Virtuoso Infotech Pvt. Ltd.

virtuoso
INFOTECH

About Virtuoso Infotech

- Fastest growing IT firm; Offers the flexibility of a small firm and robustness of over 30 years experience collectively within the leadership team
- Technology expertise & passionate team
- Successful client engagements across India, USA, UK, Australia and Argentina
- Handle enterprise solutions that involve **30,000 active users**, more than 20 servers, **data volume as big as 5 million entries per day**

Cryptocurrency

- Bhargav Mehta

Quick Recap

- What are ledgers?
- What is a blockchain?

Agenda

- Distributed Ledger (DLT)
- Introduction to Cryptocurrency
- Transaction
- Security
- Mining and Proof-of-work
- Incentive
- Valuation
- Top Cryptocurrencies

Distributed Ledger Technology [DLT]

- Spread across several nodes or computing devices.
- Each node replicates and saves an identical copy of the ledger.
- No central authority.
- Updates to the ledger are independently constructed and recorded by each node.
- The nodes then vote on these updates to ensure that the majority agrees with the conclusion reached. This is called **Consensus**

Distributed Ledger Technology [DLT]

- Generally used synonymously with Blockchain. However - **Every blockchain is a distributed ledger, but not every distributed ledger is a blockchain.**
- Not all distributed ledgers employ a chain of blocks to provide a secure and valid distributed consensus.
- Other options are Directed Acyclic Graphs based of which IOTA, HashGraphs are few of the most popular.
- These options improve upon the few shortcomings of blockchain of which the foremost is transaction speed which is very limited due to Proof Of Work.

Introduction to Cryptocurrency

- Cryptocurrency is a digital currency that uses cryptography to generate currency and verify transactions.
- No central issuing authority or body - Decentralized control.
- Fully digital currency that is transferred between a peer to peer network.
- Transactions are added to a distributed public ledger – generally Blockchain.
- It is not a data that can be duplicated.
- There are a lot of nodes keeping track of the same ledger.

Transaction

- A transaction just says, “Bhargav gives 20 Bitcoin to Yogesh.”
- A transaction is broadcasted in the network, sent from one peer to every other peer. This is basic p2p-technology.
- The transaction is known almost immediately by the whole network. But only after a specific amount of time it gets confirmed.
- Confirmation is a critical concept in cryptocurrencies. Once confirmed, the transaction is part of an immutable record of historical transactions [Blockchain].

Security

- Here cryptography comes into play
- Cryptocurrency transactions are done through cryptocurrency wallets, where each member has a private key and public key.
- Sender signs the transaction with their private key and attaches the sender’s public key to the transaction broadcast.
- In case if you loose your private key, there is no way you can retrieve your data as there is no other way to access it.
- Before every transaction it checks if you have enough coins. However network delays can cause Request order to be different.

Proof-of-Work / Mining

- But What about? Network Delays and Confirmation Validation.
- Double spending problem
- To validate a transaction you have to find a hash – a product of a cryptographic function – that connects the new block with its predecessor.
- This is called the **Proof-of-Work.** And the process is called **Mining.**
- The network rules are such that the difficulty is adjusted to keep block production to a specific time. [10 minutes for bitcoin.]
- More miners engage in the mining, more difficult to produce a block.
- The higher the total difficulty, the harder it is for an attacker to overwrite the block.

Why? Incentive

- Why would you or someone manage a ledger? It takes immense computational power and resources.

- For every new block you add you get cryptocurrency as reward. Currently you get 12.5 new coins for every new block you add for Bitcoin.

- There are also transaction fees that can be obtained after processing the transactions

Valuation

- Adoption rate
- Supply - Demand
- Market sentiments
- News and Hypes
- Currently it is very volatile as the value is determined as potential and instead of currency it is used for trading
- However, in future when actual applications come up, their valuation may be determined by their utility and liquidity.

Top Cryptocurrencies

Bitcoin

Ethereum

Ripple

Litecoin

Dash

Zcash

Bitcoin (BTC)

- The first streamlined cryptocurrency.
- Uses "**Hash-Cash**" as a proof of work.
- It is the most popular cryptocurrency.
- June 2018, market cap - $128.3 Bn; June 21, 2018 closing - $6707.04.

Ethereum (ETH)

- Enables **Smart Contracts** and **Distributed Applications (ĐApps)** to be built and run without downtime, fraud, control or interference.
- The applications run on its platform-specific cryptographic token, **ether**.
- Ether is like a vehicle for moving around on the Ethereum platform, sought by mostly devs looking to develop and run apps in Ethereum.
- It can be used to “codify, decentralize, secure and trade just about anything.”
- Second after Bitcoin among all cryptocurrencies.
- June 2018, market cap - $47.47 Bn; June 21, 2018, closing - $525.77.

Ripple (XRP)

- It is a real-time global settlement network that offers instant, certain and low-cost international payments. Enables banks to settle cross-border payments real time, with transparency and lower costs.

- Ripple's consensus ledger -- its method of conformation -- doesn't need mining, a feature that deviates from bitcoin and other altcoins.

- This reduces the usage of computing power, and minimizes network latency.

- Believes that 'distributing value is a powerful way to incentivize certain behaviors'. Currently plans to distribute XRP primarily "through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP."

- June 2018, market cap - $18.9 billion; June 21, 2018, closing - $0.534.

Litecoin (LTC)

- Amongst initial cryptocurrencies, was often referred as ‘silver to Bitcoin’s gold.’
- Litecoin is based on an open source global payment network that is not controlled by any central authority.
- Uses "**scrypt**" as a proof of work, which can be decoded with the help of CPUs of consumer grade.
- It has a faster block generation rate and hence offers a faster transaction confirmation.
- June 2018, market cap - $4.89 Bn; June 21, 2018 closing - $96.7.

Zcash (ZEC)

- “If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself.
- Offers privacy and selective transparency of transactions. All transactions are recorded and published on a blockchain, but details such as the sender, recipient, and amount remain private.
- Offers its users the choice of ‘shielded’ transactions, which allow for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a **zk-SNARK** developed by its team.
- June 2018, market cap - $713.254 Mn; June 21, 2018, closing - $190.22.

Thank You!

Virtuoso InfoTech Pvt. Ltd.
4th Floor, Victory Landmark, Opp.
D-Mart,
Behind Dominos Pizza, Baner, Pune.

+91 8087081318
support@virtuosoitech.com

www.virtuosoitech.com