Cryptocurrency

The idea of 'cryptocurrencies' has been on the discourse since 1998 itself. The first known attempt for creating a digital cryptocurrency was B-Money and Bit Gold, but both never came into reality. Cryptocurrencies are the digital or virtual currencies working on the cryptographic principles. As the name indicates, it doesn't have any physical existence or they are not tangible. They merely exist as a set of programming codes. Yet provides high security and usability than many existing currencies.

Cryptocurrency works on blockchain technology, we have already seen how blockchain works. In the case of cryptocurrency, the ledger keeps the track of cryptocurrency that is generated and transacted across the network. Every individual in a particular blockchain will have a unique account Id/address. The cryptocurrency is always associated with this accounts (Currency is Debited and Credited to this account).

People can manage their account through the application called wallets. Through the wallets, anyone can make the transaction to anyone on the network (both the sender and receiver must have an account). The transactions are verified by nodes and added to the blockchain ledger. So the immutable and encrypted ledger of blockchain is the backbone of cryptocurrency.

Suppose initially, my wallet has credited with 100 units of cryptocurrency. From there onwards every movement of every unit of currency will be recorded in the public ledger, every participating node in the network can watch the past as well as the present of each unit of currency in the system. Thus it will be a more transparent monetary system.

Other notable features of blockchain are also applicable to cryptocurrency; the encryption mechanism, peer to peer network, and no central authority/central server to control. Each cryptocurrency will be working on a blockchain protocol. One of the most famous cryptocurrency is bitcoin which relies on the bitcoin blockchain. And ether is another fast-growing cryptocurrency which runs on Ethereum protocol. While comparing with the traditional currencies, the cryptocurrencies provide highly anonymous nature for participants. The only visible identity of a user will be his account ID, rest everything will be encrypted. The participants will not have any idea about the real identity of a user.

Satoshi Nakamoto An unknown person or a group of people who first proposed and developed the Bitcoin. With nearly 980,000 bitcoins in hand, he is considered to be one of the richest person in the world. After initial involvement and support Nakamoto handed over the control of network and source code to community members and disappeared.

Bitcoin

Bitcoin is the first Cryptocurrency as well as the first blockchain implementation in the world. We have already discussed what cryptocurrency is. In this section, let us explore

little deep into the topic with the most famous cryptocurrency, Bitcoin. The historical aspects of its creator and all have already pinpointed at many places. However, for the sake of continuity let's have a glance. Based on the conceptual framework put forward by some researchers in late 90's Satoshi Nakamoto introduced bitcoin in 2009. It does follow the exact structure of a typical Blockchain with P2P shared network, Distributed ledgers, and cryptographically protected data.

Bitcoin Working

So how someone can use the Bitcoin service? May the people are already familiar with the method. It is simple and we don't need any technical knowledge or programming skills to use Bitcoin. The first thing we have to do is create an Account in Bitcoin blockchain. For that, the simplest way is to create a digital wallet. There is a number of wallet service providers like coinbase and BitCore. While creating an account the user has to provide a 'Key' (similar to a password). Using this key the wallet will generate a valid bitcoin Private key-Public Key pair. The public key will be visible to all and it is the visible account ID of the user. On the other hand, the user keeps the private key by himself, it is the access key to his account. If a person loses his private key he loses access to his account and his money.

Buy Bitcoin

The easiest way to own Bitcoin is to buy them from a bitcoin exchange. There are a number of online bitcoin exchanges which exchange normal currency to bitcoin. People can exchange their normal currency for bitcoin and move it to their wallet. Another method to own bitcoin is to participate in Bitcoin mining.

Transactions

Sending bitcoin from one account to another is called as a transaction. It is usually done through wallets. The wallet app will provide an interface where we can input the account Id of the recipient and the amount we wish to transfer. Once we have made the transaction, the miners will verify the transaction and add to the blockchain ledger if it is a legitimate one. In Bitcoin, the transactions are cost-free. Usually, a transaction validation time is about 10 minutes in bitcoin, but if we give a small transaction fee we can speed up the process.

Bitcoin Mining

The mining is the most important as well as the interesting topic in bitcoin. This is the process by which new transactions are validated and added to the so- called 'blockchain'. This demands dedicated mining hardware and thus, not all nodes are involved in mining. Those nodes who are participating in mining pro- cess is known as 'miners'. When a new bitcoin transaction happens in the network that is broadcasted on the network. The miners listen to this broadcasting and engage in transaction verification. Once the transactions are verified they are added to a block.

So what do miners actually do?

Here, the mission is to find a hash value for the new block. The miner who finds the hash value first is rewarded with some bitcoins called block reward. Now it is 12.5 BTC. The reward is halved every 210,000 blocks or roughly every 4 years. Finding hash value is not a big deal. Every node can do that. Therefore, a difficulty level is associated with it to make the nodes compete with each other. The difficulty level is a measure of how difficult is to find the hash. Difficulty level shrinks the set of hash values that a block can have. Without difficulty level, the hash can have any of the value within the super gigantic set of 2^256 possibilities (since the length of hash = 256 bits). By associating a difficult level, the target set is reduced considerably. The difficulty level is speci- fied in terms of a number of zeroes, which means the miner has to find a hash value which starts with a specified number of zeroes. The nodes keep finding different hash values and checks whether it satisfies the required difficulty level. Since the data of a block remains same, the hash is always same. Therefore, the only possibility to try out different hash values is by associating a nonce with the content of the block. The nonce is an arbitrary string of 32-bit length. i.e. H(block + nonce)

Being a small target set, the probability of finding success is reduced. The miners keep changing the nonce in a brute force manner and the corresponding hash is computed each time. This is the real game and the computational power of nodes really matters here because the miners have to try out large combina- tions of 'Nonce'. The node which equipped with dedicated hardware and high computational power has a greater chance to win this game and get the block reward. Those who find hash first will broadcast the block along with the nonce. By receiving this, others stop mining and validate whether the received hash satisfies the specified difficulty level. If yes, the nodes show their acceptance by adding it to the blockchain.

