Cryptocurrency

In the first section, the blockchain and its structure have been discussed. Before we going to explain one of the famous blockchain (or Blockchain protocol) the Bitcoin, it would be better having a look into the terms 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. There are many advantages as well as disadvantages for cryptocurrency which will be discussed in the next chapter.

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 process 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 specified 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 combinations 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 transaction 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.

Government can’t De-monetize

Most of the cryptocurrencies work as a decentralized system and its exchange rate is fixed dynamically according to the demand-supply factors. No government regulation or anything can’t stop such independent cryptocurrencies. The only thing that a government can do is restrict the conversion of it to normal currency. However, they can’t stop the transactions in cryptocurrencies.

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.

Supports Money Laundering/Black Market

The anonymity of the cryptocurrency makes it attractive to the black market and money launderers. Since the identity is not revealed anywhere misuses are reported several times. Famous two are the “silk road” website which provides illegal drugs and other illegal items payable by bitcoin and recent ‘Wannacry’ cyber-attack.

The discussion is still going on and most of the governments have not yet formulated any direct legal frameworks regarding this. Of course, the potentials of cryptocurrency can be used to develop a more transparent economic system, but the loopholes and security threats have to be taken care of before taking such big leaps. A potential technology like this can’t be avoided forever, so we can expect a fully legalized cryptocurrency based economic system soon.

Ethereum

Ethereum is an Open Source Blockchain platform which allows anyone to develop and deploy Blockchain based Applications. **Any kind of application including cryptocurrency, tokens, wallets, social apps etc. can be developed and deployed in a Distributed Environment of Ethereum.** In other words, rather than sticking with the cryptocurrency alone, Ethereum opened the possibilities of the 'blockchain' and 'distributed ledger' technology to other application domains. Ethereum is not a single network rather it is more like a protocol for internode communication. Actually, in Ethereum many networks exist alongside. The community Ethereum Network, Community test network and other private Blockchain networks like

- Private network
- Public test network
- Main Ethereum network

> “
>
> ## Ethereum
>
> The inventor Vitalik Buterin has done what Tim Berners-Lee had done to the networks. World Wide Web(WWW) brought the individual networks under a single umbrella. Similarly, Ethereum incorporated all blockchain functionalities in a single network and avoided creation of individual blockchains for each purpose.
>
> ”

How to be the part of Ethereum?

Basically, there is two type of users in a typical Ethereum blockchain. The one who issues a DApp (or a smart contract) and others who participates in the contract.

Every user will have an account in Ethereum, they are called Externally Owned

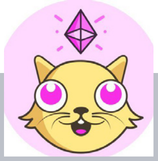
Accounts (EOA). Same way every DApp will have an account address in Ethereum known as Contract Accounts. User transaction is associated with these unique accounts. Users can make transactions with both other EOA accounts as well as Contract Accounts.

DApp

DApp is the 'Decentralized Applications' running on the blockchain. They are the applications that run on blockchain without any centralized control. We can say bitcoin is a decentralized application that runs on Bitcoin blockchain. But it is the Ethereum blockchain that extended the scope of decentralized application and popularized the word DApp.

DApp uses the shared ledger instead of a server to record and store all the transactions. The DApps will have a set of backend codes as well as a user interface. In Ethereum, these backend codes will contain the smart contract and the front end will provide a user interface for the user to interact with the blockchain. Once the smart contracts are deployed on the blockchain, then the DApp will become accessible in the blockchain. Then any node in the blockchain network can use the DApp.

The DApps can be developed for any business use cases. Any application that is currently running on the client-server model can be implemented as a DApp. Some examples of Ethereum DApp:- Green Ether Project, splitcoin, The immortals



CryptoKitties

CryptoKitties is the first game in Ethereum blockchain. A participant can buy and sell crypto kittie token from the issuer. The transaction will be done in Ether. The game had witnessed an unprecedented demand from buyers and Ethereum network was flooded with the transactions.

Components of Ethereum

Smart contracts

Smart contracts are the nerves of Ethereum blockchain framework. All the operations in Ethereum are controlled with smart contracts. Smart contract is the digital version of contracts; which is executed automatically upon satisfying predefined conditions. Of course, they are lines of codes and it is used to exchange anything of value in a more secure and transparent way.In Ethereum, these smart contracts are written in solidity programming language. The smart contract will provide the direct contract execution between sender and receiver without a middleman.

Working of a Smart Contract.

- First, a contract account is created in Ethereum blockchain. The contract will have specific rules and actions based on that rules.

- The contract is then coded. In Ethereum, the smart contract is coded in Solidity; an Ethereum compatible high-level language.

- The coded contract is deployed in Ethereum network. The deployed contract will have a unique public-key address, the address is used to reach the contract in the network. Once the contract is deployed in, it can't be modified even by the Issuer.

Ether

Every collectively run network need some fuel to exist. Bitcoin is the fuels of bitcoin network and Ether is the fuel of Ethereum. Ether is the cryptocurrency of Ethereum network, and it is the backbone of transactions in Ethereum. Ethereum website put it in this way “Ether is a form of payment made by the clients of the platform to the machines executing the requested operations". Similar to the blockchain, the Ethereum network exists in a consistent state because of the computational and other resources spent by individual nodes, Ether is the reward provided to those individual nodes. As more people getting interested in Ethereum, the value of Ether is also surging on daily basis. Today, Ether is the most demanded cryptocurrency after Bitcoin.

