

# **FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGIES (ITUA40181B)**

# Unit I

# Introduction to Blockchain

Dr. Priya M Shelke


[priya.shelke@viit.ac.in](mailto:priya.shelke@viit.ac.in)

# References

1. “Blockchain for Enterprise Application Developers” by Ambadas Tulajadas Choudhari, Arshad Sarfarz Ariff, Sham M R, Wiley Publications
2. Dr. Google

# Lecture 2

# What is blockchain?

- 
- A blockchain is a type of database.
  - Blockchain is a shared, immutable ledger for recording transactions, tracking assets and building trust.
  - Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.
  - A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

# Issues faced by current business world

Counterfeit Detection

---

Ethical sourcing

---

Quality Management

---

# Issues faced by current business world

Needing to reveal more

---

Reducing faith in central banks

---

Numerous other problems

---

# Challenges articulated





# Need of Blockchain

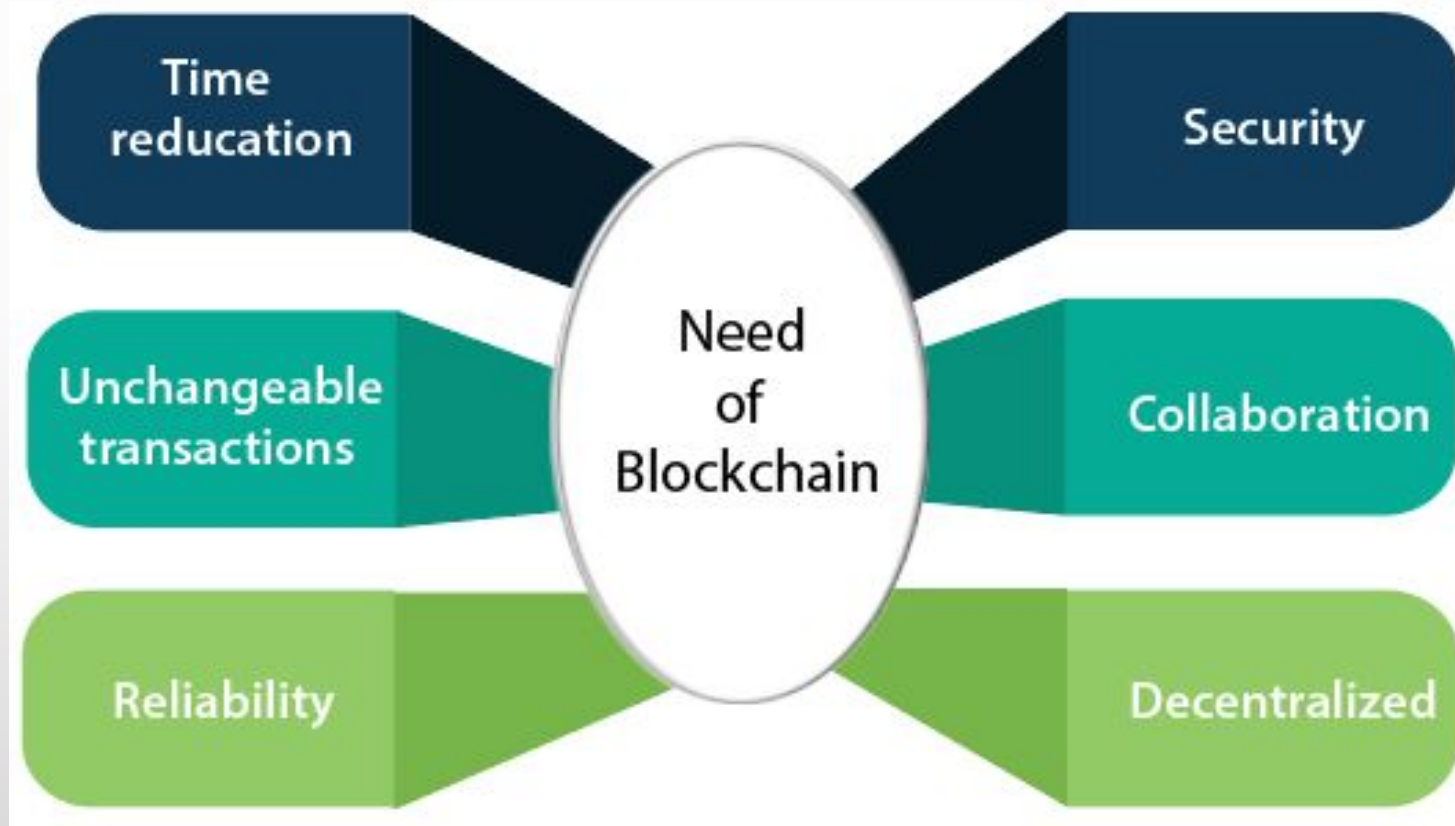
# We need blockchain because..

- Operations often waste effort on duplicate record keeping and third-party validations.
- Record-keeping systems can be vulnerable to fraud and cyberattacks.
- Limited transparency can slow data verification.
- And with the arrival of IoT, transaction volumes have exploded.
- All of this slows business, drains the bottom line — and means we need a better way.
- Enter blockchain.

