classmate
Date 2/7/21
Page

UNIT:- IV

Cryptocurrency:-

* History:- (Bitcoin)

The idea of cryptocurrency is not new. Over the 10 years before crypto-currencies the concept had been introduced by Computer Engineer Wei Dai. In 1998 he published a paper where he discussed "B-money". He discussed the idea of a digital, ~~pseudonyms~~. Currency which could be sent along a group of Untraceable digital pseudonyms.

The same year, another attempt by the name of Bit Gold was drafted by blockchain pioneer Nick Szabo. Bit Gold ~~was drafted~~ equally looked into creating a decentralized digital currency. Szabo's idea was spurred by inefficiences within the traditional financial System.

The Both Coins were never officially launched, they were part of inspiration Behind Bitcoin.

In 2008 Satoshi Nakamoto published the White paper called "Bitcoin: A peer to peer Electronic cash system" describing the functionality of Bitcoin blockchain network.
Later, Satoshi Nakamoto, whose true identity remains a mystery, mined the first block of Bitcoin network effectively piloting the Blockchain technology. The first mined block is known as Genesis Block.

Start of Cryptocurrency Market:-
After the birth of Bitcoin as first Cryptocurrency, solutions had to be found in order to trade them.
In March 2020, the first Cryptocurrency Exchange appeared in the name of bitcoinmarket.com (now defunct)

From 2011 to 2013, Bitcoin managed to reach parity with US dollar in february. By May 2013 the Cryptocurrency market counted 10 digital assets including Litecoin. Another major Crypto asset joined in august in the name XRP(Ripple).

→ Ethereum & ERC-20 Tokens

On July 30th 2015, The Ethereum network was launched. Currently the second crypto asset in terms of market capitalization, it brought smart contracts to cryptocurrency world. These allow Ethereum blockchain to run an entire ecosystem on its blockchain while also hosting its own native currency. Ether (ETH).

The smallest unit of Ether is known as Wei.

1 Wei = 0.000 000 000 000 000 001 ETH

The cryptocurrencies which don't have their own dedicated blockchain, but use the blockchain of another crypto asset are known as tokens. The ones that are on Ethereum network are called ERC-20 tokens. The first ever ERC token launched back in 2015 known as Augur. There are currently more than 200,000 ERC tokens, which means that there is a huge cryptocurrency ecosystem running on single blockchain.

classmate
Date
Page

* Distributed ledger :-

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institution or geographies accessible by multiple people. It allows transaction to have public "witness". The participant at each node of the network can access the recording shared across that network and can own an identical copy of it.

A distributed ledger stands in contrast to a centralized ledger. A centralized ledger is more prone to cyber attacks and fraud. Blockchain is a type of Distributed ledger used by bitcoin.

A distributed ledger can be described as a ledger of any transaction or contracts maintained in decentralized form across different locations and people, eliminating central authority.

All the information on the ledger is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures.

Once the information is stored, it becomes an Immutable database.

Advantages :-

Centralized ledgers are prone to cyber-attacks distributed ledger are inherently harder to attack because of all the distributed copies need to be attacked simultaneously for an attack to be successful.
All records are resistant to malicious change.
Distributed ledger allows for Extensive transparency.

Distributed ledger also reduce Operational Inefficiencies, Speed up the amount of time a transaction takes to complete, are automated and therefore function 24/7. Reduces overall cost.

It also provides an easy flow of Information which makes an audit trial easy to follow for accountants. This removes the fraud occuring and reduce the use of paper.

classmate
Date
Page

Use of Distributed ledger:-

Distributed ledger technology has great potential to revolutionize the way governments, Institutions etc work. It can help governments in tax collection, issuance of passports, recording land registries, licenses, voting proceduces etc.

The technology is making waves in several Industries including.

