VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

BCSE324L

Dr. Malathi D.

FOUNDATIONS OF BLOCKCHAIN TECHNOLOGY

Course Objectives

- To understand building blocks of Blockchain.
- To significance of Distributed Ledger Technology and Smart Contract.
- To exploit applications of Blockchain in real world scenarios and their impacts.

Expected Outcomes

- Understand Blockchain ecosystem and its services in real world sceneries
- Apply and Analyze the requirement of Distributed Ledger Technology and Smart Contract
- Design and Demonstrate end-to-end decentralized applications
- Acquaint the protocol and assess their computational requirements

Distributed Ledger Technology

Distributed Ledger Technology

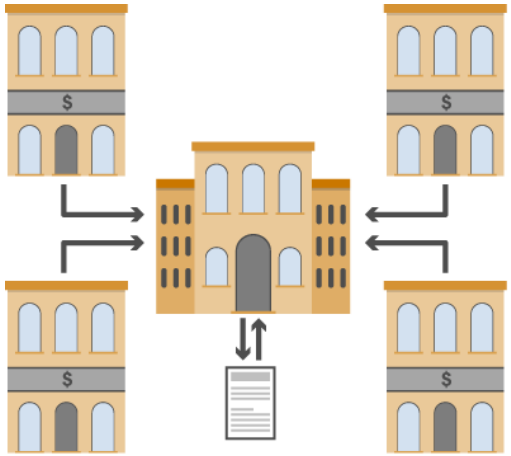
- Origin of Ledgers
- Types and Features of Distributed Ledger Technology (DLT)
- Role of Consensus Mechanism
- DLT Ecosystem
- Distributed Ledger Implementations
    - Blockchain – Ethereum
- Public and Private Ledgers
- Registries and Ledgers
- Practitioner Perspective: Keyless Technologies, Transparency as a Strategic Risk, Transparency as a Strategic Asset, Usage of Multiple IDs
- Zero Knowledge Proofs
- Implementation of Public and Private Blockchain

Distributed Ledger Technology

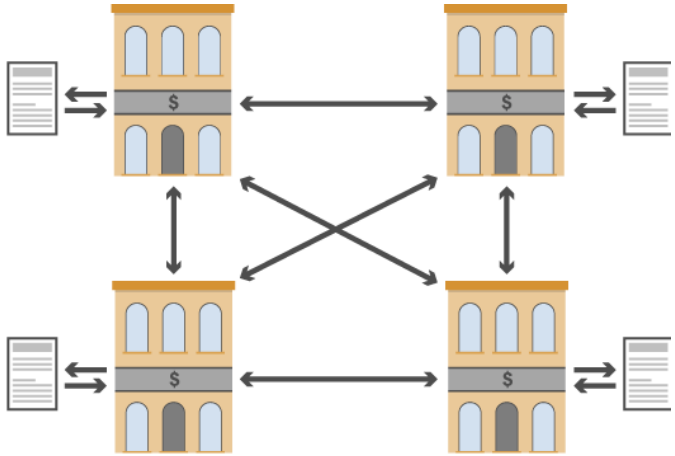
- Distributed ledger technology (DLT) is a **digital system for recording the transaction of assets** in which the transactions and their details are **recorded in multiple places at the same time**.
- Distributed ledgers have **no central data store or administration functionality**.
- **Characteristics**: Enable the **simultaneous access, validation and updating** of records.
- It **works on a computer network** spread over **multiple entities, locations or nodes**.
- DLT is the technology **blockchains are created from**, and the infrastructure **allows users to view any changes and who made them, reduces the need to audit data, ensures data is reliable, and only provides access to those that need it**.
- In a distributed ledger, **each node processes and verifies every item**, thereby **generating a record** of each item and **creating a consensus** on its veracity.
- A distributed ledger can be **used to record static (registry) and dynamic data (financial transactions)**.
- **Blockchain is a well-known example of a distributed ledger technology**.

Distributed Ledger Technology

- **Traditionally**, Organizations have long gathered and stored data in multiple locations either on paper or in siloed software, **bringing the data together in a centralized database only periodically**.
- **Example**:
  - A company might have different bits of **data held by each of its divisions**, with divisions **contributing that data to a centralized ledger** only when required.
  - **Multiple organizations working together** typically **hold their own data** and **contribute it to a central ledger** controlled by an **authorized party** only when requested or required.



Centralized Ledger



Distributed Ledger

Distributed Ledger Technology

- Nowadays, DLT has the **ability to minimize or eliminate the time-consuming and error-prone processes** needed to reconcile the different contributions to the ledger, also ensure that **everyone has access** to the current version and its **accuracy can be trusted**.
- DLT's **main difference from traditional centralized ledgers** is that
  - a **copy of the ledger is distributed** to each node on the network
  - every node can **view, modify and verify** the ledger
  - ensure **trust and transparency**.
- Distributed ledgers have been around for decades but have become more well-known, researched, used, and developed **since Bitcoin was introduced**.
- Distributed ledgers can be **used in nearly every industry** where data is collected and used.
- **All blockchains are distributed ledgers, but not all distributed ledgers are blockchains**.
- Though DLT enhances accountability, security, and accessibility, it is **still complex and difficult to scale**.

Distributed Ledger Technology

Origins of ledgers

- **Ledgers**, which are essentially a record of transactions and similar data, **have existed for millennia in paper form**. They became digitized with the rise of computers in the late 20th century, although computerized ledgers **generally mirrored what once existed on paper**.
- **Required a central authority to validate the authenticity of the transactions** recorded in them. **For example**, **banks need to verify the financial transactions** that they process.
- 21st-century technology has enabled the **next step in record-keeping with cryptography, advanced algorithms, and stronger and near-ubiquitous computational power**, making the distributed ledger an increasingly viable form of record-keeping.
- Improved **connectivity through intranet and internet protocols** allowed for much more data to be collected, analyzed, and used.
- Now be many users with access to data, it is necessary to have **someone verify the changes**.
- Computer and data scientists developed programs that **reduced the need for auditing data**, uses **automation and data encryption techniques** to verify transactions or changes in a database's state.
- This is called **consensus**—the act of automated **majority agreement on transaction validity**, where a transaction is **simply a change** made to a database's state.