# We will use blockchain for..

- **Greater trust** - With blockchain, as a member of a members-only network, you can rest assured that you are receiving accurate and timely data, and that your confidential blockchain records will be shared only with network members to whom you have specifically granted access.
- **Greater security** - Consensus on data accuracy is required from all network members, and all validated transactions are immutable because they are recorded permanently. No one, not even a system administrator, can delete a transaction.
- **More efficiencies** - With a distributed ledger that is shared among members of a network, time-wasting record reconciliations are eliminated. And to speed transactions, a set of rules — called a smart contract — can be stored on the blockchain and executed automatically.

# We will use blockchain for..



# History of Money



## EVOLUTION OF MONEY

VECTOR ILLUSTRATION







# History of Money

- Whether it's the dollar, pound, rouble, rupee, euro or yuan, physical or digital, our entire world is built on currency exchange. But from barter, banknote to bitcoin, the means of exchange have evolved significantly.
- **9000 B.C.: Barter begins**
- Bartering was first recorded in Egypt in 9000 B.C., when farmers would go to market to exchange cows for sheep, with grains passing through the hands of harvesters in exchange for oils.
- As barter developed along ancient trade routes, articles of exchange became more sophisticated. Egyptian papyrus, precious stones and chariots could now buy you exotic animals, skins and minerals from Africa and Asia. Although hieroglyphics show us trade was not hassle-free, with arguments over price a common occurrence.



# History of Money

- **600 B.C.: The world's first coin**
- Putting an end to such arguments, the first known currency was recorded in the ancient kingdom of Lydia (now part of Turkey). The world's [first coin](#) proudly displayed the head of a roaring lion on one side, with simple markings on the other.
- Irregular in shape and size, the coins were made from electrum – a naturally occurring mix of gold and silver – and minted according to weight, with the lowest denomination weighing a meager 0.15 grams. For that reason, coins were often weighed rather than counted.



# History of Money

- **1250 A.D.: International trade flourishes**
- The Florin was issued in Florence around 1250 A.D.; this gold coin kept a stable value for more than a century. It was accepted across Europe and its stability played an important role in encouraging international trade on the continent.
- **1290 A.D.: Banknotes are introduced**
- In the 13th century, travelers such as Marco Polo introduced the concept of banknotes to Europe from China, where paper currency had been in circulation since the eleventh century. But Europe was not ready for banknotes; it took another 300 years for them to take off, with Sweden the earliest adopter.

# History of Money

- **Middle Ages: Columbus destabilizes currency**
- The Black Death and the rise of counterfeit coins caused severe inflation. Prices returned to normal by the mid-1400s. But when Columbus established contact with the Americas later that century, a flood of precious metals on the European market destabilized currency for centuries.

# History of Money

- **1871: The start of e-money**
- Founded as the New York and Mississippi Valley Printing Telegraph Company in 1851, Western Union built a transcontinental telephone line across America in 1861. But after a party of Sioux warriors cut a large part of the wire to make bracelets, the pace of change slowed. When some of the bracelet-wearing warriors fell ill, a Sioux medicine man declared that the great spirit of the “talking wire” had sought revenge for its destruction. Western Union was left to connect the East and West Coast of America, with the first fund transfer via telegram taking place in 1871: the concept of e-money was born.

# History of Money

- **1950: The first credit card**
- Created in 1950 by Frank McNamara when he found himself without enough cash to pay for dinner, the Diners Club Card was the world's first credit card. Realizing his shortfall as he reached into his pocket to pay for dinner, McNamara was forced to call his wife and ask her to bring cash to the restaurant. He vowed this would be the last such supper.
- Today, more than half of all transactions in the U.S. and U.K. are put on plastic thanks to McNamara's embarrassing dinner.

# History of Money

- **1967: The invention of ATMs**
- Legend has it that John Shepherd-Barron devised the [world's first automatic teller machine](#) while taking a bath, which has historically proven to be the single best place to have an epiphany. Eureka! He pitched the idea to Barclays Bank, with the first model installed in Enfield, North London, in 1967.
- As plastic payment cards had not yet been invented, early ATMs used checks impregnated with carbon 14 – a radioactive substance – and paid out a maximum of £10 at a time. The expanding ATM network then paved the way for the rise of debit cards.
- In 2016, ATMs are now simply a (sometimes frustrating) fact of our daily lives. Convenience is a drug with the most bitter and exponential buildup of tolerance. As soon as you have even a smidgen, it becomes a standard requirement and you suddenly lose any idea of how people survived without it.

# History of Money

- **1983: Telephone banking**
- The Bank of Scotland offered Nottingham Building Society customers the first Internet banking service, named Homelink. Customers needed a television set and a telephone to send transfers and pay the bills, building the foundations for Internet banking as we know it.
- **1990: Internet banking**
- The beginning of the 90s marked the bloom of click-and-brick euphoria, wherein businesses and banks alike sought to gain the loyalty of their customers by expanding into the web. But this strategy proved trickier than previously thought, as it took over 10 years for Bank of America to acquire [2 million Internet banking users](#).

# History of Money

- **2005: Chip and pin**
- In 2005, retailers that had not yet signed up to chip and pin became liable for fraudulent transactions, as shoppers downed their pens and tapped in four-digit personal codes at pay points instead. Retailers were up in arms; at the time of the shift, around four in ten bank cards were yet to be upgraded to chip and pin technology.

