Lobstex (LOBS)

Zerocoin: Masternodes: Anonymous

Trust Thy Trustless

Whitepaper v1.0

Introduction

Cryptocurrency is a digital asset that inherently act as an exchange medium using the technology of cryptography to safely secure it's concerned transactions resulting in control of the newly generated additional currency units and subsequently verifying the asset transfer.

If we look back at the history of cryptocurrencies, Satoshi Nakamoto, the pseudonymous inventor of Bitcoin, never had the intention of inventing a cryptocurrency viz. Bitcoin. Nakamoto, made an announcement in late 2008 about Bitcoin, he mentioned about the development of an electronic cash system based on peer to peer.

"Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority".

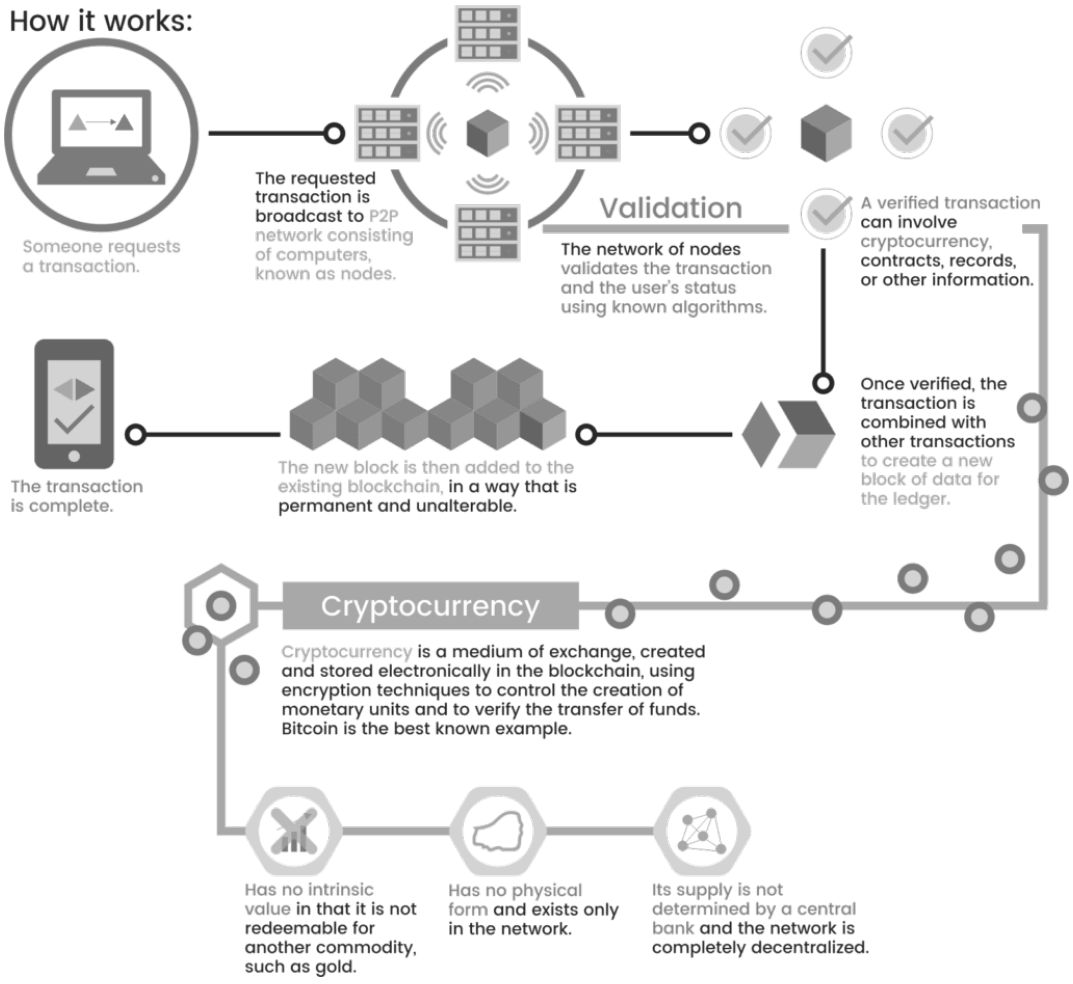
– Satoshi Nakamoto, 09 January 2009, announcing Bitcoin on SourceForge.

