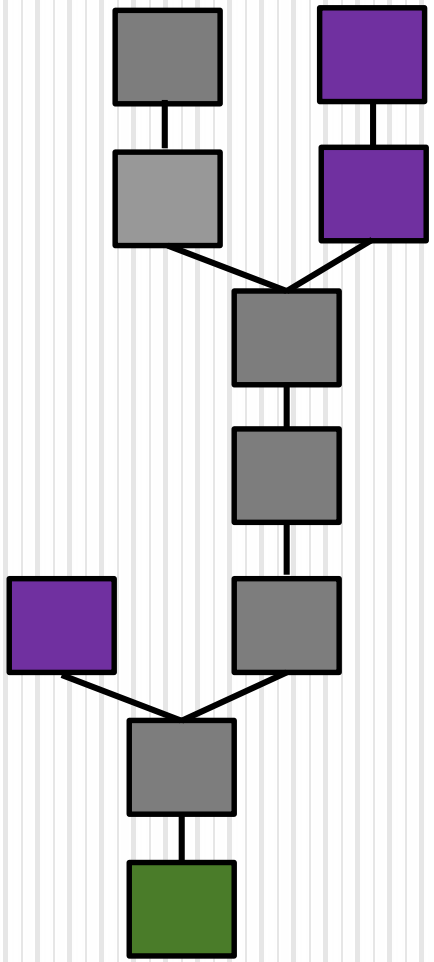
Virtuoso Infotech Pvt. Ltd.

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**

Blockchain



- Yogesh Kanhurkar

Agenda

- Cryptography
- Ledger
- Double Spending Problem
- Introduction to Blockchain
- Features
- Types
- Uses

Cryptography

- Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

Cryptography

- Various aspects in **information security** such as **data confidentiality**, **data integrity**, **authentication**, and **non-repudiation** are central to modern cryptography.
- Modern cryptography exists at the intersection of the disciplines of **mathematics**, **computer science**, **electrical engineering**, **communication science**, and **physics**.
- Applications of cryptography include **electronic commerce**, **chip-based payment cards**, **digital currencies**, **computer passwords**, and **military communications**.

Ledger

- A ledger is the principal book or computer file for recording and totaling economic transactions measured in terms of a monetary unit of account, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.
- The ledger is a permanent summary of all amounts entered in supporting journals which list individual transactions by date.
- A company's financial statements are generated from summary totals in the ledgers.

Types of Ledger

- **Sales ledger**
  - records accounts receivable.
  - This ledger consists of the financial transactions made by customers to the company.
- **Purchase ledger**
  - records money spent for purchasing by the company.
- **General ledger**
  - representing the five main account types: **assets**, **liabilities**, **income**, **expenses**, and **Capital**.

Unit of Account

- A unit of account in economics is a nominal monetary unit of measure or currency used to represent the real value (or cost) of any economic item; i.e. goods, services, assets, liabilities, income, expenses.
- It is one of well-known **functions of money**. It lends meaning to **profits**, **losses**, **liability**, or **assets**.
- A unit of account in financial accounting refers to the words that are used to describe the specific **assets** and **liabilities** that are reported in **financial statements** rather than the units used to measure them.

Double Spending Problem

- The risk that a digital currency can be spent twice.
- Double-spending is a problem unique to digital currencies because digital information can be reproduced relatively easily.
- With digital currency, there is a risk that the holder could make a copy of the digital token and send it to a merchant or another party while retaining the original.
- Fundamental cryptographic techniques to prevent double-spending while preserving anonymity in a transaction are **blind signatures** and particularly in offline systems, **secret splitting**.

Introduction to Blockchain

- A blockchain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography.
- It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".
- For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

Introduction to Blockchain

- Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.
- Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.
- Decentralized consensus has been achieved with a blockchain.

Introduction to Blockchain

- Blockchain was invented by **Satoshi Nakamoto** in 2008 to serve as the public transaction ledger of the cryptocurreency **bitcoin**.
- The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a **trusted authority** or **central server**.

What is Block?

- Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree.
- Each block includes the cryptographic hash of the prior block in the blockchain, linking the two.
- The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block.

Features

- SHA256 Hash Function
- Public Key Cryptography
- Distributed Ledger & Peer to Peer Network
- Proof of Work
- Incentives for Validation

Types

- **Public Blockchain:**
  - A public blockchain has absolutely no access restrictions.
  - Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol).
  - Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.
  - e.g. Bitcoin and Ethereum.

Types

- **Private blockchains**
  - A private blockchain is permissioned.
  - One cannot join it unless invited by the network administrators. Participant and validator access is restricted.
  - This type of blockchains can be considered a middle-ground for companies that are interested in the blockchain technology in general but are not comfortable with a level of control offered by public networks.
  - Typically, they seek to incorporate blockchain into their accounting and record-keeping procedures without sacrificing autonomy and running the risk of exposing sensitive data to the public internet.

Types

- **Consortium blockchains**
  - A consortium blockchain is often said to be semi-decentralized.
  - It is permissioned but instead of a single organization controlling it, a number of companies might each operate a node on such a network.
  - The administrators of a consortium chain restrict users' reading rights as they see fit and only allow a limited set of trusted nodes to execute a consensus protocol.

Uses

- The sharing economy
- Governance
- Prediction markets
- Stock trading
- Identity management
- Land title registration
- Crowdfunding
- Supply chain auditing
- File storage
- AML and KYC
- Protection of intellectual property

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