# History of Money

- **2009: The birth of bitcoin and programmable money**
- After Satoshi Nakamoto posts a paper about the cryptocurrency on the Internet in 2008, the first bitcoins are issued in 2009 against a backdrop of the global financial crisis.
- In the early days, individuals used the [bitcointalk forums](#) to negotiate the value of the first bitcoin transactions, with one payment of 10,000 bitcoins used to indirectly buy two pepperoni pizzas from Papa John's in 2010 (based on today's bitcoin price, those pizzas cost more than \$4 million).
- Digital, decentralised, flexible and secure, the birth of programmable money gives us control of our currency. Who knows, someday our driverless car might be able to pay nearby vehicles to let us overtake when we're late for work. The possibilities are endless and exciting.



# History of Money

- **2014: Apple Pay**
- Continuing the fintech revolution, Apple Pay is released to the public through an iOS update in 2014. The mobile service lets consumers pay using the Apple device, removing the need for a wallet. And with nearly 40 percent of U.S. retailers now accepting contactless payments, it will soon be time to leave the plastic at home.

# History of Money

- **2016: Blockchain**
- Even though bitcoin is gaining more traction as time goes by, banks and businesses still seem more interested in the underlying blockchain technology for better or worse.
- However, [as of 2016](#), the Blockchain industry has already received over a billion dollars of investment and industry-wide recognition with over 35 blockchain projects announced by the world's foremost financial institutions including NASDAQ and NYSE.

# Lecture 3

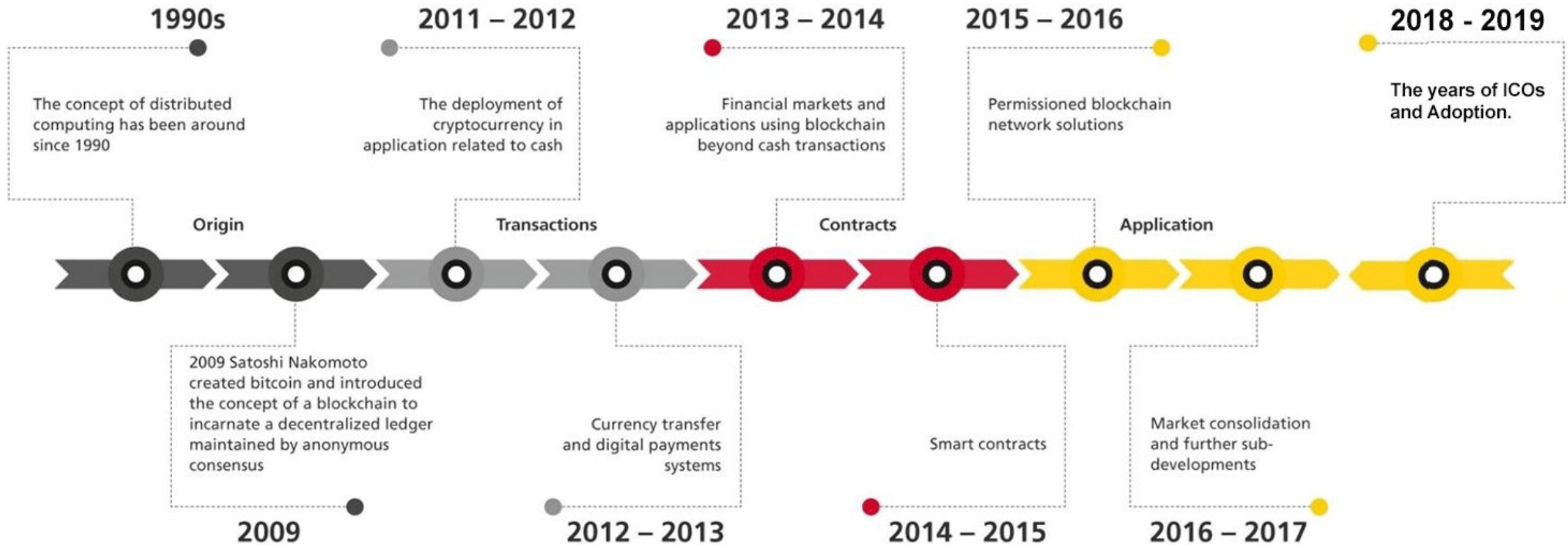
# History of Blockchain

# Fei / Rai Stone



- Humanity has been using distributed ledger around 1000 years ago.
- While blockchain, we know is the new concept, the idea of having a distributed ledger was discovered long back.
- On the Yap islands of Western Pacific Ocean, native islanders used stone currency named Fei or Rai.
- They used large stone disks, usually of 8-12 ft in diameter.
- These stones were very large, heavy and difficult to move. Rai were considered extremely valuable, but given their size, weight, and relative fragility, they were not typically moved after being placed in a specific location.
- If a rai were gifted or exchanged, the new owner(s) of a disk may not have lived in the close proximity to it. To ensure that ownership was known and indisputable, an oral ledger was used within communities to maintain transparency and security.
- According to the researchers, this oral ledger – told through stories shared by the Yapese and passed down over generations – helped the community to record and communicate changes in ownership of the rai, for things like wedding gifts, political enticements, or even paying ransom.
- Instead of moving the stones, people kept in mind what transaction had happened. It is said that even when stone is submerged or lost, people could still transact that stone based on a mental map they had.
- This mental map was in everyone's mind and everyone knows who owns it; it was like the distributed ledger and each had their own copy.