Nakamoto, took along the concept of digital cash and added a dimension of decentralization, after the concept of digital money failed in 90's decade :

" … after more than a decade of failed Trusted Third Party based systems (Digicash, etc), they see it as a lost cause. I hope they can make the distinction, that this is the first time I know of that we're trying a non-trust based system".

– Satoshi Nakamoto in an E-Mail to Dustin Trammell

The problems faced in this system were double spending and consensus system to verify without having a central authority in control. In a network having decentralized perspective, there is no particular server. Thus, every single unit of node or network fulfil this promise of completing the job. The network works on the basis of every single peer having a list of all transactions to verify and check regarding the validity and of forthcoming transactions and minimise the risk of double spending. The proposed consensus included a set of rules, most of which regard transaction's validation and transaction's block. The latter are transaction groups close in time, cryptographically concatenated to compose the blockchain, that led to birth of cryptocurrency.



Source: Blockgeeks

The main properties of cryptocurrency includes: Irreversible (once a transaction is made it is not possible to retrieve it back), Pseudonymous (neither the transaction nor accounts are connected to there real identities of users), Permission-less (no central authority to monitor and gatekeeping to your transactions on blockchain), Boundary-less (no geographical boundaries for any transaction), Secure (cryptographically only public key is visible, private key is always protected), Fast (transaction takes place near instantaneous in real time).

Evolution of Privacy

The first cryptocurrency i.e. Bitcoin works on the principle of transparency at an unprecedented level which the people find difficult to comprehend. Every transaction made on Bitcoin blockchain is traceable, in public scrutiny and are stored on blockchain network permanently. The addresses used in Bitcoin blockchain provides the visibility and information regarding the origin and destination of bitcoin transactions. Although, the addresses are private in nature but overtime they can be easily traced with the help of tracking back transactions on blockchain and can be pinpointed to the origin providing a complete history of all the nature, time and place (ip) to locate the same. As the bitcoin blockchain is transparent anyone can track the final and used balance of a wallet or address. As the users provide the identity of wallet address to offer and receive services/goods, the anonymity of a transaction gets hampered. Given the nature of permanency of blockchain what might not be traceable or trackable presently could be traced easily in future. An advice to users can be provided to users to generate new addresses for every transaction on internet. The bitcoin was perceived to be

anonymous network for payment flow, however, it is the pinnacle of transparency on a decentralized network.

The basic ideology behind the first cryptocurrency Bitcoin and for that matter every other crypto in world was created with an intention of removing the centralized governance of prevailing monetary system and providing the power and governance to people by snatching from the governance of governments and centralised banking system. The technology of cryptography was used to make the monetary system transparent and free from the clutches of centralization. The transparent technology behind Bitcoin provided it as an alternative to controlled monetary assets having the various layers of security and anonymity to an extent.

1. Fungible: Every unit of the crypto currency base has the same value and can be interchanged on mutual basis. There is no inherent risk of blacklisting and debasement because of depreciated transactional history
2. Private: Upto a certain extent the transactions, the wallet, history and nature are not traceable easily
3. Decentralized: Every node on the network has equal controlling power over blockchain minimizing the centralized nature of prevailing monetary currencies. The crypto does not represent any central authority to adhere to.

The revolution in financial sector sermonize the needed freedom in managing and maintaining one's financial aspect of transferring value from one end to another without having any pre required permission from centralised agencies whether government or banks or any third party, giving the

transparency to all transactions provided it is used for only legal means, for this purpose it was created.

Masternode

"If you don't find a way to make money while you sleep, you will work until you die." - Warren Buffett

Masternode can be best described as a network of decentralized nodes to utilize some peculiar functionality which a normal node doesn't entails. The basic features includes instant transactions with the privacy status in addition to bring stability to blockchain. The masternodes perform some other functions too in comparison to normal nodes. The masternode function was first conceptualized by the cryptocurrency Dash.

The special functions which master nodes perform in comparison to normal nodes are:

✓ Heightening the private nature of transactions

✓ Making transactions instantaneous

✓ Providing base for healthy governance and equality in voting system

✓ Additionality to Budget provisioning and Treasury functions

The Masternodes (MN) does not work on a standalone point, however, are always interacting and communicating with other basic nodes to make the network more decentralized and performing the required functionality.