1. Finance
2. Music & Entertainment
3. Artwork
4. Supply chain
5. Diamond & precious assets.

While the distributed ledger technology has multiple advantages, it's in a nascent stage and is still being Explored in how to adapt it in best possible way.

classmate
Date
Page

* Ethereum :-

The Ethereum blockchain is a powerful distributed global infrastructure that enables to complete various projects using smart contracts.

It is decentralized, open-source blockchain. Ether is the native cryptocurrency of this platform After Bitcoin it is second-largest cryptocurrency by market capitalization. It has its own programming language called Solidity.

Ethereum was created to enable developers to build & publish smart contracts and distributed applications (dapps) that can be used without risk of fraud or third-party interference.

It describes itself as world programmable blockchain

1. Create your own cryptocurrency.
   Ethereum allows you to create a stable token that you can use as a new currency or virtual share.

These tokens use Standard Coin API, means they are compatible with any wallet on Ethereum blockchain

2. Raise funds.
You can use smart contracts for fundraising on ethereum blockchain. You can create smart contracts that specifies a goal and a deadline so if you fail to achieve goal, all donations will automatically returns to donor without any commissions and disputes.

3. Build virtual organizations.
You can write the smart contract that create a blockchain based organization. You can add people to your organization and set voting rules. Members will be able to vote, If required no. of votes are reached then your smart contract will execute automatically.

4. Develop decentralized applications.
Ethereum allows you to build fault-tolerant & secure decentralized applications.

Ethereum Blockchain Block Structure

A block is a data structure that contains two main sections.

1) A header (contains data that describes the block)
2) A body.

Transactions are added to the body and submitted to blockchain network. Miners takes the block and tories to solve mathematical puzzle.

In Ethereum, the mining process uses the submitted block header and arbitary number called a nonce (number used once). The miner picks a value nonce and calculates the hash if result doesn't match with pattern the miner picks another nonce to calculate hash this process continues until the miner find a nonce that results in a hash that matches the pattern.

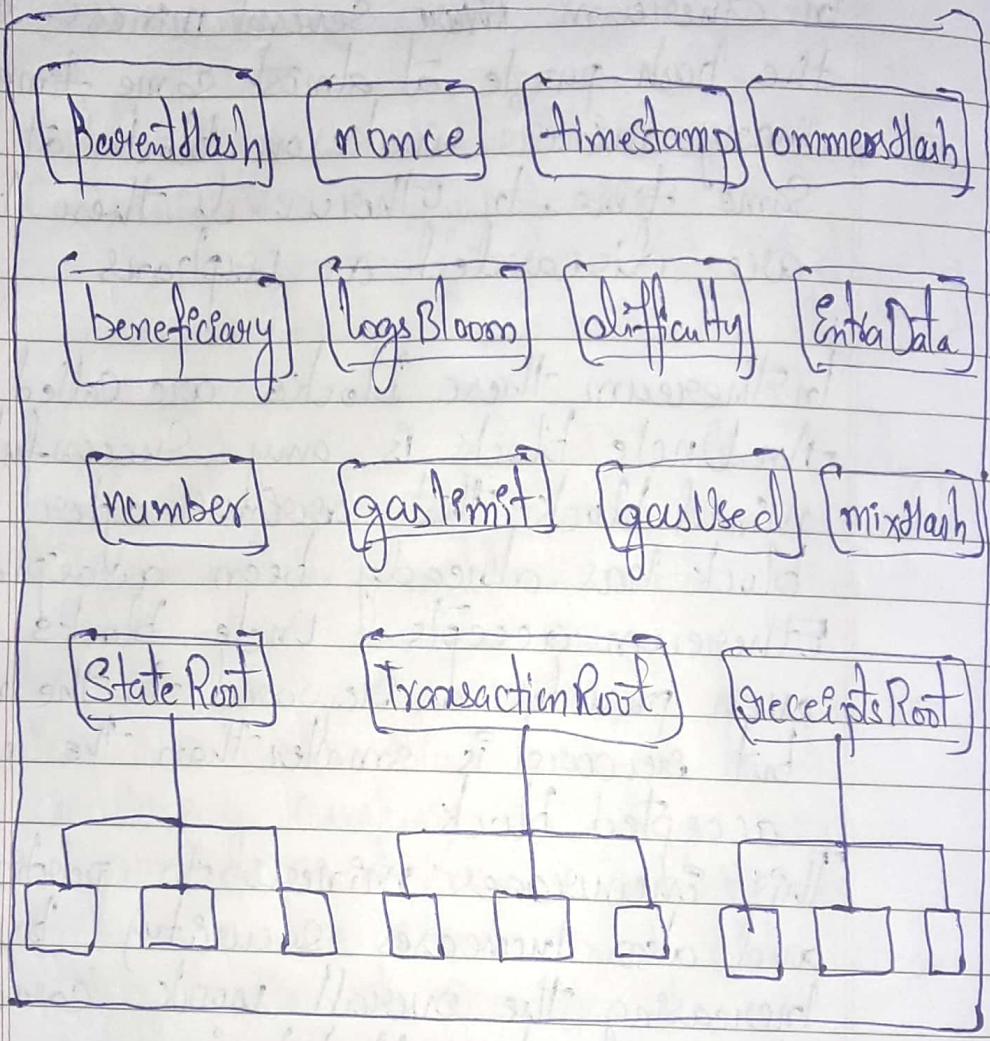
The miner that finds a solution broadcast that solution to the rest of the network and collects the rewards (in Eth)