Distributed Ledger Technology

Types of Distributed Ledger Technology

- The Distributed Ledgers can be broadly categorized into three categories:
  - **Permissioned DLT**: Nodes have to **take permission from a central authority to access or make any changes** in the network. Mostly these types of permissions include identity verification.
  - **Permissionless DLT**: There is **no central authority to validate transactions**, rather **existing nodes are collectively responsible for validating the transactions**. Various consensus mechanisms are used to validate transactions based on predefined algorithms.
  - **Hybrid DLT**: It is combined with both permissionless and permissioned DLTs and can benefit from both of them.
- Some other types of DLT are
  - **Blockchain**: **Transactions are stored in the form chain of blocks** and each block produces a unique hash that can be used as proof of valid transactions. Each node has a copy of the ledger which makes it more transparent.
  - **Hashgraph**: Records are stored in the form of a directed acyclic graph. It uses a different consensus mechanism, **using virtual voting as the form consensus mechanism for gaining network consensus**. Hence nodes do not have to validate each transaction on the network.

Distributed Ledger Technology

Types of Distributed Ledger Technology

- **Directed Acyclic Graphs (DAG)**: **Uses a different data structure** to organize the data that brings more consensus. **Validation of transactions requires the majority of support from the nodes** in the network. Every node on the network has to provide proof of transactions on the ledger and then can initiate transactions. In this nodes have to **verify at least two of the previous transactions** on the ledger to confirm their transaction.
- **Holochain**: Holochain is termed as the next level of blockchain as it is much more decentralized than blockchain. It is a type of DLT that simply proposes that each node will run on a chain of its own. Therefore **nodes or miners have the freedom to operate autonomously**. It basically moves to the **agent-centric structure**. Here agent means computer, node, miner, etc.
- **Tempo or Radix**: Tempo uses the method of making a partition of the ledger this is termed sharding and then all the events that happened in the network are ordered properly. Basically, transactions are added to the ledger on basis of the order of events than the timestamp.

Distributed Ledger Technology

Features of Distributed Ledger Technology

- **Decentralized**: It is a decentralized technology and **every node will maintain the ledger**, and if any data changes happen, the ledger will get updated. The **process of updating takes place independently** at each node. Even small updates or changes made to the ledger are reflected and the history of that **change is sent to all participants** in a matter of seconds.
- **Distributed**: To counter the weaknesses of having one ledger to rule all, there is no one authoritative copy and have specific rules around changing them. This would **make the system much more transparent and will make it a more decentralized authority**. In this process, **every node** or contributor of the ledger will try to **verify the transactions with the various consensus** algorithms or voting. the voting or participation of all the nodes depends on the rules of that ledger.
- **Immutable**: Distributed ledger **uses cryptography to create a secure database** in which data **once stored cannot be altered** or changed.
- **Shared**: The distributed ledger is not associated with any single entity. It is **shared among the nodes on the network where some nodes have a full copy of the ledger while some nodes have only the necessary information** that is required to make them functional and efficient.

Distributed Ledger Technology

Features of Distributed Ledger Technology

- **Append only**: Distributed ledgers are append-only in comparison to the traditional database where data can be altered.
- **Smart Contracts**: Distributed ledgers can be **programmed to execute smart contracts**, which are self-executing contracts **with the terms of the agreement between buyer and seller** being directly written into lines of code. This allows for transactions to be **automated, secure, and transparent**.
- **Fault Tolerance**: Distributed ledgers are **highly fault-tolerant because of their decentralized nature**. If one node or participant fails, the data remains available on other nodes.
- **Transparency**: Distributed ledgers are transparent because **every participant can see the transactions** that occur on the ledger. This transparency **helps in creating trust among the participants**.
- **Efficiency**: The distributed nature of ledgers makes them highly efficient. Transactions can be **processed and settled in a matter of seconds**, making them **much faster** than traditional methods.
- **Security**: Distributed ledgers are highly secure **because of their cryptographic nature**. Every transaction is recorded with a cryptographic signature that ensures that it cannot be altered. This makes the technology **highly secure and resistant to fraud**.

Distributed Ledger Technology

How do distributed ledgers work?

- DLT works based on **principles of decentralization**. It eliminates the need for a central authority and **reduces the risk of a single point of failure**.
- DLT **operates on a peer-to-peer (P2P) network**, where multiple nodes store, validate and update the ledger simultaneously, make the whole process much **faster, more effective, and cheaper**.
  - The process begins with the **replication of digital data** across the network of nodes.
  - **Each node maintains an identical copy** of the ledger and **independently processes new update** transactions.
  - To ensure consensus, **all participating nodes employ a consensus algorithm** that determines the correct version of the ledger.
  - Once a consensus is reached, the **updated ledger is propagated to all nodes**, ensuring synchronization and accuracy.
- DLT **uses cryptography to securely store data** and cryptographic **signatures and keys to allow access** only to authorized users.
- **Creates an immutable database**, which means information, once stored, cannot be deleted and any updates are permanently recorded for posterity.

Distributed Ledger Technology

How do distributed ledgers work?

- **Architecture represents** a major change in **how information is gathered** and **communicated** by moving record-keeping **from a single, authoritative location to a decentralized system** in which all **relevant entities can view and modify the ledger**.
- **Transparency**: All other entities **can see who is using and modifying the ledger**. This transparency provides a **high level of trust** among the participants and **eliminates the chance of fraudulent activities** occurring in the ledger.
- DLT **removes the need for entities using the ledger to rely on a trusted central authority** that controls the ledger or an outside, third-party provider to perform that role and **act as a check against manipulation**.
- Because they are **decentralized, private, and encrypted**, DLs are **less prone to cybercrime**, as **all the copies stored across the network** need to be **attacked simultaneously** for the **attack to be successful**.

Distributed Ledger Technology

Industries Using Distributed Ledger Technology

- One of the more well-known distributed ledgers is **Hyperledger Fabric**.
- Some industries that have implemented DLT solutions include **aviation, education, healthcare, insurance, manufacturing, transportation, and utilities**.
- **Supply chains can benefit greatly from DLT**.
- **Many factors** make these chains **inefficient, inaccurate, and susceptible to corruption or losses**.
- **Fujitsu, a global data and information technology company**, has designed distributed ledger technology **to enhance supply chain transparency and fraud prevention** by securing and tracking data.
    - **Fujitsu's Rice Exchange** was created to trade rice, ensuring data regarding **sources, prices, insurance, shipping, and settlement** are recorded on the ledger.
    - **Anyone can look at any data** and find accurate information **regarding the entire process** because it cannot be changed.
    - All **data is entered and secured automatically** by the platform—it will eventually **provide tracking information for rice shipping containers** as they are shipped to their final destinations.
- **Other industries**: DLT has applications in **voting systems, intellectual property rights management, gaming** and much more.

