Bitcoin – A New Currency in the Era of Investment

Pranjal Kumbhare[1]

[1]*Student, MBA.Tech in Information Technology, NMIMS Shirpur, Maharashtra, India*

Abstract - *over the last decade, research on Bitcoin and other cryptocurrencies has increased exponentially across several disciplines: economics, law, finance, engineering fields, accounting, and others. As the uses of blockchain technology are expanding, more and more disciplines are getting attracted to it. This paper provides an assessment of the current scenario of the issue.*

The bitcoin protocol can inculcate the global financial transaction volume in all electronic payment systems, without any custodial third-party holding funds. It only requires participants to have a computer and a broadband connection. A redistributed system is planned within which group actions turn up over a network of micropayment channels (payment channels or transaction channels) that transfer the worth via blockchain. If Bitcoin transactions can get signed with a new sighash (signature hash) type that addresses malleability then these transfers may occur by contracts between untrusted parties through a series of decrementing time locks.

Key Words: **bitcoin, ledger, blockchain, transaction, mining.**

1. INTRODUCTION

Bitcoin currency is a decentralized payment system that is based on maintaining a public transaction ledger in distributed manner unlike the traditional method. It is maintained by unknown participants known as miners, who execute a protocol. The distributed data structure called blockchain is maintained and extended. Work proof is an important aspect for which the miners are responsible to provide the solution of.

2. CURRENT SCENARIO OF PAYMENT METHODS

2.1 Cash

Cash is represented through some physical object, generally note or we can say even a coin. When a specific note or a coin is lent to someone, the value which the coin or a note holds gets automatically transferred to him/her, regardless the involvement of any given third party as depicted in Fig 1. given below. Any kind of credit relationship is not at all needed in such case. That's why the parties can remain unknown easily. Nowadays the physical cash that is used daily has its own advantage. Any one that possesses the physical object is the owner of it. Furthermore, no matter who, any individual can participate easily in the traditional cash payment system. No permission is needed to access it. The disadvantage of cash system is that both the money lender and buyer of a product and money receiver or a seller of a product have to be present physically while the transaction is being done at the same place in order to make trade possible, which is not really possible in some cases.

2.2 Digital Cash

An ideal payment method can transfer the value of money electronically with the help of cash data files as shown in Fig 2. given below. When these cash data files are brought to use, they generate a disadvantage of their own, even though they prove advantageous in the same manner as of a physical cash, but can get circulated freely on electronic networks. Such data file can be sent to anyone via social networking websites. These can be further shared easily at negligible cost. Such situation is undesirable for monetary transactions since they cannot serve for carrying out ideal transactions. This creates the problem of "double spending problem".

2.3 Electronic Payment

For preventing the problem of double spending, classical electronic payment systems rely on a central authority that checks whether payments are correct are not. In such systems, the bank generally manages the accounts and transactions related to all those buyers and even the sellers. Buyer has to make an associate order and then submit it, which then gets verified and in this way the payment is initiated.

Figure 1
Cash Transaction

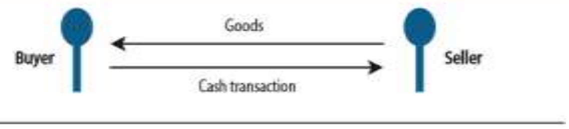
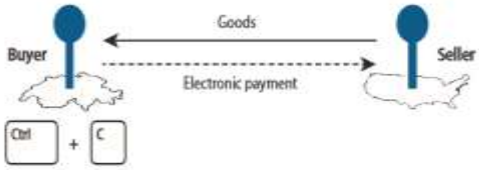


Figure 2
Electronic Payment



3. ADVANTAGE OF MICROPAYMENT CHANNELS

3.1 A Network of Micropayment Channels can solve Scalability

If there is a transaction taking place between two parties, it is not generally known to other external parties. But in a bitcoin network, other parties are also able to view the transactions. By letting this happen, settling the final relationship at a later stage enables Bitcoin users to conduct several transactions without bloating up the blockchain. Nowadays, during a transaction two parties where one of them is the payee, the other has to trust the third party which creates a counter party risk and incurs transactions costs. But in the bitcoin network, they don't have to create trust in a centralized party who is involved in those transactions. This helps to establish a trustless structure with the help of time locks.

Billions of transactions can be carried out per day with the help of strong computational power of modern computers. Huge amounts of funds can be transferred between parties in decentralized bitcoin network. The balance gets updated automatically after the transaction.