However, as it is a special category which comes with some pre qualification to enjoy the higher benefits compared to basic nodes to keep the systematic malignancy in abyss. There are some entry point barriers to operate masternodes as one need to keep a collateral of the basic currency units under lock, and it varies from one currency to other.

The basic requirements to setup Lobstex Masternode:

- A minimum amount of coins : 10000 LOBS
- A separate VPS (virtual private server) Ubuntu 16.04 x 64 operating 24 x 7 for hosting wallet
- A dedicated IP address to do the same
- Additional storage space for saving the blockchain

The masternode owners gets incentivized more by providing a collateral to the blockchain system compared to Pow or Pos miners. As a result of this, masternodes give genuine services to the whole blockchain in a validation system of bondage. The concerned bondage is not permanent as the owners are responsible for providing stability as collateral or liquidating by shutting the node off. The benefits of having a masternode weighs more to not having one, as it provides more consistency and locking the coins means less circulating supply resulting in appreciation of concerned cryptocurrency.

Proof of Stake (PoS)

Proof of Stake is a system of validating the transactions on blockchain to achieve a consensus in a distributed manner. The algorithm is different from Proof of Work, however the purpose and outcome remains same keeping the process unlike.

The first time Proof of Stake was idealized in a cryptocurrency forum bitcointalk dated back at initial stage of Bitcoin in 2011, however, the idea was first conceptualized in a cryptocurrency name Peercoin back in 2012, later on followed by other coins like Blackcoin, Navcoin, Nxt, etc

In a system of proof of work the miners are rewarded to solve complex mathematical problems governed by an algorithm with an aim to validate the given transactions on blockchain and generating new blocks, however, in case of proof of stake the algorithm determines and chooses the new block in a simplistic and deterministic manner which depends on the wealth of wallet holder, called as staking.

There is no block reward in Proof of Stake like PoW, as the crypto currency or coins generated from the start remains unchanged and as there is no reward per block, the transactional fee is taken by miners, thus, in the system of PoS, miners might also be called as forgers.

The validators in proof of stake does not use the computational power of their machines, as the only requirement is having the number of coins in

your wallet and staking them receives new coins depending on the complexity and difficulty of concerned blockchain. The number of coins in your wallet or wealth determines the stake or coins one will generate over the course of time.

The new scenario of such staking has opened up the options to discourage PoW coins in future because of the benefits it entails:

1. The PoW requires a high computational power from machines, however PoS is simplistic and resulting in huge savings in energy, which is unfortunately a limited resource.

2. In comparison to PoW, the chain on PoS is safer, as network attacks on blockchain become highly expensive, take a case of hacking where a 51% attack happens and the reaction will be of high appreciation in coin value on market, thus making it more unlikely.

In the Proof of Stake system of algorithm, the efficiency in generating new coins increases manyfold as it is environmental friendly and having substantially low costs compared to PoW gauging more participation from the coin holders or masses which finally result in the main aim of creating blockchain's decentralization freeing from the clutches of autocratic monetary system.

Zerocoin Protocol

Zerocoin aims to be the protocol which is decentralized in nature using the e-cash schematics providing quite a proven user anonymity and security of coin based on simplistic assumption of a distributed consensus in an online and append-only transactions over the blockchain. zLOBS works on zero-coin protocol by enforcing zero-knowledge proofs. The zLOBS (zerocoin) feature will be activated at 43201 block when the PoW will end.

How to mint process: Firstly you need to select the number of coins when you want to send a private transaction with zLOBS. After determining the numbers, the balance of your normal coin will reduce by crediting the new zLOBS having no history of transaction. The concept of burning comes in picture, the old coins gets burned using cryptography making it inaccessible and creating a preventive shield to use old coins by anyone on chain and tracking the same to one's transactional history. The total supply remain unchanged with new coins on system and old coins being burnt, one is ready to do the most private transaction in world without having any trace-ability.

The denomination of minting zLOBS are in 1,5,10,50,100,500,1000 and 5000 currently on Lobstex chain. Take an example of '100' new zLOBS to be minted, after burning the old coin instantly the new coins '100' zLOBS will be credited in your wallet having no history of whatsoever.

How to Spend: If you want to make a private and anonymous transaction, the new '100' zLOBS will be used in the process. The amount will be sent to a wallet with no history attached to it, in any denomination of choice from the pool.

Repeating the process : In the same manner, whenever a private transaction is the need, the wallet owner will mint the new coins and send it to new wallet 'n' number of times, keeping the privacy as focus.

