
[6] https://www.moneycrashers.com/bitcoin-history-how-it-works-pros-cons/
[7] https://www.tripwire.com/state-of-security/security-awareness/security-concerns-risks-related-bitcoin/
[8] https://www.lbmc.com/blog/security-concerns-bitcoin-cryptocurrencies
[9] https://www.elliptic.co/our-thinking/bitcoin-money-laundering
[10] https://www.investopedia.com/tech/what-are-legal-risks-cryptocurrency-investors
[11] https://www.investopedia.com/articles/forex/091013/future-cryptocurrency.asp
[12] https://www.buybitcoinworldwide.com/mt-gox-hack