3.2 Micropayment Channels do not require trust

Without proper cryptographic signatures, the blockchain does not know what amount of money is owned by whom. If Alice claims to have transferred 100 dollars to Bob and Bob claims that Alice only transferred 50 dollars then finding out the legitimate transaction or the right amount of money transferred can be difficult. The network needs to know which set of balances is correct. This problem is solved in blockchain by the use of blockchain ledger as a times-tamping system.

Both parties can sign a transaction like a 2X2 multi-signature address where they agree on the current balance state. Now, whenever a transaction is carried out between them, the balance will get updated. There will be two different states – the current correct balance, and any old deprecated balances. There is just a single correct current balance, and many old balances which are deprecated. So, in bitcoin network a bitcoin script is devised after which all old transactions are invalidated, and only the new transaction is valid. This helps to identify the legitimacy of a transaction and false claim problems can be prevented from occurring.

4. HOW BITCOIN WORKS VIA BLOCKCHAIN

Bitcoin is not a real coin or a real currency. It does not belong to any specific region or a country. It is just a virtual representation unit of measurement. There is no as such physical illustration through which a bitcoin gets depicted. A Bitcoin unit can be hugely divisible and it can get divided into millions of Satoshis which is the littlest part or a fraction of a given Bitcoin. The Blockchain of a Bitcoin is actually a record that usually carries the past records of all Bitcoin transactions, as well as the new creation of latest Bitcoin BTC units. This is usually observed as the ledger of the Bitcoin system. The Bitcoin Blockchain process is quite interesting. It is made up of sequences of blocks. Each and every block that is present has the potential to build on its previous block. The new information regarding the new Bitcoin transaction(s) is also contained in this. The common time between any two Bitcoin blocks is ten minutes. Anybody can transfer and browse the Bitcoin Blockchain that is in use. That is basically a ledger: public record. The word "ledger" has to be addressed carefully here. No single instance exists of the bitcoin's blockchain. Rather each participant has freedom to manage her/his ledger's copy.

It is usually done through opening the user's account at any given and verified Bitcoin Exchanges. Fiat currency is then transferred into it. The account user has to convert the money to buy Bitcoin units on the exchange.

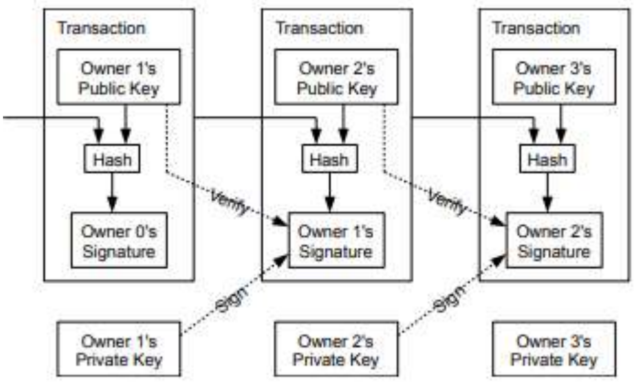
The account user will then use the funds to shop for Bitcoin unit or one in all the numerous different cryptoassets that are available on the bitcoin exchange. Because of such large availability and wide usage of Bitcoin, the valuation on these big exchanges is incredibly viable with comparatively tiny bid spreads.

5. TRANSACTIONS OF BITCOIN

Electronic coin is defined by chain of several digital signatures. The coin is signed digitally by an owner via the hash of preceding transaction and public key of next user and is transferred further to after adding this to coin. The payee can always verify his ownership by checking the signatures.

The major problem in this process is that payee can't verify where the coin is being double spent or not. This is generally solved by introducing a mint. A mint is a trusted authority who checks all transactions. He finds out if they are being double-spent. The coin returns to mint after any transaction and a new coin is issued. This new issued coin is trusted as not being double-spent. This indeed generates a new problem. As whole of it depends on company having the mint so this becomes same as the interference from bank. Somehow payee has to get ensured that any previous owners didn't sign any of the earlier transactions. We care about the earliest transaction done in the process so even if there are later attempts of double-spending it shouldn't matter. If we know all the transactions in the process we will come to know if there's any transaction missing.

Mint know all the transactions and knows which happened first and which happened later. If we want to do this without the help of a trusted party, we must publicly announce the transactions. A system is needed for users to agree the sequence in which the transactions took place. Payee can be proved which transaction took place earlier on the basis of agreement from most of the nodes on which was received first.