The initial supply and rate of issuance of Ether was determined during the presale took place in 2014. Other than the initial supply (which is about 72 million) new ether coins are issued whenever new blocks are created. But this issuance method will possibly change when 'Ethereum' adopts new consensus algorithm.

Ethereum Clients

Ethereum Clients are the tools used to connect to the Ethereum blockchain for developmental or mining purposes. Some of the Ethereum clients are listed below.

- Geth — Geth is an Ethereum client working in GO language. Geth has a command line interface (CLI) tool that communicates with the Ethereum Network and acts as the link between the different nodes in the network.

- Eth — C++ Eth is a powerful Ethereum client which is more focused on miners.

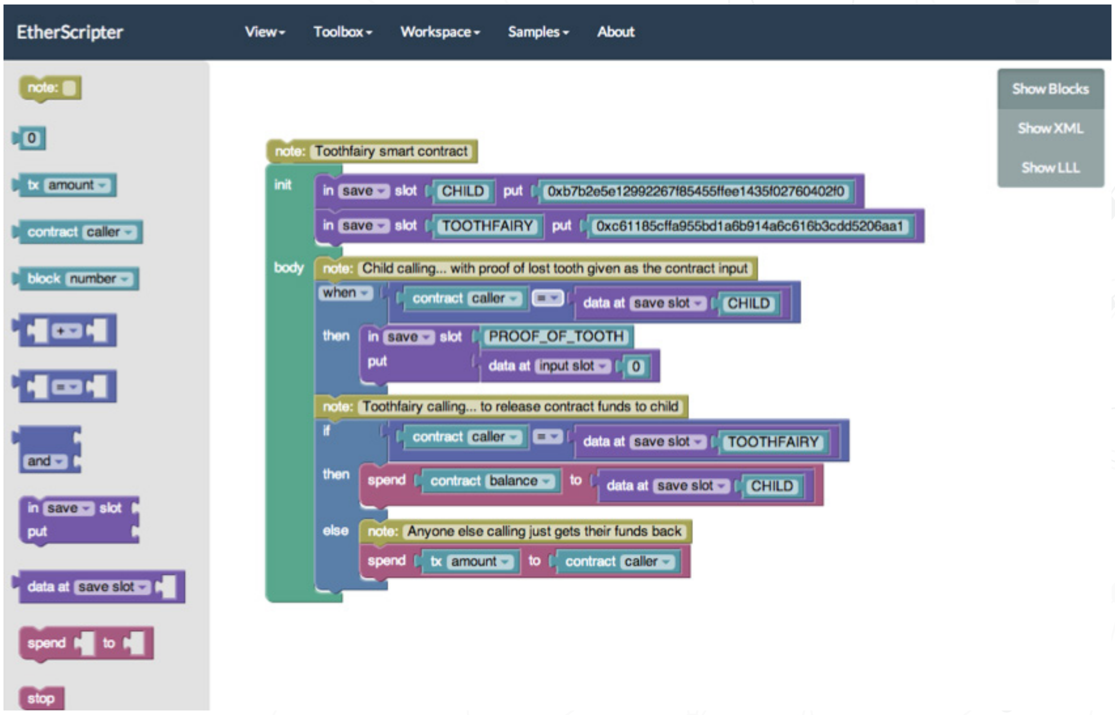
- Pyethapp — this client is useful for DApp development using python. 'Pythapp' is also an excellent choice for research and academic purpose in Ethereum blockchain.

EVM

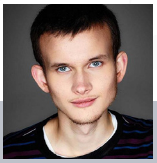
The EVM is the engine behind the whole Ethereum blockchain. Smart contracts are run on the Ethereum Virtual Machine (EVM) - the decentralized, consensus-driven computer which distinguishes Ethereum from earlier Blockchains. This Virtual Machine runs its own language of bytecode. For this reason, several languages for writing contracts have been developed. Of these, the most popular one is Solidity. Solidity is a JavaScript-like language developed specifically for writing Ethereum Smart Contracts. The Solidity compiler 'sol-c' turns this code into Ethereum Virtual Machine bytecode, which can then be sent to the Ethereum network, as a transaction to be given its own address. Every participating node will have an EVM installed in it.

Etherscripter

Etherscripter is a visual smart contract builder tool in Ethereum. It provides a GUI for creating smart contracts in simple steps. Etherscripter provides a simple drag and drop interface where the corresponding backend codes in Serpent, LLL, and XML will be generated automatically. Using Etherscripter even a non-programmer can create smart contracts.



```
note: Toothfairy smart contract
init
    in save slot CHILD put 0xb7b2e5e12992267f85455ffee1435f02760402f0
    in save slot TOOTHFAIRY put 0xc61185cffa955bd1a6b914a6c616b3cdd5206aa1
body
    note: Child calling... with proof of lost tooth given as the contract input
    when contract caller = data at save slot CHILD
    then in save slot PROOF_OF_TOOTH
         put data at input slot 0
    note: Toothfairy calling... to release contract funds to child
    if contract caller = data at save slot TOOTHFAIRY
    then spend contract balance to data at save slot CHILD
    else note: Anyone else calling just gets their funds back
         spend tx amount to contract caller
```



“

Vitalik Buterin

Vitalik is the creator of Ethereum. He first discovered blockchain and cryptocurrency technologies through Bitcoin in 2011, and was immediately excited by the technology and its potential. He co-founded Bitcoin Magazine in September 2011, after intensive researches about blockchain he wrote the Ethereum white paper in November 2013. He now leads Ethereum's research team, working on future versions of the Ethereum protocol.

.

”