THEORY AND EVOLUTION OF CRYPTOCURRENCY: BITCOINS – ETHEREUM.

REBEKAH J, PREETHI M, SANDHYA K, NAGANANDHINI K

MASTERS OF BUSINESS ADMINISTRATION – PANIMALAR ENGINEERING COLLEGE, ANNA UNIVERSITY.

Abstract: cryptocurrency is a digital currency which leads the market now-a-days. The knowledge about which led the destination of cryptocurrency and the evolution of cryptocurrency is explained. Bitcoins and ethereum are the most popular cryptocurrencies. They use the block chain technology. Thereby we see the future of the cryptocurrency.

Keywords: cryptocurrency, bitcoins, ethereum, block chain technology, proof of work.

1. An introduction to cryptocurrency:

Cryptocurrency is a virtual currency that is secured by cryptography. It is a method of using encryption and decryption to secure communication in the presence of third parties with ill intent. Cryptography requires a computer algorithm like [sha256] a public key that a user shares with everyone and a private key which is acts as a digital signature for a user.

Computational algorithm

private key

public key

As of 2020, there are approximately 5392 cryptocurrencies available. There are plenty more to come in the upcoming years. Bitcoins were the first blockchain-based cryptocurrency. It remains the most popular and most valuable. The new cryptocurrency crops up every single day. Now cryptocurrency is a bit similar to real-world currency just that it does not have any physical embodiment. Now, some other features of cryptocurrency it has some limits on how many units can exist. In bitcoins this limit exceeds 21 million after this no more bitcoins will produce. You can easily verify the transfer of funds. The hashing algorithm that bitcoin uses makes it very easy for a user to determine whether a transaction is valid or not. It operates independently of a bank or a central authority. It works in a decentralized manner. The new units can be added only after certain conditions are met. For example for bitcoin only after the block has been added to the blockchain build the miner be rewarded for the bitcoin and this is the only way new bitcoins can be generated.

In cryptocurrency international transaction are faster. Many years ago physical tokens have been being used as means of payment (e.g. Gold coin, bank notes etc.)

Physical tokens

2. History of currency

Over 3000 years ago, money make entry in the human history. The bartering system was the first system used in early days. Bartering is the exchange of goods it is a direct trade. The traded product is known as medium of exchange. Around 770bc the chinese are created the small size model of exchange product as the medium of exchange. Later the demo product convert into circular shape (coin).

During 600 bc lydia's king alyaltes introduced the minted as the official currency and these currencies are made-up of silver, gold and electrum. Again the chines are the one who convert the coin into paper currency. It increase the international trade. In 21st century they are two type of currency. They are mobile payment and virtual currency.

Virtual coins are begin with the cryptographic david charm. In 2009 the mystery person named satoshi nakamota created a first cryptocurrency, bitcoin. He created a new way to transaction that feature mainly the decentralization.

2.1 digital currency

Digital currency is the intersection of both money and technology. It is one which is available in digital or electronic form. Nowadays, everything is evolving into digitalization. It is intangible and can only be accessed on devices such as smartphones and computers. It is also known as digital money, electronic money, electronic currency, and cyber cash.

Digital currencies can be utilized to buy goods and services. There are various types of digital currencies, the most important is that the cryptocurrency.

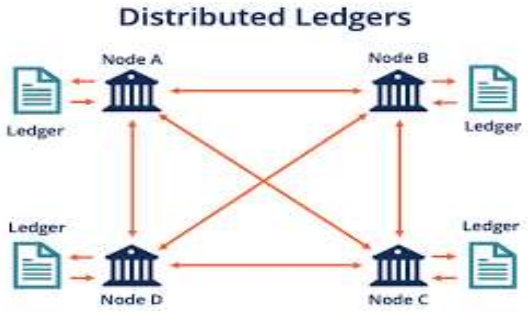
2.1.1 bitcoins

In 2008 under the pseudonym, satoshi nakamoto bitcoin was originated with the white paper. The creators developed the cash-like payment system that permitted electronic transactions and its many advantageous characteristics of physical cash.

