Minning of Bitcoin Technology
Ishita Tiwari, Alisha Goyal, Ankita Joshi

1B.Tech Scholar, Department of CSE/IT, Global Institute Of Technology, Jaipur, India
2,3Assistant Professor, Department of CSE/IT, Global Institute Of Technology, Jaipur, India

Abstract—“Bitcoin Technology” Bitcoin is an innovative technology that offers several benefits, such as fast transaction speeds, low costs, and the elimination of the need for a third-party intermediary to process transactions. Unfortunately, BitCoin has faced resistance from regulators because the technology has been used for nefarious purposes, including online drug purchases and Ponzi schemes.

This note provides a basic explanation of how BitCoin works and is currently regulated on federal and state levels. This note argues that BitCoin should not be forced into old regulatory frameworks that do not adequately balance security concerns with the benefits of BitCoin. BitCoin should not be regulated at the federal level. Instead, state regulations should focus on BitCoin providers that can unilaterally transfer or block transfers of BitCoin on behalf of users. State regulators should require such providers to register with their given states, maintain adequate books and records, implement advanced cyber security standards, conduct audits of their operations, and submit reports to state regulators. In crafting these regulations, regulators should keep in mind that vague or poorly drafted regulations will chill innovation.

A Bitcoin would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

Keywords –Bitcoin Technology, Blockchain, Wallet, Payment Processing, Economy of Bitcoin.

I. INTRODUCTION

Bitcoin emerged out of the 2008 global economic crisis when big banks were caught misusing borrowers’ money, manipulating the system, and charging exorbitant fees. To address such issues, Bitcoin creators wanted to put the owners of bitcoins in-charge of the transactions, eliminate the middleman, cut high interest rates and transaction fees, and make transactions transparent. They created a distributed network system, where people could control their funds in a transparent way.

Bitcoin has grown rapidly and spread far in a relatively short period of time. Across the world, companies from a large jewelry chain in the US, to a private hospital in Poland, accept bitcoin currency. Multi-billion dollar corporations such as Dell, PayPal, Microsoft, Expedia, etc., are dealing in bitcoins. Websites promote bitcoins, magazines are publishing bitcoin news, and forums are discussing cryptocurrencies and trading in bitcoins. Bitcoin has its own Application Programming Interface (API), price index, trading exchanges and exchange rate.

However, there are issues with bitcoins such as hackers breaking into accounts, high volatility of bitcoins, and long transaction delays. Elsewhere, particularly people in third world countries find Bitcoins as a reliable channel for transacting money bypassing pesky intermediaries.[1]

II. HISTORY OF BITCOIN

The first Bitcoin protocol and proof of concept was published in a Whitepaper in 2009 by a shadowy individual or group under the pseudonym Satoshi Nakamoto. Eventually Nakamoto, who remained mysterious, left the project in late 2010. Other developers took over and the Bitcoin community has since grown exponentially. While Satoshi Nakamoto's real identity remains shrouded in mystery, it is on record that he communicated extensively in Bitcoin's early days. Let us speculate on questions like when he started working on Bitcoin, to what extent he was inspired by similar ideas and what was the motivation for bitcoin.

III. METHODOLOGY

The project was distributed in different modules and further in various sub tasks. Firstly all the tasks were
collected to be there in the project for achieving the projected plan. Then the tasks were divided according to the different modules. Different modules identified were:

Creation of first Bitcoin: It is believed that Satoshi started coding Bitcoin around May 2007. He is said to have registered the domain bitcoin.org in August 2008. Around that time, he started sending emails to a few individuals he thought might be interested in the idea of bitcoins.[1]

In October 2008, he publicly published a white paper that dwelt on the Bitcoin protocol, and released the Bitcoin code as well. Then he stayed in contact for about two years, during which he interacted actively in forums, communicated with several developers and later he also submitted patches to the initial code. He maintained the source code along with other developers, tackling issues as they happened. By December 2010, as others had slowly taken over, he quietly left the scene.

Entities: The entities involved in the implementation and maintenance of Bitcoins are:

- The Blockchain platform
- Cryptographic algorithms
- Bitcoin miners which are computers or specialized machines that mint the currency and make possible transactions
- People who participate in the transactions and thus help to move the payment system

- Bitcoin Transaction: We shall now see how a new block of bitcoin transaction is created.
- A bitcoin miner creates a block by using the following steps –
  - Gathering pending transactions, preferentially those with transaction fees first, and then the free ones
  - Verifying the transactions for their validity
  - Solving a hashing problem
  - According to the statistics, in October, 2015, blockchain.info site stated that, the average number of transactions per block was 411, and as of May 2018, the current number of pending unconfirmed transactions is around 2495.

- Reward And Cost Per Bitcoin Transaction: Assuming that one bitcoin is worth $400, the reward of 25 bitcoins per block is worth around $10,000, ignoring negligible amount of transaction fees. Taking average number of transactions per second as 2, and the number of transactions per block as 1200, the reward per transaction works out to $8.33. It is found that the cost of electricity consumed in mining is close to the reward which makes mining bitcoins not so profitable. The basic problem of mining as of now, is the 1 MB limit on block size which makes it possible to have at most only 10 transactions per second.

- Bitcoin Handle Double Spending Problem: For digital cash system, a payment network necessarily should have valid accounts, balances and transaction records. The biggest bottleneck common to every payment network is the double spending problem which is the case when same money is used multiple times to do transactions.[1]

To prevent double spending, all transactions have to be recorded and validated every time in a central server where all the balance records are kept. However, in a decentralized network, every node on the network has to do the job of a server; it has to maintain list of transactions and balance records. Thus, it is compulsory for all nodes/entities in the network to keep a consensus about all these records. This was achieved by using the blockchain technology in bitcoins.