In Ethereum there several miners solve the hash puzzle at almost same time as many miners work on block at the same time. In other words then blocks are discarded as orphans.

In Ethereum these blocks are called Uncles. An Uncle block is any Successfully mined block that arrives after the block has already been accepted. Ethereum accepts Uncle blocks and even provides a reward to the miners, but reward is smaller than the one accepted block.
This encourages miners to participate and also increases security by increasing the overall work carried out on entire blockchain.

Block header:
It contains data that describes the block.

Block Header



ParentHash:- Hash value of previous block. Ethereum uses Keccak-256 algorithm

Nonce:- A number selected that causes the hash value of current block's header to adhere to specific pattern

Time Stamp :- Data & Time of block created

Uncle Hash :- The hash value of current block's list of Uncle blocks.

Beneficiary :- The miner's account that receives the reward for mining the block.

LogsBloom :- Logging information stored in a Bloom filter (a data structure that quickly finds if some element is a member of a set)

Difficulty :- The difficulty level used in mining the block.

Extra Data :- Extra data used to describes the block.

Block number :- The Unique number for block.

Gas limit :- The limit of gas for the block.

Gas Used :- The amount of gas used by transactions in the block.

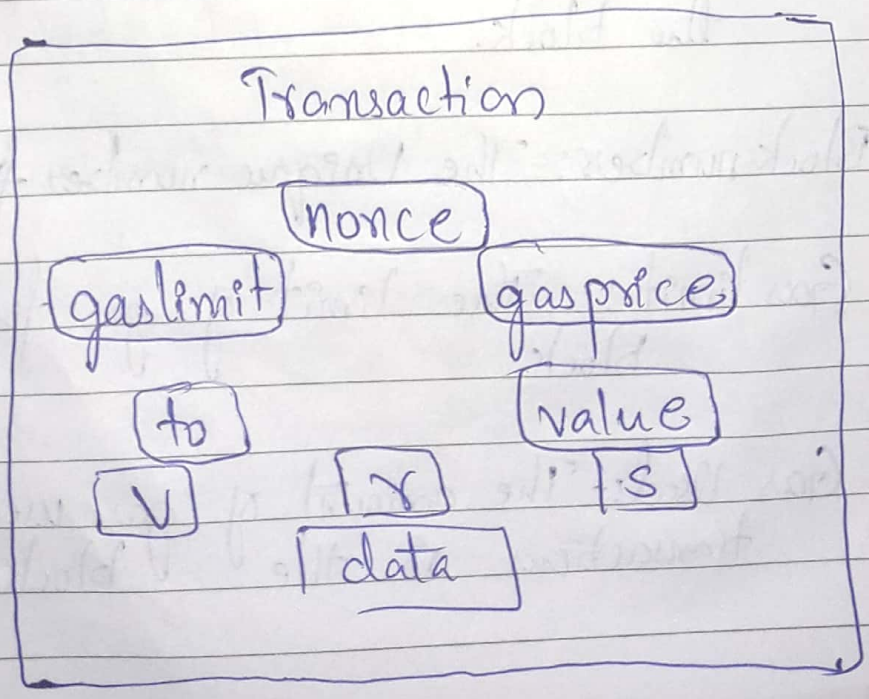
MixHash:- A hash value that is combined with nonce value that the mined nonce meets difficulty requirements.