Cash transaction

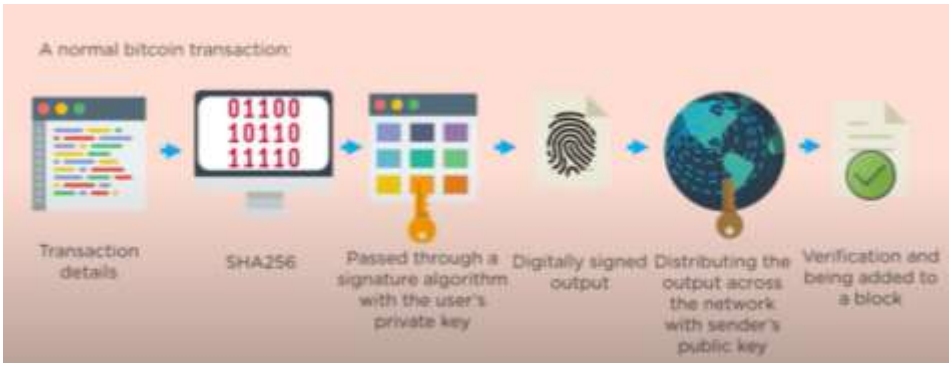
Electronic payment

Payment system with a distributed ledger



Bitcoin is a virtual monetary unit and it has no physical representation. A bitcoin unit can be divided into 100 million. The bitcoin block chain database carries a record of all past bitcoin transactions including the creation of a new bitcoin. It is referred to as the ledger of the bitcoin.

In a normal bitcoin transaction first, we have the transaction details. This details who you want to send it to and how many bitcoins you want to send them then it passes through a hashing algorithm. For bitcoin, we use the sha256 algorithm the output that you obtain is pass through a signature algorithm with the user's private key. This is used to uniquely identify the use of the output and then distributed to cross the network for people to verify. It can be created by using the sender's public key. The people who verify the transaction to check whether it's valid or not as known as miners. Now after this is done the transaction and several others are added to the block chain and it cannot be changed again. Sha256 algorithms are very safe to use. This encryption is very difficult to hack. A bitcoin is a digital currency that is decentralized and works on block chain technology. It uses the peer-to-peer network to perform transactions.. It is very similar to how real life currencies works. Bitcoins transactions are manuel which means you have to personally perform these transactions. For bitcoins it takes 10 minutes to perform the transactions which is the amount of time it takes for a block to be added to the block chain. Block chain is used for money in real life transaction. Now there is a limit to how many bitcoins can exceeds which is 21,000,000 million is supposed to hit this number by the year 2040. Bitcoins is used for transactions involving goods and services. As of january 2021 one bitcoins is equal to 35, 66,516.55 indian rupees.



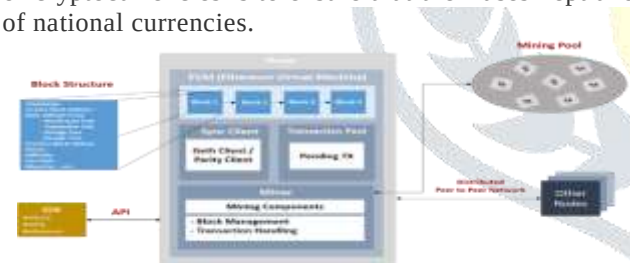
There are two major cryptocurrencies in the market: bitcoin and ether

2.1.2

Ether:

Ether may be a currency that accepted within the ethereum network. The ethereum network uses block chain technology to create an open source platform for building and deploying de- centralised application.

bitcoin and ether both of them use block chain technology that is nothing but a technology that involves transaction being added to a container called block and creating a chain of blocks during which data can't be altered. Currencies is mined using a method called proof of work which is a form of mathematical puzzle that needs to be solved before a block can be added to the block chain finally these are widely used across the world. Ether it can be used as a currency within the ethereum network although it can be used for real life transactions as well. In ether the transactions are manuel, automatic or programmable. This transactions take place when certain to be met. Ether takes about 20 seconds to do a transaction. Ether is used to power the ethereum network and power real life transaction as well. Ether is employed as a fuel within the ethereum network to power both of those things. Ether is expected to be around for a while but not to exceed 100,000,000 units. Ether uses a block chain technology to create a ledger that triggers a transaction when a certain condition is met. Ethereum we use ethash algorithm for hashing. As of january 2021, one ether equal to rupees 1, 12,725.05 indian rupees. The whole world is cleary divided when it comes to cryptocurrencies on one side you have supporters like elon musk, bill gates who says cryptocurrencies are better than regular currencies. On the opposite side we've people completely against it. People like warrant buffet a nobel prize winner in the field of economics. He said cryptocurrencies increases the criminal activities. In future there is going to be a conflict between regulations since several cryptocurrencies are linked with terrorist attack government wants to regulate how cryptocurrencies work. On the other hand the emphasis of cryptocurrencies is to ensure that their uses kept anonymous. By the year 2030 cryptocurrencies would occupy 25% of national currencies.



2.1.3 Difference between bitcion and ethereum

BITCOIN VS ETHEREUM

S.no	Bitcoin(btc)	Ethereum(eth)
1.	Both bitcoin and ethereum are decentralized cryptocurrencies.	
1.	Bitcoin is defined as “digital dollar”.	Ethereum is defined as the coin value known as “ether”.
2.	It leads the first position in the most popular cryptocurrencies.	Following bitcoin, it is second most popular cryptocurrencies.
3.	Bitcoin is operated by the technology known as “block chain”.	Ethereum also uses block chain technology which is also known as “smart contract”.