So we can say that bitcoins like other cryptocurrencies are mere token entries stored in the decentralized databases that keep consensus of all balance and account records. It is to be noted that cryptography is used extensively to secure the consensus records. Bitcoins and other cryptocurrencies are secured by math and logic more than anything else.

Bitcoins and cryptocurrencies have gained recognition and adoption based on their perceived value by their creators and users.

IV. BLOCKCHAIN TECHNOLOGY

A blockchain is basically a perpetually growing list of records, called blocks. These blocks are linked and secured by using cryptography. Each block generally contains a cryptographic hash of the previous block along with timestamp and transaction data. By its design, a blockchain does not allow modification of the data.

It is an open, distributed ledger that records transactions between different parties efficiently and in a verifiable and permanent way. A blockchain, as shown in figure below is typically managed by a p2p or peer-to-peer network collectively following a protocol for communication between nodes and for validating new blocks. Once recorded, the data in any given block cannot be altered without consensus of the network majority.

In case of bitcoins, the blockchain is a public ledger that records bitcoin transactions. It is implemented as a chain of blocks. Each block contains a hash of the
previous block up to the genesis block which is the first block of the bitcoin blockchain. This is however achieved without any trusted central authority: the working of the blockchain is performed by a network of communicating nodes running bitcoin software. Transactions of the type payer A sends B bitcoins to payee C are broadcast to this network using existing software applications. Bitcoins are created as a reward for payment processing work in which users who offer their computing power verify and record payments into a public ledger. Called mining, individuals engage in this activity in exchange for transaction fees and newly minted bitcoins. Besides mining, bitcoins can be obtained in exchange for other currencies, products, and services. Users can buy, send, and receive bitcoins electronically for a nominal fee using wallet software on a personal computer, mobile device, or a web application. Bitcoin is the first implementation of a concept called “crypto-currency”, which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto.

**Blockchain Architecture:** For starters, let’s first learn what is blockchain technology. Logically, a blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that is grouped together in a network (peer-to-peer). In other words, blockchain is a combination of computers linked to each other instead of a central server, meaning that the whole network is decentralized. To make it even simpler, the blockchain concept can be compared to work done with Google Docs. You may recall the days of tossing over doc. documents and waiting for other participants to make necessary edits. These days, with the help of Google Docs, it is possible to work on the same document simultaneously. The blockchain technique allows digital information to be distributed, rather than copied. This distributed ledger provides transparency, trust, and data security. Blockchain architecture is being used very broadly in the financial industry. However, these days, this technology is employed not only for cryptocurrencies, but also for record keeping, digital notary, and smart contracts.

- **Work Flow Of Blockchain:**

![How Blockchain Works](image)

*Fig 1: Workflow Of Blockchain*

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.

- **Transaction:** Generally we use coins for transaction but here we had pretended coinbase transactions do not exist. Coinbase transactions can only be created by Bitcoin miners and they’re an exception to many of the rules listed below. The figure above shows the main parts of a Bitcoin transaction. Each transaction has at least one input and one output. Each input spends the satoshis paid to a previous output. Each output then waits as an Unspent Transaction Output (UTXO) until a later input spends it. When your Bitcoin wallet tells you that you have a 10,000 satoshi balance, it really means that you have 10,000 satoshis waiting in one or more UTXOs. Each transaction is prefixed by a four-byte transaction version number which tells Bitcoin peers and miners which set of rules to use to validate it. This lets developers create new rules for future transactions without invalidating previous transactions. These Bitcoin due to transaction broadly came up and by cryptocurrency technology spread over the market. Using the public and private keys help us to ensure the security since the data would be in cipher text format that would easy for anyone is decrypt without any proper key. Public key is broadcasted so it would be easily available while private key is present only to the sender who is sending the data in encrypted format.
Fig 2(a): Transactions
An output has an implied index number based on its location in the transaction—the index of the first output is zero.

V. CONCLUSION

Bitcoins can be helpful to a lot of people. Since they are an international currency, you can use them in any country without having to convert between currencies. The Blockchain is really secure and it lets you make sure your money goes to/comes from the right person. People receiving Bitcoins won't have to pay anything for the transactions, and Bitcoins have a lot of support. All of these will definitely help Bitcoin get more users, and if everyone uses Bitcoin it could replace official currencies. Sure, it has some disadvantages, but some of those are because Bitcoin is a new thing, so as time goes on they will be less of a problem. The others can easily be avoided.

VI. FUTURE SCOPE

A private initiative that has created a virtual currency and a payment system based on cryptography and decentralized management, Bitcoin is considered not only an interesting, but also a disruptive technical innovation by many observers.

- It's true that bitcoin has been far more stable in 2019 than in previous years. In 2017, bitcoin’s price rose from about $1,000 to almost $20,000 before ending the year at about $14,500. In 2018, bitcoin plunged from that level at the beginning of the year to less than $4,000 by year’s end.
- After a rejuvenating 2019, it appears bitcoin is on the rise once more. While its underlying market is virtually inscrutable—billions of dollars shuttle between traders in the black market—there is one fundamental change on the horizon.
- Given Bitcoin's volatility, it is easy to guess that by 2025 it could be worth as much as $150,000 per coin if some of the conservative predictions manage to come to fruition. However, some true believers out there feel that Bitcoin's price could hit $500,000 by 2025!

REFERENCES

[1] https://www.researchgate.net/publication/281773799_Research_and_Challenges_on_Bitcoin_Anonymity
[2] https://blockgeeks.com/guides/what-is-blockchain-technology/
[3] https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin-wallets
[4] https://bitcoinmagazine.com/articles/research-paper-bitcoin-disrupts-international-monetary-policy
https://www.academia.edu/Documents/in/Bitcoin