Distributed Ledger Technology

Industries Using Distributed Ledger Technology

Healthcare

- Used to improve **patient data management**, streamline processes and **enhance security**.
- Medical **records can be securely stored and shared**, ensuring **data privacy and integrity**.
- Smart contracts can **automate insurance claims**, **reducing administrative burdens** and **improving efficiency**.
- Enables **secure and transparent clinical trials**, ensuring the integrity of data and **enhancing trust in the research process**.

Banking and finance

- One notable use case is the **implementation of smart contracts in trade finance**.
- Smart contracts facilitate the seamless execution and **settlement of trade transactions**, **reducing inefficiencies** and **eliminating the need for intermediaries**.
- DLT enables **faster cross-border payments**, enhances **Know Your Customer processes** and provides **secure digital identity solutions**.

Distributed Ledger Technology

Industries Using Distributed Ledger Technology

Supply chain management

- Distributed ledgers help organizations **track and verify the movement of goods**, ensuring authenticity and preventing fraud.
- Enables **real-time visibility into supply chain operations**, reduces paperwork and minimizes inefficiencies.
- For example, a distributed ledger solution can be used to **track the origin of goods, ensuring ethical sourcing and enhancing consumer trust**.

Real estate

- DLT has the potential to improve the real estate industry by **simplifying property transactions, reducing paperwork and enhancing security**.
- With the implementation of **smart contracts**, property transfers can be **automated, ensuring accurate and tamper-proof records of ownership**.
- Provide **transparent and auditable property registries**, reducing the risk of fraud and disputes and **removing the need of costly intermediaries**.

Distributed Ledger Technology

Uses of Distributed Ledger Technology

- **Record transactions**: DLT enables **secure, transparent, and decentralized transactions** without the need for a central authority. DLT can record **any type of transaction**, not just financially based ones.
- **Secure identities**: DLT can be used to **create a secure and tamper-proof digital identity** for individuals, as the technology can **provide a reliable way to verify identities** and **prevent identity theft**.
- **Collect votes**: DLT can be used to **create a secure and transparent voting system** that can **prevent voter fraud** and ensure the **integrity of the voting process**.
- **Enter contracts**: DLT allows for **smart contracts**, programs that **automatically execute or complete based on prevailing conditions**. **Example**: an **insurance claim may automatically release funds** once it has been processed and approved. This **limits errors**, and DLTs make it more **difficult for bad actors to alter information**.
- **Demonstrate ownership**: DLT can be **used to record property transactions**, creating a tamper-proof and transparent record of ownership and transfer of property. Though **there are some limitations on translating** real-world ownership of physical assets to a distributed ledger, the ledger may be **able to convey an unchangeable source of truth regarding ownership.**

Ethereum

- Ethereum is **a decentralized, open-source blockchain platform** that enables developers to build and deploy smart contracts and decentralized applications (dApps).
- Launched in 2015 by Vitalik Buterin & a team of co-founders, Ethereum introduced significant innovations to the blockchain space, most notably the concept of **smart contracts, which are self-executing contracts with the terms of agreement directly written into code**. It is widely recognized by:
  - **Investors** for its native cryptocurrency, ether (ETH).
  - **Developers** for its role in blockchain and decentralized finance application development.

Key Components

1. **Ethereum Virtual Machine (EVM):** The EVM is the runtime environment for smart contracts on Ethereum. It is a decentralized, globally distributed computer that processes the smart contracts. The EVM ensures that every smart contract and dApp operates as programmed, without any possibility of downtime, censorship, or third-party interference.
2. **Ether (ETH)**: Ether is the native cryptocurrency of the Ethereum platform. It is used primarily to pay for transaction fees and computational services on the Ethereum network. When users interact with smart contracts or perform transactions, they pay "gas" fees in ETH to incentivize network participants (miners or validators) to process their transactions.

Ethereum

3. **Smart Contracts:** Smart contracts are **self-executing contracts with the contract terms directly written into code**. These contracts automatically enforce the rules and obligations of an agreement, removing the need for intermediaries. For example, a smart contract could be programmed to release funds only when certain conditions are met, such as the delivery of goods.
4. **Decentralized Applications (dApps):** dApps are applications that run on a decentralized network like Ethereum, rather than being hosted on a centralized server. dApps leverage Ethereum's blockchain to operate autonomously, securely, and transparently. Examples of dApps include decentralized finance (DeFi) platforms, gaming applications, and social networks.
5. **Consensus Mechanism:**

- **Proof of Work (PoW)**: Initially, Ethereum used PoW, where miners competed to solve cryptographic puzzles to add new blocks to the blockchain. This process required significant computational power.
- **Proof of Stake (PoS)**: With the Ethereum 2.0 upgrade, Ethereum transitioned to PoS, a more energy-efficient consensus mechanism. In PoS, validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral.

Ethereum

Key Features:

- **Accessibility**: Ethereum is open to anyone. It's designed to be scalable, programmable, secure, and decentralized, enabling the creation of secured digital technologies.
- **Utility Token**: Ether (ETH) is primarily used to compensate for work supporting the blockchain. However, it can also be used to pay for goods and services where accepted.
- **Development Platform**: Ethereum is a blockchain-based platform known for its cryptocurrency, ether (ETH).
- **Secure Digital Ledgers**: The blockchain technology behind Ethereum allows for the creation and maintenance of secure public digital ledgers.
- **Comparison with Bitcoin**: While Ethereum shares some similarities with Bitcoin, it has different long-term goals and limitations.
- **Proof-of-Stake**: Ethereum uses a proof-of-stake mechanism for transaction validation.
- **Technological Foundation**: Ethereum underpins many new technological advancements based on blockchain.

Ethereum

Ethereum 2.0 (Eth2)

- Ethereum 2.0 is a major upgrade to the Ethereum network aimed at improving its scalability, security, and sustainability. It includes the **transition from PoW to PoS** and the introduction of shard chains, which allow the network to **process many transactions in parallel, significantly increasing its capacity**.