4.	Bitcoin uses a hashing algorithm which is "sha-256"	"ethash" is a cryptographic algorithm used in ethereum.
5.	10 minutes is taken to add new block in the block chain.	Only 12 to 15 seconds taken to add new block in the block chain.
6.	Only 21 million bitcoins can be mined as the supply of bitcoin	Total supply of ethereum is that of 18 million eth every year.
7.	There can be 219,34 transactions held per day.	There can be 659,051 transactions held per day

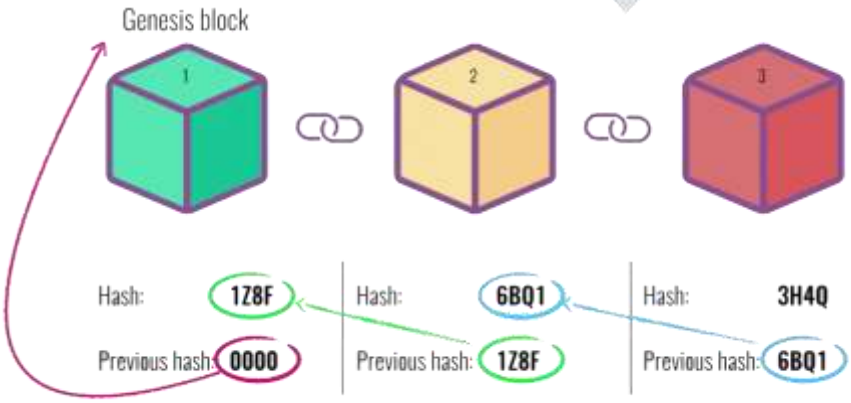
2.14 block chain technology

Likely as the name blockchain, it consists of chain of blocks which contains information. Blockchain technology was discovered in 1991 by a group of researchers for digital timestamps. Lately at 1999, satoshi nakamoto implemented bitcoin using blockchain technology. Blockchain is a distributed ledger which is open and can be used by anyone. Once a data has been recorded in blockchain it becomes very difficult to change it. Recent development of blockchain results in smart contracts which is implemented in ethereum at 2015.

Blockchain works with some algorithms such as cryptography algorithm, decentralized network, consensus mechanism, distributed ledger. There are protocols which keeps the network efficient, secure, real-time (peer-to-peer), reliable and functional. Blockchain protocols acts as the real transformative power for bitcoin.

Creation of a block

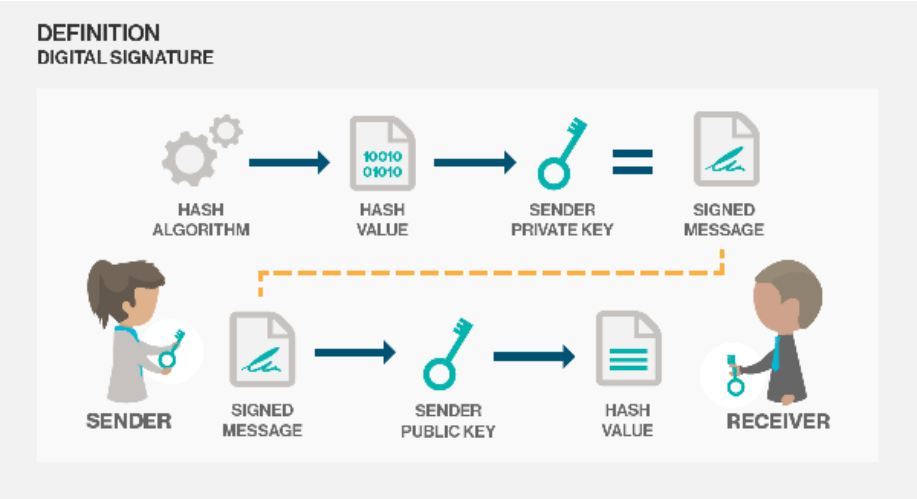
Each block contains some hash, data, and hash of previous block. In the bitcoin blockchain, a block contains the data of sender, receiver and the amount of transaction. Hash is compared like a fingerprint as it is unique. Once a block has been created, its hash has been calculated. Changing any data in a block will also changes the hash and all the following blocks and it is no longer the same block. Hash of the previous block creates the chain of blocks and keeps the blockchain secure. Every block has hash and the previous hash. The first block does not have the previous block since it is the first block and is known as the genesis block.



Transaction using blockchain

When someone initiates the transaction, the transaction is firstly requested to any node in a network. It is then broadcasted across the network and it is picked by various miners who are part of the network. The signer signs for a transaction and miners runs a hash algorithm which generates 32 or 64 bits' hash value and this hash value is encrypted using the signers private key, thereby it is known a digitally signed document.