# BLOCKCHAIN HISTORY



# Evolution of Blockchain



- **Phase 1- Transactions**
- **Phase 2- Contracts**
- **Phase 3- Applications**

# Phase 1- Transactions

- **2008-2013: Blockchain 1.0: Bitcoin Emergence**
- Most people believe that Bitcoin and Blockchain are one and the same thing. However, that is not the case, as one is the underlying technology that powers most applications of which one of them is cryptocurrencies.
- Bitcoin came into being in 2008 as the first application of Blockchain technology. Satoshi Nakamoto in his whitepaper detailed it as an electronic peer-to-peer system. Nakamoto formed the genesis block, from which other blocks were mined, interconnected resulting in one of the largest chains of blocks carrying different pieces of information and transactions.
- Ever since Bitcoin, an application of blockchain, hit the airwaves, a number of applications have cropped all of which seek to leverage the principles and capabilities of the digital ledger technology. Consequently, blockchain history contains a long list of applications that have come into being with the evolution of the technology.



# Phase 2- Contracts

- **2013-2015: Blockchain 2.0: Ethereum Development**
- In a world where innovation is the order of the day, [Vitalik Buterin](#) is among a growing list of developers who felt Bitcoin had not yet reached there, when it came to leveraging the full capabilities of blockchain technology, as one of the first contributors to the Bitcoin codebase.
- Concerned by Bitcoin's limitations, Buterin started working on what he felt would be a malleable blockchain that can perform various functions in addition to being a peer-to-peer network. Ethereum was born out as a new public blockchain in 2013 with added functionalities compared to Bitcoin, a development that has turned out to be a pivotal moment in Blockchain history.

# Phase 2- Contracts

- **2013-2015: Blockchain 2.0: Ethereum Development**
- Buterin differentiated Ethereum from Bitcoin Blockchain by enabling a function that allows people to record other assets such as slogans as well as contracts. The new feature expanded Ethereum functionalities from being a cryptocurrency to being a platform for developing decentralized applications as well.
- Officially launched in 2015, Ethereum blockchain has evolved to become one of the biggest applications of blockchain technology given its ability to support [smart contracts](#) used to perform various functions. Ethereum blockchain platform has also succeeded in gathering an active developer community that has seen it establish a true ecosystem.
- Ethereum blockchain processes the most number of daily transactions thanks to its ability to support smart contracts and decentralized applications. Its market cap has also increased significantly in the cryptocurrency space.

# Phase 3- Applications

- **2018: Blockchain 3.0: the Future**
- Blockchain History and evolution does not stop with Ethereum and Bitcoin. In recent years, a number of projects have cropped up all leveraging blockchain technology capabilities. New projects have sought to address some of the deficiencies of Bitcoin and Ethereum in addition to coming up with new features leveraging blockchain capabilities.
- Some of the new blockchain applications include [NEO](#), billed as the first open-source, decentralized, and blockchain platform launched in China. Even though the country has banned cryptocurrencies, it remains active when it comes to blockchain innovations. NEO casts itself as the Chinese Ethereum having already received the backing of Alibaba CEO Jack Ma as it plots to have the same impact as Baidu in the country.

# Phase 3- Applications

- **2018: Blockchain 3.0: the Future**

- In the race to accelerate the development of the Internet of Things, some developers, so it fit, to leverage blockchain technology and in the process came up with IOTA. The cryptocurrency platform is optimized for the Internet of things ecosystem as it strives to provide zero transaction fees as well as unique verification processes. It also addresses some of the scalability issues associated with Blockchain 1.0 Bitcoin.
- In addition to IOTA and NEO, other second-generation blockchain platforms are also having a ripple effect in the sector. Monero Zcash and Dash blockchains came into being as a way of addressing some of the security and scalability issues associated with the early blockchain applications. Dubbed as privacy Altcoins, the three blockchain platform seek to provide high levels of privacy and security when it comes to transactions.

# Phase 3- Applications

- The blockchain history discussed above involves public blockchain networks, whereby anyone can access the contents of a network. However, with the evolution of technology, a number of companies have started adopting the technology internally as a way of enhancing operational efficiency.

# What is Blockchain?

- *Blockchain* is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
- An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).
- Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

# Blockchain simplified

- Blockchain seems complicated, and it definitely can be, but its core concept is really quite simple.
- A blockchain is a type of database.
- A database is a collection of information that is stored electronically on a computer system.
- Information, or data, in databases is typically structured in table format to allow for easier searching and filtering for specific information.
- What is the difference between someone using a spreadsheet to store information rather than a database?

# Blockchain simplified

- Spreadsheets are designed for one person, or a small group of people, to store and access limited amounts of information.
- In contrast, a database is designed to house significantly larger amounts of information that can be accessed, filtered, and manipulated quickly and easily by any number of users at once.
- Large databases achieve this by housing data on servers that are made of powerful computers.
- These servers can sometimes be built using hundreds or thousands of computers in order to have the computational power and storage capacity necessary for many users to access the database simultaneously.
- While a spreadsheet or database may be accessible to any number of people, it is often owned by a business and managed by an appointed individual that has complete control over how it works and the data within it.