The anonymity feature of Lobstex (LOBS) offers the par level of best practices in crypto world when one mints and spend the zLOBS (zerocoins)

There are two layers or systems of Lobstex (LOBS)

LOBS (as the base coin)
zLOBS (zerocoin)

LOBS is the base coin of chain, which acts as normal coin in compared to any other blockchain coin like Bitcoin. Every transaction of LOBS is visible on the chain using explorer and transparent in nature, keeping the address on same level as Bitcoin blockchain having public history and accessible to all.

The zLOBS (zerocoin) layer is however will provide the full privacy and anonymity to the transaction and it works by using the method of minting new coins and spending the same. The zerocoin protocol is the mechanism where the old coins are burnt to provide new coins with no history and then converting the new coins to old coins, and the process goes on and on to remove the traces of any public visibility. In contrast to other methods of

coins having mixing algorithm, zLOBS does not interact or rely upon any other wallets or entity for mixing coins, thus it works on the fundamental of creation of new coins in Lobstex's own zerocoin protocol instead of relying on unhealthy mixing of old coins which might prove to be vulnerable in regard to full privacy.

Budget System and Governance

Lobstex Budget System allows for community based governance. The fundamental challenge to a blockchain comes when the work gets halted after the deployment of it due to lack of funds. Thus, there has always been a pressing need for additional funding in order to carry on the process and development. Lobstex Budget system allows for the necessary funding for developers fee, marketing and miscellaneous tasks to be performed.

How Budget system works

Lobstex budget system relies on the fair and transparent governance of community. It is the Masternode holders who can vote for a particular budgetary task. The 'Yes' has to be more than 'No', for a task to be accepted. The budget proposals can be seen from Tools, debug console of wallet using "mnbudget show" command and voted by using "mnbudget vote" in the console.

To keep the community driven projects focus will be more on development of project and it's marketing strategies. Lobstex derives the value from the consensus system of governance to give equal opportunity to take part in the process of decision making for the future needs. The master nodes apart from providing the stability to blockchain keep the decentralized governance in control.

Lobstex (LOBS) Specifications

Website: www.lobstex.com

Official launch date : 02 MAY, 2018

Coin Basic Specs

Name: Lobstex

Ticker: LOBS

Algorithm: Quark

Type: PoS and PoW (Initially)

RPC Port: 15156

P2P Port: 14146

Blocks

Block Time: 60 sec

Structure:
~ 0 TO 43200 : PoW
~ 43201 to INF: Pos

Total Supply: Infinite (78.6 million in 10 years)

Circulating Supply: 7.8 mil

Masternodes

Collateral: 10000 LOBS
Mature Time : 4 Hours

Reward Structure:

~ 0 to 5000 : No Reward, 100% Miners
~ 5001 to 43200 : 50% Masternodes, 50% Miners
~ 43201 TO INF : 60% Masternodes, 40% Stakers

Staking Block Rewards

0 to 500: 5 Per Block (Anti Instamine)
501 to 100000: 40 Per Block
100001 to 300000: 30 Per Block
300001 to Inf: 15 Per Block

Zerocoin Protocol

zLOBS - activated at 43201 Block

Wallets

www.lobstex.com

https://github.com/avymantech/lobstex/releases/tag/v2.0

Block Explorer

http://explorer.lobstex.com/

https://lobstex.chainmapper.com/

Github

https://github.com/avymantech/lobstex

Roadmap

Q2, 2018 : New Exchanges , Whitepaper, Zerocoin Protocol, Publicity

Q3, 2018 : Mobile Wallets, Partnerships, New Exchanges

Q4, 2018 : LOBS Exchange, Dealership Program, Bigger Exchanges

Q1, 2019 : Colossal Protocol,QR Integration, Marketplace

Exchanges

FatBTC https://www.fatbtc.com/
CryptoBridge https://crypto-bridge.org/
Graviex https://graviex.net/markets/lobsbtc

Contact

support@lobstex.com

vacancy@lobstex.com

market@lobstex.com

Social

ANN https://bitcointalk.org/index.php?topic=3483089.0
Twitter https://twitter.com/LOBSTEXofficial
Discord https://discord.gg/pdUX3Uh
Telegram https://t.me/lobstexofficial
Reddit https://www.reddit.com/user/lobstex
Medium https://medium.com/lobstex