The digitally signed document is broadcasted into the network, once the verifier receives the document, he decrypts it using the user's public key. The hash value created after decryption is compared with hash value created by the hash algorithm, and if the hash values are equal then the signature is considered to be valid and transaction is made. Miners are issued newly created coins in reward along with transaction fee by the sender. Miners solve these mathematical work which is known as proof of work.



2.15 issue with current banking

The banking is centralized and it is issued and managed by banks and central governments. In the banking sector, the third person is needed to send money from one person to another person. The market price can change due to government influences. The supply is unlimited. It is both digital and physical transactions. The value was generated by markets and regulations. A bank account and government identification and a mobile phone are the requirements for the digital transfer. The money transactions in the bank are typically not processed on bank holidays and weekends.

There are huge problems in banking while transferring money.

1. The high transaction cost.
2. Account hacking.
3. Net frauds
4. Financial crisis

2.16 how bitcoin solves this problem?

it is decentralized and limited supply. It was created by computers. No third person is needed. The transaction was irreversible. The value was generated by people's usage/demand and supply. Only the digital way of exchange is possible. An internet connection and a computer are the minimum requirements to transfer the bitcoins. The bitcoin transaction will take 15 minutes or one hour only. Easily we can send, receive and transfer globally.

2.17 whats the future of cryptocurrency?

The future of cryptocurrency is depending up to two different result. They have both positive and negative side. Looking the positive side of cryptocurrency. They are very stable. Due to the pandemic, we loss the most of the economic level of country. But cryptocurrency (middle of november 2020) is running successfully than the previous year, it give the positive vibes about the cryptocurrency. In this result many big shot company are invested in the cryptocurrency.

Main negative side of cryptocurrency is volatile. It became high in certain period and again go to down in the fraction of second. Another reason is security measure of the cryptocurrency. The threats are increase up to 51%of attack. Cryptocurrency have a mixture of future.

2.18 why cryptocurrency ban in india?

The main reason foe banning cryptocurrency in india is aadhar card. When the government introduced the jan dhan-aadhar mobile trinity. The main purpose of act is linking the bank account to the aadhar card so that indian government can easily eye on the transaction and activity of the people in the country. It also has the drawback of we can easily crack into the account it is highly risk to maintain the cryptocurrency. So, indian government think that banning the cryptocurrency will help to secure country secret and citizen account details.

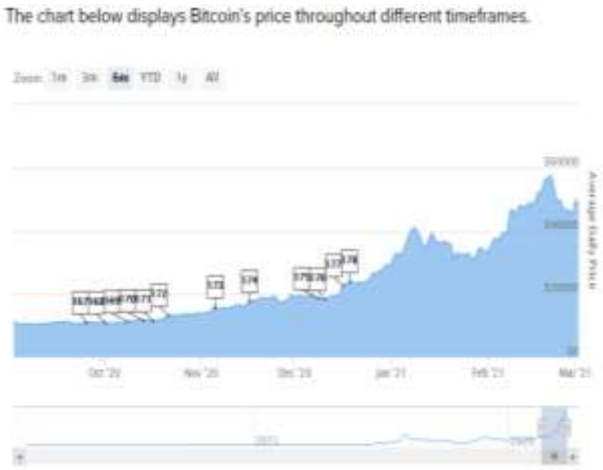
The difference between national digital currency and cryptocurrency. The cryptocurrency has the feature of decentralized and the country currency have feature of centralized.

3. Data collection

Secondary data:

Secondary data is the data that has been previously gathered and readily available from other sources.

Figure no:1



source: https://99bitcoins.com/bitcoin/historical-price/

Bitcoin average daily prices for last one year from october 2020 to march 21, 2020 are shown in figure 1 which is self-explanatory about fluctuations in the price.

4. Conclusion

Even though there are hackers it is impossible to hack blockchain in bitcoin or any cryptocurrencies because the hackers should hack countless devices and collect information. Since everything is being digitalized and also we ensure the cent percent security, cryptocurrencies will lead the future.

5. References

[1] economic times monday, 11 dec. 2017 page no. 3

[2] https://blockonomi.com/mt-gox-hack/ accessed on feb. 27, 2018

[3] https://coinmarketcap.com/all/views/all/ accessed on feb. 27, 2018

[4]nakamoto, s. 2008. Bitcoin: a peer-to-peer electronic cash system. Available: https://bitcoin.org/bitcoin.pdf. Accessed 10 aug 2017.

[5]narayanan, a., bonneau, j., felten, e., miller, a. & goldfeder, s. 2016. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, new jersey:
Princeton university press.

[6]karsai, mrton, hang-hyun jo, and kimmo kaski.“ bursty human dynamics”. Springer international publishing, 2018.

[7]k.-i. Goh and a.-l. Barabasi. “burstiness and memory in complex ´ systems”. Epl (europhys. Lett.), 2008