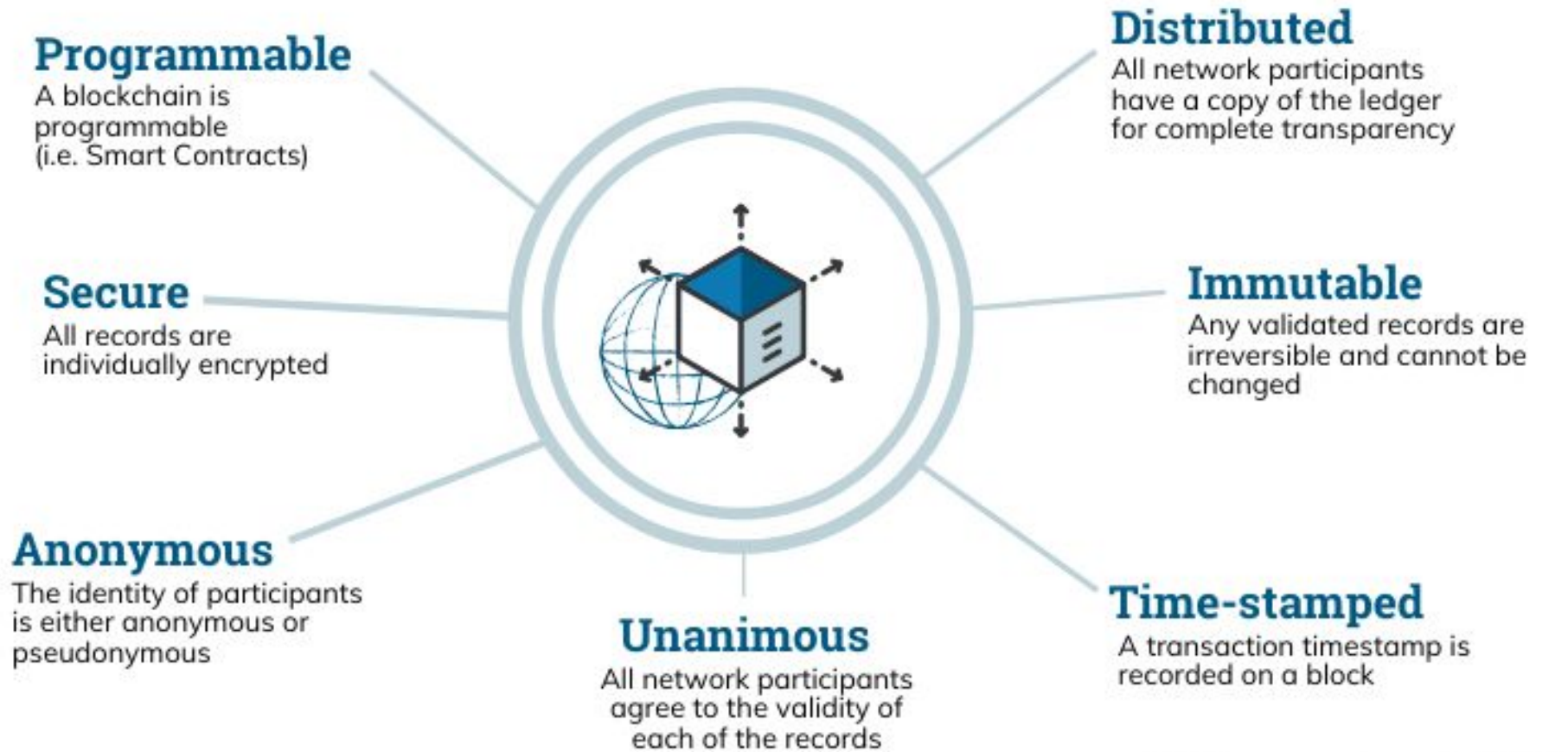
# So how does a blockchain differ from a database?

- **Storage Structure**

- One key difference between a typical database and a blockchain is the way the data is structured. A blockchain collects information together in groups, also known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are chained onto the previously filled block, forming a chain of data known as the “blockchain.” All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled.
- A database structures its data into tables whereas a blockchain, like its name implies, structures its data into chunks (blocks) that are chained together. This makes it so that all blockchains are databases but not all databases are blockchains. This system also inherently makes an irreversible timeline of data when implemented in a decentralized nature. When a block is filled it is set in stone and becomes a part of this timeline. Each block in the chain is given an exact timestamp when it is added to the chain.

- A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.
- Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.
- The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).
- Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a [hash](#).