Use Cases

1. **Decentralized Finance (DeFi):** Ethereum is the foundation of the DeFi movement, which seeks to **create decentralized financial services, such as lending, borrowing, trading, and insurance, without relying on traditional financial institutions**. Examples include platforms like Uniswap (decentralized exchange), Aave (lending), and MakerDAO (stablecoin issuance).
2. **Non-Fungible Tokens (NFTs):** NFTs are unique digital assets **representing ownership of a specific item or piece of content, such as art, music, or virtual real estate**. Ethereum's blockchain is the most popular platform for creating and trading NFTs, thanks to its smart contract capabilities. Examples of NFT marketplaces include OpenSea and Rarible.
3. **Supply Chain Management:** Ethereum's blockchain can be used to create transparent, traceable supply chains. Smart contracts can automate processes such as tracking the movement of goods, verifying authenticity, and ensuring compliance with regulations.

Ethereum

4. **Governance:** Decentralized Autonomous Organizations (DAOs) use Ethereum's smart contracts to enable decentralized governance. Members of a DAO can vote on proposals and decisions are executed automatically based on the outcomes of these votes. DAOs are used for a variety of purposes, including managing investment funds and coordinating community projects.

Advantages of Ethereum

1. **Versatility:** Ethereum is a versatile platform that **supports a wide range of applications** beyond simple transactions.
2. **Developer Ecosystem:** Ethereum has a large and active developer community, which **continually contributes to the platform's growth and innovation**.
3. **Network Effects:** As one of the first and most widely used blockchain platforms, Ethereum **benefits from strong network effects, attracting more users, developers, and projects**.

Challenges

1. **Scalability:** Ethereum has faced scalability issues, with the network **becoming congested during periods of high demand, leading to slow transaction times and high gas fees**.
2. **Energy Consumption:** Under PoW, **Ethereum consumed a significant amount of energy**, similar to Bitcoin. The move to PoS with Ethereum 2.0 is designed to reduce energy consumption dramatically.
3. **Security and Complexity:** Smart contracts are powerful but can be complex to write and audit. Bugs or vulnerabilities in smart contracts can lead to significant losses.

Public and Private Blockchain

- **Distributed Ledger Technology (DLT)** refers to **decentralized and digitally managed ledgers** (databases maintained across numerous networked computers).
- **Information is validated** using a **consensus mechanism** and **stored in blocks**, with a **copy of the entire blockchain kept on each participating drive**.
- **Blockchain**, an application of DLT technology, serves as a **decentralized virtual transaction ledger**, enabling **transactions to be recorded and processed without intermediaries**.
- Due to their **decentralized nature**, DLT and blockchain technology facilitate **secure and confidential information sharing and transactions**.
- However, **not all blockchains are the same**. Each type serves a **specific purpose** and has its **unique advantages**. Blockchains can be broadly categorized into three groups:
  - Public Blockchains
  - Private Blockchains
  - Federated (or Consortium) Blockchains
- Additionally, there are mixed forms such as **public/private permissioned or public/private permissionless blockchains**.

Public and Private Blockchain

Public Blockchain vs. Private Blockchain

- Public and private blockchains are both **distributed peer-to-peer networks** where **each participant** keeps a **copy of the common ledger**.
- The distinction between them can be determined by answering three questions:
  - Who is allowed to **participate** in the network?
  - Who is allowed to **validate blockchain entries** according to the consensus mechanism?
  - Who is allowed to **keep the decentralized ledger**?

Public Blockchain

- A public blockchain is a completely **decentralized public ledger where everyone can participate**.
- Because anyone can participate, they generally **use cryptography in their programming to secure the ledger**, but the **transactions are publicly viewable**.
- Networks often include **incentive mechanisms to encourage participation**.
- Every network contributor **can read, write, and verify blockchain entries**.
- **Decision-making and validation** are performed through **consensus mechanisms** like "Proof of Work" or "Proof of Stake."
- **All participants** can **operate a node** within the network and **create tokens through mining**.

Public and Private Blockchain

- **Advantages**
  - **elimination of intermediaries** for transactions and register maintenance
  - allowing **direct transactions** between sender and recipient
  - **increased transparency** since all transaction data is public
- **Disadvantage**
  - **significant computing power** required for validation, especially with Proof of Work
  - **openness and transparency** of public blockchains can be a disadvantage for some **applications requiring private transactions**.
- **Examples**: Bitcoin and Ethereum

Private Blockchain

- A private blockchain is **managed by a network administrator** and is **accessible only to a specific group of permitted participants**.
- The network administrator **controls access** and is **aware of all participants**.
- **Transaction information** is **only viewable by involved parties**, and the **administrator** **can grant or deny certain privileges**, such as read or write permissions.

Public and Private Blockchain

- **Validation** is performed by the **network operator or a designated group** according to **predefined rules**.
- **Private blockchain** is **not formally decentralized** but is a **distributed ledger secured by cryptography**.
- **Advantage:**
  - **fast processing of transactions**
  - capable of **handling thousands per second due to the limited number of validators**.
- **Disadvantage**
  - private blockchains **contradict the core principle of decentralization**.
- **Examples**: Hyperledger and Ripple

Which Blockchain for Which Project?

- **Public blockchains** are ideal for **applications benefiting from an open system**. For example, **Ethereum combines public blockchain benefits with smart contracts**, suitable for uses in **real estate and healthcare**.
- **Private blockchains** are suitable for **internal company applications**, allowing businesses to **select participants** and **manage transaction content**. Companies can **assign specific rights** to participants, ensuring **controlled access** and **internal validation**.

Public and Private Blockchain

How Cryptocurrency Public Ledgers Work?

- A **cryptocurrency** is a **decentralized cryptographic token** that facilitates **value exchange** between network participants.
- The public ledger **maintains participants' identities, balances, and transactions** securely and **pseudo-anonymously** by automatically:
  - **Recording all transactions** and verifying that participants have the **tokens to transfer**.
  - **Securing the ledger** using **distributed consensus protocols** that compare data stored in each copy.
  - **Removing human involvement** from the auditing process, **reducing errors and corrupt** practices.
- Typically, a user **initiates a transfer** through an **interface or command**. The blockchain **verifies the sender's public and private keys**, **assigns a new private key to the recipient**, and **records the transaction** on the blockchain. **This transaction becomes part of an automatic verification process**.