Value of Bitcoin

The value of bitcoin has drastically increased and touched new heights in the last couple of months. So a general question that may arise in anyone's mind is 'who determines the value (or more economically speaking exchange rate) of bitcoin. As we know there is no central bank or any other designated agency to control it; then how the value is determined, or who determines it? The answer lays in the basic economics, which is demand and supply. Following is the simplest model to determine the value of bitcoin.

T : Total bitcoin transaction/second

D : Duration that a BTC needed by a transaction

S : Supply of the bitcoin

P : Price of the bitcoin

We have

S/D=Bitcoins available per Second

T/P= Bitcoins needed per Second

According to demand-supply rule, when the supply of the bitcoin increases the demand decrease consequently the price will also decrease. And when the demand increases the supply of bitcoin will also decrease, consequently the price of the bitcoin will also increase.

At an equilibrium state, where the supply S over D, is equal to the demand T over P. We can deduce the price P as

S/(D)=T/P

Equilibrium state:-

P=TD/S

That is at equilibrium, the price should be equal to T times D divided by S.

This is the very basic equation to calculate bitcoin exchange rate. The value of the bitcoin basically depends on the demand and supply. However, there are many other factors including public perceptions, mining difficulty level, energy consumption for mining process etc. that are taken into consideration while calculating the actual exchange rate. So that there will be some slight variations in exchange rate across the different market. It is evident that a single authority can't control the value of bitcoin, rather it is determined strictly based on the user transaction.

Community, Politics and Regulations

Along with the enormous possibilities it opened, the Bitcoin (or the cryptocurrencies as a whole) poses potential threats also. The latest discourses on crypto currencies are mostly related to this aspect, especially that from government authorities and financial institutions. The cryptocurrencies can bring a lot of benefits to existing economic systems as well as the society. But an unfettered and anonymous economic regime also raises many other questions like security, illicit usage, black money etc. The discussion is still going on and both sides are upholding their own version. Here are some of the advantages as well as disadvantages of the cryptocurrencies.

Advantages

Transaction Speed

Cryptocurrencies offer very fast transaction which is far more superior than the Present banking transaction speed. Bitcoin takes a maximum of 10 minutes for validating a transaction and it is about 10 seconds in Ethereum.

Anonymity

Cryptocurrency transactions are fully anonymous and it is not possible to identify who had done this transaction or to whom this transaction is made. The participants will be using only the network address of the sender and receiver. No identity of those participants will be published in the shared ledger.

No restriction on payments

It is the most noticeable advantage of cryptocurrency. There is no restriction on transactions. The user can send the currency at anytime from anywhere to everywhere. That means no time boundaries like bank holidays.

Less /No transaction fees

The cryptocurrency transactions are normally free. Or the fee is much less than present financial transaction charges. In bitcoin, anybody can do transactions without paying any transaction fees. The user also has the option to offer trans- action fees for speeding up their transaction. That is if a person is providing a transaction fee, more miners will come to validate the transaction; hence the transaction gets validated fast.

Immutable transactions

Cryptocurrencies are one of the most secure currency systems available today. It has the 'immutable' property; i.e. If one transaction had occurred in the blockchain based cryptocurrency, it is irreversible. So the chances of fraudulent transactions are nearly impossible.

Secure Payment information

Cryptocurrency transactions don't use any identity of the users. They will only use the wallet address of the sender and receiver, all other information is securely hashed and no one can retrieve it back. When someone sends a cryptocurrency to another person/entity, none of the personal information will be shared with them. Only the particular amount of bitcoin will be transferred from one account to another account.

No Inflation

Most of the cryptocurrencies have a fixed number of currencies in their exchequer. In case of bitcoin, it is 21 million. Once the entire thing has mined there won't be any more new bitcoins. So there is no chance for inflation.

Disadvantages

Less Acceptance

Even though the demand for 'cryptocurrency' is steadily increasing, the point is that many governments have not given any official approval for 'cryptocurrency' transaction. And its usage is now limited some specific domains only. Moreover, the 'cryptocurrencies' are still far away from the common mass.

Inconsistent rate

It can consider either as an advantage or disadvantage. Although there is a strict demand supply rule to define the exchange rate of cryptocurrencies, present market trends indicate an uncommon surge in the exchange rate of cryptocurrencies, especially that of Bitcoin. But it is believed soon that it will attain the normal pace.

Government Ban

As we said government can't control cryptocurrencies, but they can ban it and illegalize its transaction. Of course, it cast a shadow over such ambitious, unfettered movements.

Deflation can happen

Cryptocurrencies are generally limited in number and its exchange rate is basically depended upon the supply and demand. Since most of the cryptocurrencies have only a fixed number of currencies, the possibilities of deflation are greater than any other economic system. In case of bitcoin, if someone holds the bitcoin for a long time, then the supply will reduce and still the demand will increase and it will create deflation.

Key recovery is impossible

Since most of the cryptocurrencies don't have a central authority, every individual is responsible for keeping their account safe. If anyone loses the wallet key, no one can help them get it back.