# The Properties of Distributed Ledger Technology (DLT)



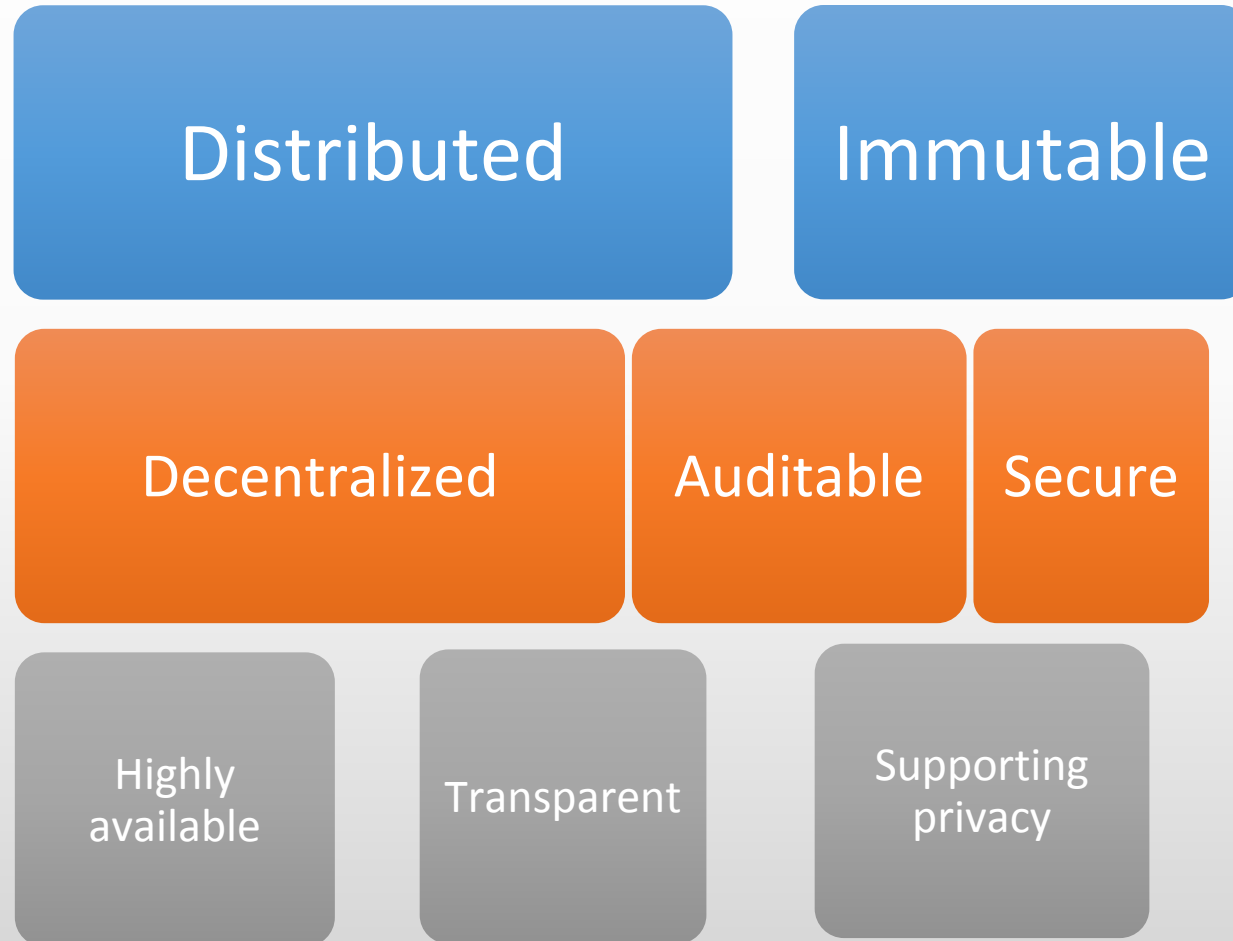
© Euromoney Learning 2020

# Key terms related to blockchain

- **Parties/participants**- Organizations or systems that participate in the network for reading or updating the data.
- **Open**-Protocols and details of working are not closed or proprietary. Blockchain's protocols are published and documented for everyone's consumption.
- **Distributed ledger**-A log of transactions that is same for all the nodes connected and synced with the network. In simple terms, every participant has the same copy of the log they all are maintaining together.
- **Peer-to-peer network**-A network in which participants are connected to each other than a central server or hub.
- **Permanent**-The ledger that is probabilistically impossible to change once it is agreed by participants.

# Lecture 4

# Blockchain characteristics



# Distributed

- The single consistent theme in the blockchain is collaboration. For collaboration to happen there has to be more than one system.
- Blockchain processes and stores data at multiple participants and so by nature it is distributed system.
- All network participants have access to the distributed ledger and its immutable record of transactions.
- With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.



# Immutable

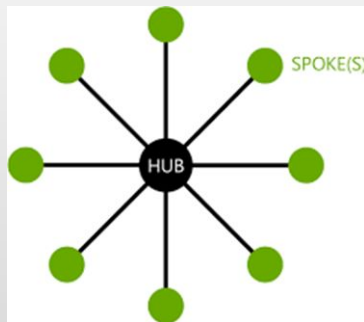
- As with existing databases, Blockchain retains data via transactions
- The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.
- The transaction is, immutable, or indelible
- Ensures that the next block in a blockchain is the one and only version of the truth
- Keeps powerful adversaries from derailing the system and successfully forking the chain
- Many Consensus mechanisms, each with pros and cons

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others....

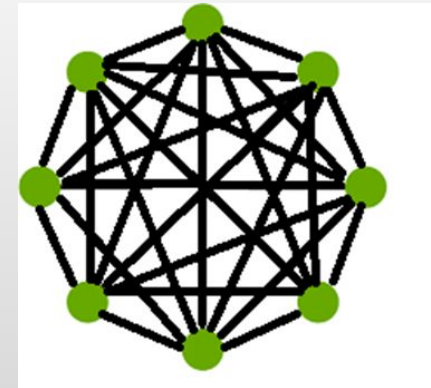
# Decentralized

- There is no single decision making authority in blockchain network; the decision to store or reject certain data is taken collectively by participants based on preset rules.
- This lack of central control makes blockchain decentralized. It helps blockchain maintain high availability.
- Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

Legacy Network  
Centralized DB



Blockchain Network  
Distributed Ledgers



# Auditable

- Blockchain does not only share the current state but the entire journey or log of how the state has been arrived.
- The log is available for each node to inquire.
- This makes activities happening on blockchain auditable.