Recording and Verification Process

- Blockchains operate differently, but generally, **transactions are recorded in files called blocks**.
- These blocks contain **several transactions, timestamps, and other data encrypted through algorithms**.
- Most blockchains **use hashing algorithms to send specific information from the block** and **include the** resulting hexadecimal number **(hash) in the next block.**

Public and Private Blockchain

- **Next block includes the previous block's hash, creating a secure chain** of information.
- This progressive hashing **builds a long chain of files** that **cannot be altered** as long as enough participants are involved.

Node Selection

- Most blockchains **allow one node to add a proposed block to the chain** through various mechanisms.
- Some **randomly select** specific nodes, while others use **voting or competitive hashing**.
- The method of block production is determined by the developers and the community.

Transactions

- Transactions are usually **automatically verified before a block is created**.
- **Users without** the appropriate amount of **tokens cannot make transactions**.
- Nodes **assemble blocks using various techniques**, often utilizing a **memory pool** (mem pool) that **stores unconfirmed transactions**.
- These transactions are typically **sorted by the fees users pay to the nodes** and processed accordingly.

Public and Private Blockchain

Consensus

- **Nodes place transactions** in the block they propose, **hash the required information**, and **broadcast it to the rest of the network**.
- Through various validation processes (consensus mechanisms), the network usually **agrees on the block's validity by comparing hashes**.
- **Any change** in a block's information **produces a different hash**, so identical hashes from the block's data indicate validity.
- Consensus mechanisms generally involve **validating nodes using the same block information** to generate a hash.
- If the **majority of the network generates hashes** that match the proposed block, it is **accepted**. Otherwise, the block is **rejected**, and the network moves to the next block.

Advantages of Cryptocurrency Public Ledgers

- **Transparency**: Transaction details can be **queried and verified by anyone** without disclosing personal information, making the system **more transparent** than traditional banking systems.
- **Security**: **Ledgers cannot be altered by anyone**, given enough network participation, removing the need for trust in financial institutions, which can be susceptible to corruption.

Public and Private Blockchain

Concerns About Cryptocurrency Public Ledgers

- **Scalability**: To enhance scalability, decentralization, or security, one often has to be sacrificed. The **increasing number of transactions enlarges the blockchain**, requiring more storage or innovative ways to **reduce the storage burden**.
- **Transaction Capacity**: Many blockchains **cannot match the speed of current payment systems**, leading to **increased transaction fees and processing times** as participation grows.
- **Security**: Large networks or **advanced techniques are required** for security. **Proof-of-work** blockchains need **significant participation** to avoid being taken over by entities with enough hashing power. **Proof-of-stake** blockchains **can centralize** by requiring large financial collateral. **Incentives are crucial** for maintaining participation and security.

Registries

- A registry is a **database or a system that keeps track of records**, often focused on **specific types of information or entities**.

Characteristics

- **Centralized or Decentralized**: Registries can be either centralized, managed by a single authority, or decentralized, managed by multiple participants.
- **Specific Purpose**: Typically designed to **track a specific type of data**, such as **property ownership, identity information, or membership records**.
- **Access Control**: Access to the registry **can be public, private, or restricted** to specific participants.

Examples

- **Land Registry**: **Tracks ownership and transactions** related to land and real estate.
- **Health Registry**: **Records patient information and medical history**.
- **Membership Registry**: **Maintains records of members** in an organization or association.

Use Cases

- **Government Services**: Property and land ownership records.
- **Healthcare**: Patient information and medical history.
- **Membership Organizations**: Tracking members and their status.

Ledgers

- A ledger is **a record-keeping system that logs transactions and balances**, traditionally used in accounting but now extended to digital and blockchain contexts.

Characteristics

- **Decentralized**: In blockchain, ledgers are often decentralized and **maintained by multiple participants in a network**.
- **General Purpose**: Can **track a wide range of transactions and records** beyond specific registries.
- **Immutable**: Transactions recorded in the ledger are **immutable**, meaning they **cannot be altered once added**.
- **Consensus Mechanisms**: In blockchain, **ledgers use consensus mechanisms** (e.g., Proof of Work, Proof of Stake) **to validate and secure transactions**.

Examples

- **Blockchain Ledgers**: **Bitcoin and Ethereum** ledgers record all transactions of their respective cryptocurrencies.
- **Financial Ledgers**: **Track debits and credits** in traditional and digital finance.
- **Supply Chain Ledgers**: **Record the movement of goods and materials** through a supply chain.

Use Cases

- **Cryptocurrencies**: **Recording transactions and ownership of digital assets**.
- **Financial Accounting**: Maintaining records of financial transactions and balances.
- **Supply Chain Management**: Tracking the provenance and movement of goods.

Registries and Ledgers

Key Differences

1. Scope

- Registries: Typically have a specific focus, such as property ownership or membership.
- Ledgers: Have a broader scope, tracking various types of transactions and records.

2. Structure

- Registries: Can be either centralized or decentralized, often with specific access controls.
- Ledgers: In the blockchain context, are typically decentralized and use consensus mechanisms for validation.

3. Immutability

- Registries: May allow updates and changes to records.
- Ledgers: Transactions are generally immutable once recorded.

4. Use Cases

- Registries: Used for specialized record-keeping needs.
- Ledgers: Used for general-purpose transaction recording and verification.

Registries and Ledgers

Integration in Blockchain

- **Blockchain Registries**: Some blockchain use the concept of registries within their ledgers. For example, a blockchain might have a land registry that tracks property transactions in an immutable ledger.
- **Blockchain Ledgers**: These serve as the backbone of cryptocurrency systems, recording every transaction and ensuring the integrity and security of the digital currency.

- While registries and ledgers both serve the **purpose of record-keeping**
  - registries are **more specialized** and can be either centralized or decentralized
  - ledgers, especially in the context of blockchain, are **decentralized, immutable**, and used for a **wide range of transaction tracking**.

Practitioner Perspective

Keyless Technologies

- Keyless technologies refer to systems that **enable secure authentication and access without the need for traditional keys or passwords**.
- Systems rely on **biometrics, behavioral data, and cryptographic methods** to verify identity and grant access.

Examples

- **Biometric Authentication**: Using fingerprints, facial recognition, or retina scans.
- **Behavioral Biometrics**: Analyzing patterns such as typing speed, mouse movements, or voice recognition.
- **Cryptographic Methods**: Utilizing **cryptographic keys stored on devices**, which are **unlocked through biometric or behavioral verification**.