State root:- The hash value of root node of the block's state trie

Transaction root:- The hash value of root node of the trie that stores all transactions of the block

Receipt root:- The hash of the root node of the trie that stores all transaction receipts for block.

Transactions



Nonce :- Each Ethereum account keeps track of number of transactions it executes.

Signature :- The digital signature of account power, proving the identity of the account requesting this transaction.

Gas price :- Unit price that the amount is willing to pay to execute this transaction.

Gas limit :- Maximum total amount you are willing to pay to execute this transaction.

To :- The address that is receipient of this transaction.

Value :- Total amount of Ether you want to send to receipients

Data :- The actual data submitted as transaction body.

Ethereum Gas:-

Gas refers to fee or pricing value, required to Succesfully Conduct a transaction to Execute a Contract on Ethereum Blockchain Platform. Priced in Small fraction of Cryptocurrency ether.

The Gas is used to allocate resource of Ethereum Virtual machine (EVM) so that dapps (decentralized application) such as Smart Contract can self-Execute in a secured fashion.

The Exact price of a gas is determined by network's miner, who can decline to process a transaction if gas price doesnot meet their threshold.

Gas limit refers to maximum amount of gas that you are willing to spend on a particular transaction. A higher gas limit means that you must do more work to Execute a transaction using ether or Smart Contract. If gas limit is low, miners choose to ignore transactions.

classmate
Date
Page

Ethereum's Consensus :-

Ethereum provides integrity in the way it implements immutability and smart Contracts.
Ethereum uses Consensus protocol called Proof of Work (POW), which sets the rules for validating and adding new blocks. Pow makes add blocks to the blockchain difficult, but profitable. Ethereum defines ether as its Cryptocurrency.

The Ethereum pow mechanism requires that nodes find a number that, when Combined with block's header data, produces a Cryptographic hash value that matches the current target. Finding a hash values that matches the target is hard.
The Node that finds the right value gets a small ether payment for the effort. This process is called mining, and the node that wins the prize is block's miner.

Mining is also a way to make money using Blockchain technology.

Mining has become competitive and most of today's miner invest in high performance hardware with multiple GPU to carry out complex operations.

To keep mining process fair, Ethereum uses a complexity value that makes the mining process even harder as miner gets faster. Adjusting the complexity allows Ethereum to regulate the new block frequency to an average of one new block every 12 seconds.

* DAO :-

DAO :- Decentralized autonomous organization.

ICO :- Initial coin offering.

Blockchain technology has given rise to classes of organizations & opportunities.

DAO is an organization that Operates only on the rules set forth in smart Contracts.

In reality, most DAO's require some human interactions, but the majority of the functionality is automated.

A DAO would be like a driverless car. The car waits for passenger and drives to pickup location when someone needs a ride. The autonomous car Completes the trip and passenger pays with Cryptocurrency. The car just earned some money.
The autonomous vehicle is same idea as a DAO

A DAO Conducts business and engages in transaction without requiring human interaction. Today's DAO's are relatively simple, but it is expected that they will grow in Complexity & eventually replace some existing new human based businesses.