# Secure

- Standard encryption practices
- Some Blockchains allow for “BYOE” (Bring Your Own Encryption)
- Only as good as the next hardware innovation
- All blocks are encrypted
- Some Blockchains are public, some are private
  - Public Blockchains are still encrypted, but are viewable to the public, e.g. <https://www.blocktrail.com/BTC>
  - Private Blockchains employ user rights for visibility, e.g.
    - Customer – Writes and views all data
    - Auditors – View all transactions
    - Supplier A – Writes and views Partner A data
    - Supplier B – Writes and views Partner B data

# Highly available

- Distributed and decentralized nature of blockchain network helps ensure consumers that the network always has a node available to serve the requests.
- This makes blockchain highly available

# Transparent

- In a blockchain, all the participants have a copy of ledger entries.
- Entries to the ledger are created by preset rules that are defined at network configuration.
- This sharing of data and logic encourages transparency in blockchain.

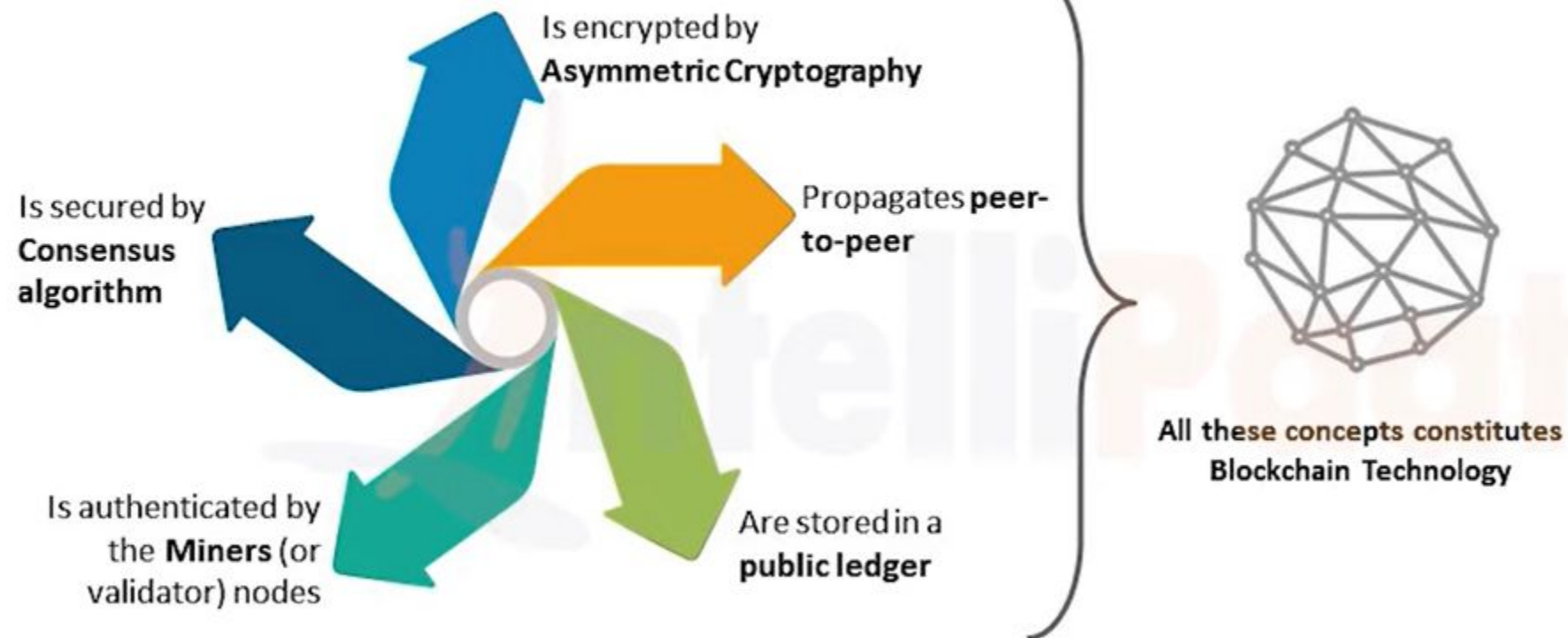


# Supporting privacy

- Blockchain does not identify individuals with identifiers that store personal information. Also, for transactions initiated by party A with party B, with cryptographic technologies used with blockchain, transactions can be initiated by party A without knowing any private information about party B.

# To sum up

In a Distributed system, transaction :



# Smart contracts

- Computer code
- Provides business logic layer prior to block submission

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

# Opportunities using blockchain

## Provenance

- Restaurant giving customers view of journey-a fish has taken to reach customer's plate
- Pharma companies detect counterfeit products
- Farm to cup journey of coffee

## Payments

- Funds transfer using cryptocurrency
- Triggering for parametric insurance
- Issuing loyalty rewards to customers based on type of activity and transactions

## Transaction ledger

- Storing health history of individuals supporting borderless healthcare
- Supporting Know Your Customer use cases for changes to demographics
- Partial ownership of high value assets such as real estate

## Identity

- E-consent management for end users
- Self Sovereign Identity based on zero knowledge proof
- End user controlled data sharing or data sell

# Why is there so much hype around blockchain technology?

- There have been many attempts to create digital money in the past, but they have always failed.
- The prevailing issue is trust. If someone creates a new currency called the X dollar, how can we trust that they won't give themselves a million X dollars, or steal your X dollars for themselves?
- Bitcoin was designed to solve this problem by using a specific type of database called a blockchain. Most normal databases, such as an SQL database, have someone in charge who can change the entries (e.g. giving themselves a million X dollars). Blockchain is different because nobody is in charge; it's run by the people who use it. What's more, bitcoins can't be faked, hacked or double spent – so people that own this money can trust that it has some value.