6. MONETARY POLICY OF THE BLOCKCHAIN

Every payment method requires rules that define the way in which new financial units get created. The original Bitcoin network is organized in a way that on an average, any block candidate with a legal hash value which is originated after every 10 minutes. The victor of the bitcoin mining competition gets a predefined value of Bitcoin. Overtime reward for the miners is halved approximately after 4 years but get progressively rewarded through the transaction fees. A lot of Bitcoin users tend to believe that the Bitcoin's limited availability can lead to deflation. They think its value will keep on increasing. However, this doesn't happen. Bitcoins don't have any fundamental worth. Their worth is set alone by expectations concerning its future value. A buyer buys a Bitcoin unit assuming that the unit will reap some profit. The worth of Bitcoin is very dynamic.

7. TRANSACTION CAPABILITY

The resolution of transactions to get initiated and carried out in absence of central authority overlooking them. During any normal transaction, a shopper submits the payment via the online banking service provided by the bank. The bank provides an infrastructure and different suppliers providing central services make sure that the transaction gets successfully executed. Within the Bitcoin network system, a monetary payment order is often overcommunicated to a range within the network node. The nodes in the network are loosely network and the sent message is forwarded till it reaches all the nodes. This decentralized system has several benefits making system extraordinarily sturdy.

8. UNIQUE CHARACTERISTICS OF A BITCOIN

Bitcoin cryptocurrency is unique in its own ways. The major one is that financial organizations like bank do not interfere which is also the best advantage. The blockchain technology is so advanced in the functionality of its nodes that other traditional third party even house or bank or other authority is not required. The property that these transactions can be carried out at any place at any time is what makes the whole process flexible even from the business point of view. The users participating can be unknown and no private data is exposed.

Another great thing making bitcoin unique absence of any kind of central authority or issuer. The process through which Bitcoins get generated is called mining. This way the growth rate of the bitcoin can be predicted. This prediction of the growth rate of the bitcoin is its another quality. Absence of authority and predictable growth rate is what makes bitcoin interesting as any form of government of any country cannot influence bitcoin currency. Thus, the depreciation or appreciation or revaluation or devaluation is not under any possible set of hands. This eliminates uncertainty due to which the currency can't become the target of any assumption which generally is the case of the traditional currency nowadays.

Since cryptography is used, trust is not really required from any of the financial institutions. This is the fourth trait. The transaction gets verified multiple times. The node is the one verifying them. This is a very trusted network so anyone else doesn't interfere. Bitcoin is not the cause of its own inflation. The currency's limited supply is apparently an advantage that helps to fight inflation. The total amount of bitcoins present in the world are already known and thus it makes their supply predictable and fixed.

9. ATTACKS ON A BITCOIN

9.1 Double spending attack

This attack is the major problem when it comes to using bitcoin while performing any kind of transaction by the user in the bitcoin blockchain network. This means a cyber-criminal can spend bitcoins twice by participating in a transaction to buy any commodity. He can misuse the transaction and make it public by adding it to public blockchain and exposing it. The public blockchain is the longest blockchain chain. After this he can remove the same and build upon a new long chain if his computer has that kind of computing power. If any merchant witnesses the specific transaction on public blockchain he trades with the attacker through assets in order to gain some bitcoins from him. If attacker suddenly decides to remove that specific transaction from public blockchain merchant loses his BTC and attacker can spend it again somewhere. Actually, the attacker by doing this process many times can spend those Bitcoins several times.

9.2 Sabotage attack

One seemingly obvious response to the logic in the previous section is that the majority attack would be "noticed" by Bitcoin users, perhaps after a period of initial confusion. As a result, the argument goes, while the attack would indeed work in the sense of obtaining the hoped-for goods or assets, there is an additional cost to consider in that the attack will harm the subsequent value of the attacker's own Bitcoin holdings — which the attacker must have to engage in the attack in the first place.

10. RISKS OF A BITCOIN

Bitcoin is mainly risky in two ways. The volatility of the price of bitcoin is what makes it risky in the first place. Thus, volatility needs to be considered seriously while thinking to invest in the bitcoin. Tversky and Kahneman discuss and give an insight into the concept they designed - that the losses are always weighed more than the gains. This is called the concept of loss aversion. Although all of this hardly matters if we consider a neutral risk perspective. Investors keep the fact in mind that any asset which is largely volatile will have less utility.