Advantages

- **Enhanced Security**: **Reduced risk of theft or hacking** compared to traditional keys or passwords.
- **Convenience**: **Eliminates the need to remember** or manage multiple passwords or physical keys.
- **User Experience**: **Smoother and quicker access** to systems and services.

Challenges

- **Privacy Concerns**: **Handling and storing biometric data** must comply with privacy regulations.
- **Implementation Costs**: **Initial setup and integration** with existing systems can be **expensive**.
- **Reliability**: Ensuring that the technology works **accurately and consistently under different conditions**.

Practitioner Perspective

Transparency as a Strategic Risk

- Transparency in business practices involves **openly sharing information** about operations, decision-making processes, and performance.
- While transparency can **build trust and accountability**, it **also poses strategic risks**.

Risks

- **Competitive Disadvantage**: **Revealing too much information** can give **competitors insights** into strategies, operational processes, and financial performance.
- **Security Vulnerabilities**: Detailed disclosures **may expose sensitive information** that can be **exploited by malicious actors**.
- **Regulatory Scrutiny**: High transparency can attract increased attention from regulators, potentially **leading to more stringent oversight and compliance requirements**.
- **Market Reactions**: Transparent **reporting of challenges or negative performance** can **lead to adverse reactions** from investors and stakeholders, **impacting stock prices and reputation**.

Managing Risks

- **Balanced Disclosure**: **Carefully deciding what information to share** while protecting critical business secrets.
- **Robust Security Measures**: Ensuring that transparent practices **do not compromise data security**.
- **Proactive Communication**: **Effectively managing stakeholder expectations and responses** to disclosed information.

Practitioner Perspective

Transparency as a Strategic Asset

- Transparency can also be leveraged as a strategic asset, **enhancing a company's reputation, trustworthiness, and stakeholder relationships**.

Benefits

- **Trust Building**: **Open communication** fosters trust among customers, investors, employees, and partners.
- **Improved Relationships**: Transparency can lead to **stronger, more collaborative relationships** with stakeholders.
- **Enhanced Accountability**: **Clear visibility into operations and decision-making processes** promotes accountability and ethical behavior.
- **Attraction of Talent**: Transparent organizations are often **more attractive to potential employees** who value honesty and integrity.
- **Regulatory Compliance**: Proactive transparency can **simplify regulatory compliance and reduce the risk of legal issues**.

Strategies

- **Clear Communication**: **Regular and honest updates** about company performance, challenges, and future plans.
- **Stakeholder Engagement**: **Actively involving stakeholders** in discussions and decision-making processes.
- **Ethical Practices**: Ensuring that **all business practices align with stated values and principles**.
- **Sustainability Reporting**: Providing transparent **reports on environmental and social impact**.

Practitioner Perspective

Usage of Multiple IDs

- The use of multiple IDs refers to the **practice of using different identification methods or credentials** for various aspects of one's digital and physical life.

Types of IDs

- **Personal ID**: **Used for everyday activities** such as social media, online shopping, and personal communication.
- **Professional ID**: **Employed for work-related tasks**, accessing corporate networks, and professional interactions.
- **Financial ID**: Dedicated to **banking, investments, and financial transactions**.
- **Government ID**: Used for **accessing government services**, voting, and other civic responsibilities.

Benefits

- **Enhanced Security**: Using different IDs for different purposes **reduces the risk of a single breach** compromising all aspects of an individual's life.
- **Privacy Protection**: Separating identities **helps to maintain privacy** and control over personal information.
- **Specialized Access**: Different IDs can be tailored to **provide appropriate access and privileges** based on the context.

Practitioner Perspective

Challenges

- **Management Complexity**: Handling multiple IDs can be **cumbersome and confusing**.
- **Interoperability Issues**: Ensuring **that different ID systems work flawlessly** together.
- **User Experience**: **Balancing security with ease of use** to avoid frustrating users.

Solutions

- **Unified Identity Management**: Tools and platforms that help users **manage multiple IDs** efficiently.
- **Single Sign-On (SSO)**: Systems that allow users to **access multiple services with one set of credentials**, while still maintaining security through backend separation.
- **Blockchain-Based ID**: **Utilizing blockchain technology to create secure, decentralized identities** that can be used across various platforms.

Zero-knowledge proofs (ZKP)

- A zero-knowledge proof (ZKP) is a **method of proving the validity of a statement** **without revealing anything** other than the validity of the statement itself.
- **ZKP is a Proof system** with a **prover, a verifier, and a challenge** that gives users the ability to publicly share a proof of knowledge or ownership without revealing the details of it.
- **In cryptography**, zero-knowledge proofs let you convince me that **you know something, or have done something, without revealing to me** what that secret thing was.

A short history of ZKPs

- Zero-knowledge in cryptography first appeared in the 1985 paper "**The knowledge complexity of interactive proof systems [GMR85]**" by pioneers **Shafi Goldwasser, Silvio Micali, and Charles Rackoff**.

  "**A zero-knowledge protocol** is a method by which **one party (the prover) can prove to another party (the verifier) that something is true, without revealing any information apart from the fact that this specific statement is true.**"

- For example: "I know X, which I'm not going to tell you, but I can prove to you that this statement involving X is true."

Zero-knowledge proofs (ZKP)

- Zero-knowledge proofs **must satisfy three properties**:
  - **Completeness**: if the statement is **true**, an **honest verifier will be convinced by an honest prover**.
  - **Soundness**: if the statement is **false**, **no dishonest prover can convince the honest verifier**. The proof systems are truthful and **do not allow cheating**.
  - **Zero-Knowledge**: if the statement is **true**, **no verifier learns anything other than the fact** that the statement is true
- Zero-knowledge proofs have transitioned from being purely theoretical to having useful **real-life applications in blockchain, secure communications, electronic voting, access control and gaming**.