Like all businesses, Ethereum-based business need funding to operate. There are ~~for~~ many funding methods. Ethereum opens new option for funding business.

Businesses that use ethereum often create their own tokens also called coins, that represent value associated with business ventures. Business sells these tokens to raise funds to launch business.

These ICOs essentially exchange one type of currency for a digital item of value. Tokens may represent an expected future values as ownership in a new venture or current value that entities the holder to some benefit. Either way tokens are similar in some ways to stock shares

- An ICO is a popular method to fund a new blockchain based business.

classmate
Date
Page

* Smart Contracts:-

A Smart Contract is a Self-Executing Contract with the term of agreement between buyer and seller being directly written into lines of code. The code and the agreements contained there in exists across a distributed decentralized blockchain network.
The code controls the execution and transactions are trackable and irreversible.

Smart Contract permits trusted transaction and agreement to be carried out without central authority.

Smart Contract are how things get done in Ethereum Ecosystem.
When someone wants to get a particular task done in Ethereum they initiate a Smart Contract with one or more people.

Smart Contracts are series of instruction written using programming language called solidity which works on the basis of IFTTT, If-This-than-that.

How does a blockchain-based marketplace work?

Say hello to Alice, a homeowner.

She needs to get the lawn in front of her house mowed.

Alice wants to get this done for the lowest price possible, so she uses a blockchain marketplace.

Alice describes the task and specifies the amount of cryptocurrency she's ready to pay.

Say hi to Bob, a handyman.

He is eager to earn money by doing odd jobs. He agrees to mow Alice's yard.

The blockchain marketplace automatically creates a smart contract for Alice's mowing job.

If Alice confirms that Bob has mowed her lawn, the smart contract will automatically transfer money to Bob.

If she doesn't confirm that Bob has mowed her yard, the smart contract will automatically send money back to Alice.

A smart contract brings the following benefits to Alice and Bob:

Consider an Example of vending machine

Step 1:- You give vending machine some money.
Step 2:- You punch the button corresponding to item u want.
Step 3:- The item comes out you collect it.

In this no third party was involved.

How would this transactions happens on ethereum network

Step 1:- You give some money and this gets recorded by all the nodes in Ethereum network and transaction get updated in the network.

Step 2:- You punch in the button the item you want and record of that get updated in Ethereum network or ledger.

Step 3:- The items comes out & you collects it and this gets recorded by all nodes & ledger

Every transaction you do through smart contract will get recorded & updated by network.

Anything that runs on blockchain need to be immutable and must have ability to run through multiple nodes without compromising on integrity. As a result smart contracts functionality needs to be three things.

1. Deterministic
2. Terminable
3. Isolated.

1. Deterministic:- A program is deterministic if it gives same output to a given input every single time.

2. Terminable:- It states that program should execute its function in time limit, should not everlast

3. Isolated:- If the contract is not isolated, this may hamper the whole system. It is critical for a contract to kept isolated in a sandbox to save entire ecosystem from negative effects.

Virtual Machines provide better deterministic, terminable and isolated environment for Smart Contracts.

The Ethereum Virtual Machine (EVM) is a Virtual machine in which all Smart Contracts function in Ethereum. It is simple yet powerful turing complete 256-bit Virtual machine.