Second risk that bitcoin possesses is being vulnerable to the attack by hackers. Cyber criminals can attack in such a way to either steal a bitcoin from the network or destabilize the entire system. Due to this volatility increases exponentially. A study conducted states that 18 out of 40 bitcoin exchanges were shut down because of cyber-attack. 2014 witnessed the shutdown of the largest bitcoin exchange due to cyber-attack. The digital platform is always susceptible to getting hacked or attacked and so this threat will be ongoing.

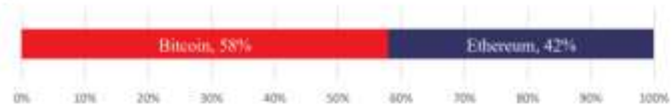
Apart from this, a couple of issues keep hindering the way in which bitcoin works. The fact that bitcoin works digitally is the first issue. Any given currency has three functions: the medium through which it is exchanged, the account through which it is operated and the value in which it is stored. The exchange medium is the prime function. First two functionalities possess problems itself. In its real form bitcoin is actually a theoretical investment as it is bought with the currency instead of being a currency. The transactions carried out to buy products through Bitcoins is low. The low-key users fall into great short-term risk in comparison to other currencies because of bitcoin's high volatility. A lot of sources keep on confirming bitcoin is an investment type than a currency type. 1/3rd users have just invested in bitcoin rather than using it as a currency for buying products. Although Bitcoin functions well when used as just a store of value.

The popularity of bitcoin amongst gamblers is the second issue. Illegal activities like terrorism, evasion of tax and buying goods like weapons or drugs through bitcoin is very common. The two main agencies - Europol and FBI are already dealing and fighting to reduce this scenario of internet crime.

11. BTC VS ETH QUANTITATIVE ANALYSIS

A quantitative analysis was prepared on the basis of several assumptions regarding the price of two cryptocurrencies – bitcoin and Ethereum. Monte Carlo simulation model was used and series of single time simulations were performed. In all after running around 100 simulations the data was obtained regarding predicted returns of both of them in 5-year period. The following results were observed and Bitcoin overrun Ethereum 58 times in simulation.

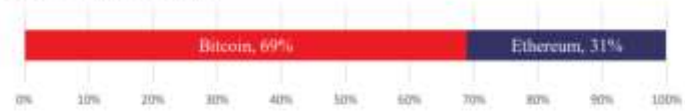
Figure 3. Monte Carlo Win Rate



12. BITCOIN – A BETTER INVESTMENT

The analysis performed above has shown bitcoin to be a better investment than Ethereum as it has performed better compared to Ethereum. Final portfolio allocation was also prepared to help investors take better decisions considering the risky situations discussed prior in the paper. This way the portfolio generated a healthy return. Finally coming to the decision making while investing, it is wise to invest 69% of money in the bitcoin and remaining 31% into the Ethereum to reap maximum benefits over 5-year period.

Figure 4. Final Portfolio Allocation



13. CONCLUSIONS

The Bitcoin creators' goal was to develop a decentralized cash-like electronic payment system. During this process, they encountered the elemental challenge about how to establish and transfer digital property rights of a unit of measurement while not being controlled by a central authority. They created the Bitcoin Blockchain to tackle it. This unique advancement in technology helps countries to store the money and to transfer it. No central authority is required in the process.

The blockchain technology provides an infrastructure allowing various applications to perform like using colored coins, smart contracts. It can also be used in fingerprint scanner to protect the integrity of data files and to keep them confidential in a blockchain network, which will transform the world of finance and other sectors.

REFERENCES

[1] W. Dai, &quot;b-money,&quot; http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, &quot; Design of a secure timestamping service with minimal trust requirements, &quot; In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, &quot; How to time-stamp a digital document, &quot; In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, &quot; Improving the efficiency and reliability of digital time-stamping, &quot; In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, &quot; Secure names for bit-strings, & quot; In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, &quot;Hashcash - a denial of service counter-measure,&quot; http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, &quot; Protocols for public key cryptosystems, &quot; In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] https://bitcoin.org/bitcoin.pdf

[9] https://fc16.ifca.ai/preproceedings/36_Vasek.pdf

[10] W. Feller, &quot; An introduction to probability theory and its applications, &quot; 1957.

[11] https://www.economist.com/sites/default/files/the_future_of_cryptocurrency.pdf

[12] https://theses.ubn.ru.nl/bitstream/handle/123456789/4434/MTHEC_RU_Sjoerd_Klabbers_s4384458.pdf?sequence=1

[13] https://faculty.chicagobooth.edu/eric.budish/research/Economic-Limits-Bitcoin-Blockchain.pdf