Zero-knowledge proofs (ZKP)

- Types of Zero Knowledge Proofs:
  - **Interactive zero-knowledge proofs** require the prover and verifier to **engage in a back-and-forth dialogue** in order to complete the proof.
  - **Non-interactive zero-knowledge proofs** are those in which the **prover sends a single message to the verifier**, who is then able to check the validity of the proof **without any further communication** from the prover.
  - **Statistical ZK-proofs** offer **computational soundness** with a small probability of error.
  - **Proof-of-knowledge (PoK)** is a subclass of ZK-proofs that shows that the **prover possesses specific knowledge related to the statement**.
  - **Proofs of shuffle and range** are used in **electronic voting and privacy-preserving transactions**.
  - **Sigma protocols** are a class of ZK-proofs that involve three steps: **commitment, challenge and response**.
  - **Bulletproofs** are designed to provide efficient **range proofs for large sets of values**.

Zero-knowledge proofs (ZKP)

Simple Example: Where's Wally?

- The simplest way to prove that **you have knowledge of something** without giving it away can be shown with the often-used "Where's Wally?" example.

  Initial Scenario

  - You and your friend are looking at an image where Wally is hidden.
  - You claim to know Wally's location, but your friend is skeptical.

  Proof Without Revealing Location

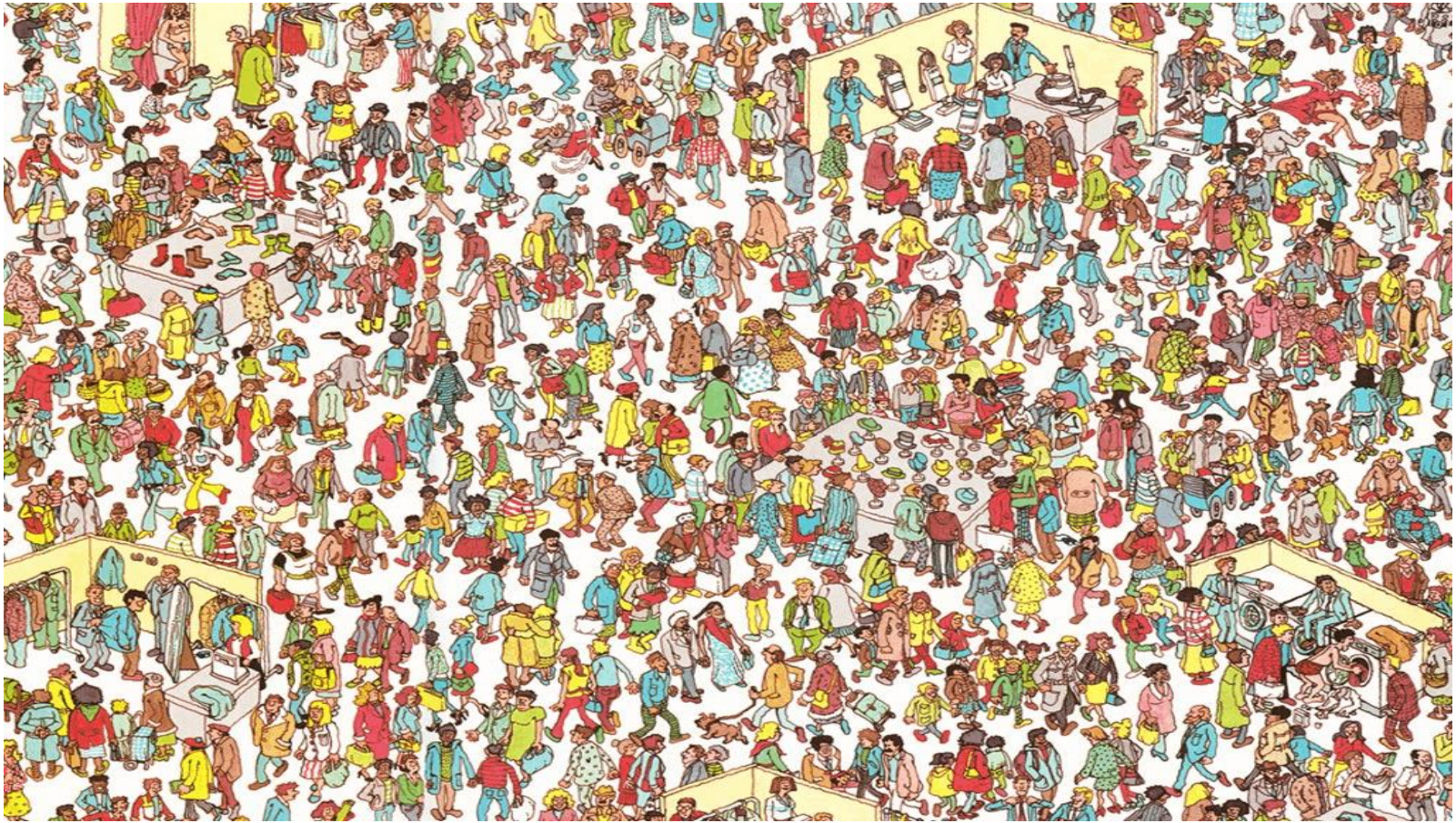
  - Take a large piece of paper and cut a small window (or hole) in it.
  - Cover the entire image with this piece of paper, aligning the hole precisely over Wally.
  - Show your friend the image through this cutout. Your friend will see Wally through the hole but won't know Wally's exact coordinates in the larger image.

  Result

  - **Your friend now has proof that you know where Wally is** because they can see Wally through the hole.
  - However, **your friend does not gain any information about Wally's exact location** within the image, thus **preserving the secrecy of Wally's coordinates**.

- This concept can be applied to cryptographic proofs where the **prover can convince the verifier that they know a secret (like a password or a specific piece of information) without revealing the secret itself**. This method ensures that the knowledge is proven without any leakage of the actual information.

Zero-knowledge proofs (ZKP)



Zero-knowledge proofs (ZKP)

Example 2: Proof of Membership (Locked Safe)

- Imagine **you are part of a secret group, and a stranger claims to also be a member**. To verify her claim without revealing any secret information, you can **use the group's locked safe as a test**.

Scenario:

- You have a **locked safe known only to the members of your group**.
- This safe can only be **opened with a secret combination code** that all true members know.

Steps to Verify Membership

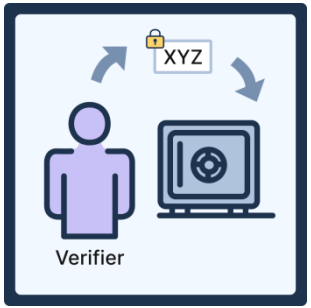
- **Write a Secret Message**: write a secret message that only you know and **place it inside the locked safe**.
- **Challenge the Stranger**: ask the stranger to **open the safe and retrieve the message** to prove her membership.
- **Verification**: If the stranger can open the safe and read back the secret message, **it proves that she knows the combination code**. Therefore, **she must be a trusted member of the group** since only members have access to the combination.