Solidity is Smart Contract language on ethereum, developed on top of EVM. It allows you to perform arbitrary computations, but main purpose is to send and receive digital token

Solidity programs

1. Addition

```
pragma solidity 0.6.6;

contract gfgMathPlus
{
    uint firstNo;
    uint SecondNo;

    function firstNoSet(uint x) public
    {
        firstNo = x;
    }
    function SecondNoSet(uint y) public
    {
        secondNo = y;
    }

    function add() view public returns(uint)
    {
        uint sum = firstNo + SecondNo;

        return sum;
    }

}
```

2. Difference

```
pragma solidity 0.6.6;

Contract gfgSubtract
{
    int16 firstNo = 2;
    int16 secondNo = 10;

function Sub() view public return(int16)
{
    int16 ans = firstNo - secondNo;

    return ans;
}
}
```

* GHOST

GHOST :- Greedy Heaviest observed Subtree

The GHOST Protocol is an Innovation first Introduced by Yonatan Sompolinsky and Aviv Zohar in December 2013

The motivation behind GHOST is that blockchain with fast Confirmation times currently suffer from reduced Security due to high stale rate - because blocks take a certain time to propogate through network.

If miner A mines a block and then miner B happens to mine another block before miner A's block propogates to B, miner B's block will end up wasted and will not contribute to network Security.

Furthermore, there is a centralization issue: If miner A has mining pool with 30% of hash power, B has 10% hashpower. A will have a risk of producing stale block 70% of time while B has 90%. Thus, if the block interval is short enough for stale rate to be high, A will be substantially more efficient simply by virtue of its size.

As described by Sompolinsky and Zohar, GHOST solve the first issue of network security loss by including stale blocks in calculations of which chain is the longest; that is to say., not just the parents & further ancestors of the block, but also the state descendants of block's ancestor (uncles) are added to calculation of which block has the largest total proof of work backing it.

To solve the 2nd issue of centralization bias we go beyond this protocol, and also provide block rewards to stales: a state block receives 87.5% of its base reward, and the nephew that includes the state block receives remaining 12.5%. Transactions fees, however, are not rewarded to uncles.

Ethereum implements a simplified version of GHOST which only goes down seven leves. defines as follows

A block must specify a parent, and it must specify 0 or more Uncles.

An Uncle included in block B must have following properties:

- It must be a direct child of k-th generation ancestor of B where $2 <= k <= 7$
- It cannot be an ancestor of B
- An Uncle must be a valid block header, but does not need to be a previously verified or even valid block.
- An Uncle must be different from all Uncles included in previous block and all other Uncles included in same block.

For every Uncle U in Block B, the miner B gets an additional 3.125% added to its Coinbase reward and the miners of U gets 93.75% of standard Coinbase reward.

The limited version of GHOST, with Uncles Includable only up to 7 generations was used for two reasons.

1. Unlimited GHOST would include too many Compilations into the Calculations of which uncles for a given block are valid

2. Unlimited GHOST with Compensation are used in Ethereum removes the Incentives for a miner to mine on the main chain and not the chain of a public attacker.

classmate
Date
Page

* Sidechain :-

Sidechains are the Emerging mechanisms that are trying to make Blockchain more Scalable and efficient. This mechanisms allowed the token and other digital asset from one blockchain to be securely used in another Blockchain and then be moved back to the Original blockchain when required.

Two most Commonly used sidechain are
1) RSK
2) Liquid

The sidechain mechanisms hold tremendous potential to enhance the capabilities of Existing blockchain. It is seperate Blockchain that is attached to its parent blockchain using two-way peg. Which makes whole process reversible.

In this Entire process, Blockchain is referred to as mainchain whill all additional Blockchain are refered as sidechains. Masterchain can be thought of as the parent chain and side chain as Sort of child chain.

Hardfork and sidechain are two different things. With the sidechain original chain remains unaffected and can be rejoined in future.

Sidechain to function it needs to have digital assets or tokens. Usually this comes from a user on parent chain. Assets that move between parent and sidechain are pegged both ways. This means the coins are transferred b/w the chains at a pre-agreed rate.

To get the coins on sidechain the user will send the coins to predetermined address connected with sidechain.

Once the locked funds from parent chain have been communicated across all chains they will become available on sidechain. The user can use the coins on sidechain. When moving cryptocurrency from sidechain back to parent chain, the process is effectively reversed.

Benefits of Sidechain :-

1. It allows new & potentially unstable s/w to get deployed and tested on sidechain. If in case the s/w ad causes harm to blockchain, the damaged will contain within the sidechain.

2. 2. The ability to have a faster mainchain, as transactions can takes place on either of sidechain. If developers are dissatisfied with the cost & speed, they can deploy dapps on sidechain.

3. Sidechain can lessen the burden of mainchain, as it can store data and process transactions, thus maintaining the integrity of mainchain while making it smaller & faster.

Sidechains are solely responsible for their security, and if there isn't enough mining power to secure a sidechain, it could be hacked. But since each sidechain is independent of each other. If it is compromised, the damage will be contained within that chain & will not affect parent chain.

The Concepts of RSK

RSK → Root Stock was born to be Compatible with Ethereum's applications but using bitcoin as underlying cryptocurrency.

RSK has created an open-source testnet called as Ginger for its sidechains. It has two-way peg with bitcoin blockchain & rewarded Bitcoin miners via merged mining with the basic idea behind the creation to give Bitcoin blockchain smart contract functionality and make payment process faster.

We can say, RSK is combination of

Turing machine resource-accounted deterministic virtual machine Compatible with Ethereum's EVM.
A two-way pegged bitcoin blockchain
A SHA-256D merge-mining consensus protocol

One of the most noticeable aspects of RSK is its focus on security, using monetary bounties to help appeal to developers, hackers and security professional to recognize vulnerabilities so that system can improve overall security for various stakeholders.

Liquid

The liquid is a sidechain-based settlement network used in traders and Exchanges that enables faster, more confidential Bitcoin transactions and provides issuance of digital asset as well.

This sidechain enables the rapid, confidential and secure transfer of funds between parties, providing a viable solution to underlying problem of delayed transaction finality of Bitcoin Network.

Liquid enables faster trading i.e almost instant bitcoin transfer between Exchanges to allow user to take benefit of Computer-assisted trading Opportunity.

Offers enhanced efficiency: this, Market makers can improve their Capital efficiency by reducing balances held across multiple Exchanges.

Liquid supports Confidential transactions for bitcoin amount as they are transferred b/w users in the system, which protects users from exposure.

When it comes to reliability, liquid software is highly reliable. Liquid blocks are programmed to be one-minute apart, making it remarkably secure.

classmate
Date
Page

* NameCoin :-

NameCoin is a cryptocurrency originally forked from Bitcoin software. A fork is simply a change in blockchain's protocol. NameCoin is based on the code of Bitcoin with additional functionality built on top of it. The namecoin used the same PoW consensus algorithm as Bitcoin. The two currencies are nearly identical.

Namecoin was developed as the basis for a decentralized Domain Name System (DNS). DNS translates human readable domain to machine readable IP Address. DNS is the mechanisms by which domain identities are linked with numerical IP addresses around the world. The decentralized of this system was intended to put an end to Internet censorship and Enhance Internet-related security & privacy.

Internet is actually based on numerical addresses called IP address. The DNS was created to make nag navigation Easier. The DNS can be thought of as Internet's address book.

Everytime we type a website address, a DNS server is contacted. The DNS servers locates the IP address of internet destination and retrieves the webpage data.

The final part of webpage domain (.com) is called top level domain (TLD) By introducing a decentralized DNS system, there can now be TLDs that exists that are not owned by anyone. The querying system for a decentralized DNS is shared on peer-to-peer system. The TLD .bit is the first and only TLD of Namecoin's domain. The steps for registering a new domain or updating an existing domain are built into Namecoin's protocol.

Namecoin is a key/value pair registration and transfer system based on Bitcoin technology. This means Namecoin can be used to record & transfer arbitary names or keys in a secure fashion. It can also attach data to this name.

Because of their links with Namecoin network, these names are difficult to censor or seize, meaning that they are resistant to outside influence. Additionally, the makers of Namecoin specify that lookups do not generate network traffic. The result of this is that Namecoin offers improved privacy capabilities.