Result

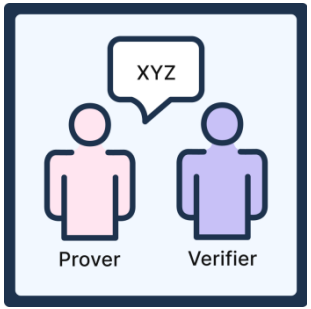
- V**erified her membership without revealing the combination code** or any other secret information.
- The stranger has **proven her claim by demonstrating knowledge of the secret code**

Zero-knowledge proofs (ZKP)

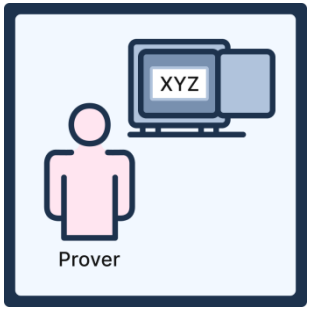
- Illustrates the concept of an **interactive zero-knowledge proof**. The prover (the stranger) can convince the verifier (you) that they possess certain knowledge (the combination code) without revealing the knowledge itself. The **locked safe serves as a challenge** that only someone with the correct knowledge can overcome, thereby **proving their identity or membership in the group** without exposing any secret information.



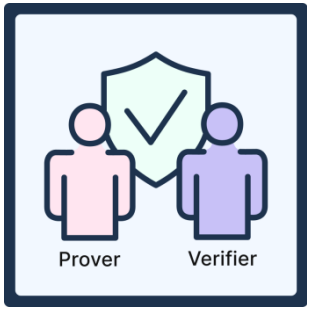
Verifier writes a secret message and put it in a locked safe



Prover returns the secret message to Verifier



Prover, who fulfils the requirements has knowledge of the combination code and opens the locked safe



Verifier is convinced that the prover really knows the combination code and can therefore be trusted

Zero-knowledge proofs (ZKP)

Example 3: Opaque Pricing

- Imagine **you and a competitor discover that you are both buying the same materials from the same supplier**. You want to **find out if you are paying the same price per kilogram**, but you can't trust each other enough to share your prices, and **you are contractually bound not to divulge this information**.

Steps to Compare Prices Secretly

- **Agree on Possible Prices:** Both of you agree that the **possible prices are 100, 200, 300, or 400** per kilogram.
- **Prepare Separate Pieces of Paper**: Each of you **prepare four pieces of paper, one for each possible price, and marks the paper that corresponds to the price you are paying**. For example, if you are paying 300, you mark the paper labeled "300" with a secret mark that only you know.
- **Exchange the Marked Papers**: Both of you **place your marked papers in an envelope and exchange** envelopes.
- **Check for a Match**: You each **look at the papers in the other's envelope** to see if any paper has a mark. If you find a paper with a mark, it means you are both paying the same price. If you don't find any marked paper, it means you are not paying the same price.

Zero-knowledge proofs (ZKP)

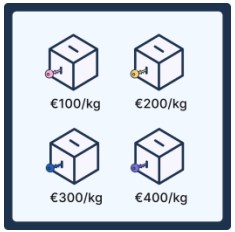
Result

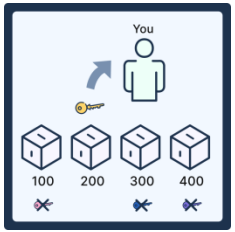
- If Prices Match
  - You both find a marked paper and know you are paying the same price per kilogram.
  - You don't learn the actual price, only that they match.
- If Prices Do Not Match
  - Neither of you finds a marked paper.
  - You both know your **prices are different**, but you **don't learn the specific price** the other is paying.

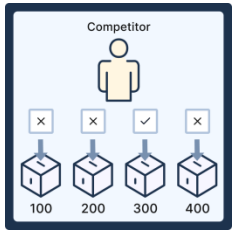
- **Confidentiality**: Neither party reveals their actual price.
- **Verification**: You can verify if prices are the same or different.
- **Trust:** This method works **without needing to trust each other** with sensitive information.

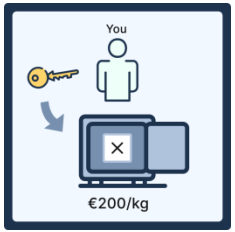
- This example demonstrates how zero-knowledge proofs can help in scenarios where **verifying information is necessary, but revealing the actual data is not an option**.

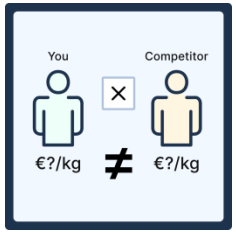
Zero-knowledge proofs (ZKP)











1. You and a competitor want to know if you are paying the same price without revealing how much each of you are paying.
2. We obtain 4 lockable lockboxes, each with a small slot that can take only a piece of paper. They are labelled 100, 200, 300, and 400 for the price per kilogram, and placed in a secure, private room.
3. You go into the room alone first. Since you are paying 200 per kilogram, you take the key from the lockbox that is labelled 200 and destroy the keys for the other boxes. You leave the room.
4. Your competitor goes into the room alone with 4 pieces of paper, 1 with a check, and 3 with crosses. Because your competitor is paying 300 per kilogram, they slide the paper with a check inside the lockbox that is labelled 300, and slide the papers with crosses into the other lockboxes. They leave the room.
5. After they leave, you can return with your key that can only open the lockbox labelled 200. You find a piece of paper with a cross on it, so now you know that your competitor is not paying the same amount as you.
6. Your competitor returns and sees that you have a piece of paper with a cross on it, so now they also know that you are not paying the same amount as them.

Text Book and Reference Books

Text Book

- Dhillon, V., Metcalf, D., and Hooper, M, Blockchain enabled applications, 2017, 1st Edition, CA: Apress, Berkeley.

Reference Books

- Diedrich, H., Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, 2016, 1st Edition, Wildfire publishing, Sydney.
- Wattenhofer, R. P, Distributed Ledger Technology: The Science of the Blockchain (Inverted Forest Publishing), 2017, 2nd Edition, Createspace Independent Pub, Scotts Valley, California, US.