# Evolution of computer applications

## Local

- Run on powerful servers
- Can be accessed only within the local network
- Both data and functionality is controlled by the owner of the infrastructure

## Network

- Run on servers
- Can be accessed using a client over internal and external network
- Data is controlled by the owner of the infrastructure
- Functionality is controlled by the owner of the application

## Web

- Run on servers
- Can be accessed over the internet
- Data is controlled by the owner of the infrastructure
- Functionality is controlled by the users

# Application types

## Centralized

Data is owned and controlled by the server

Functionality is owned and controlled by the server

Make use of Hub or Spoke (Star) network model

## Decentralized

Data is not owned or controlled by the server or any single entity

Data is not owned or controlled by the server or any single entity

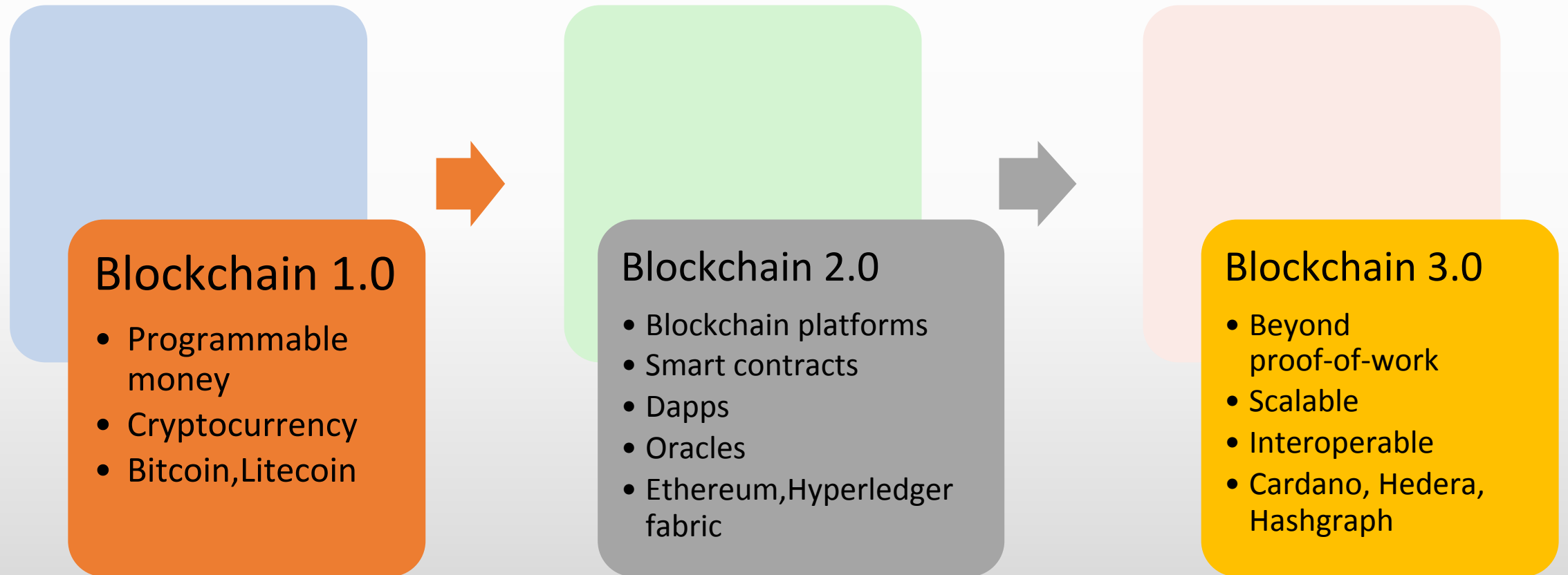
Make use of Peer-to-Peer network model



# Lecture 5

# Evolution of Blockchain

# Stages in blockchain evolution



# Blockchain 1.0

- Cryptocurrency is a central theme
- This programmable money is not managed by any central bank
- It challenged the status and indiscriminate behavior of central banks
- Initially aim was to support transactions and reward miners but as time progressed, it tries to improve transaction throughput by changing parameters that can improve speed at which blocks chain be chained.
- Alternate cryptocurrencies are known as altcoins

# Blockchain 1.0

Bitcoin- The first network that introduced cryptocurrency to the world was bitcoin. It introduced the phenomenon of storing, securing and performing transactions without the need for a bank or for that matter any centralized authority. Bitcoin has evolved and has been accepted in the market to an extent that it stands at market capitalization of 150 billion dollars, as of Sep 19.

Altcoin-Lite coin, launched after bitcoin, is also a cryptocurrency that focused on reducing the transaction time and enabling instant, near zero cost payments to anyone in the world with market capitalization of 3.4 billion. Ripple is a payment protocol that connects banks, payment providers, digital asset exchanges and corporates. Bytecoin, Namecoin and Dogecoin are few examples of cryptocurrencies that made their mark during the initial evolution period.

# Blockchain 2.0

- The key focus of Blockchain 2.0 was to take the engine used in cryptocurrencies that is blockchain and build platforms that would allow users to build business applications that provide transparency, immutability and other desired features.
- Blockchain networks also started becoming more of software platforms than a network infrastructure in this version.
- The software platform is a combination of software technologies that has prebuilt reusable or configurable components along with guidelines for development.
- This way, developers can concentrate on building business functionalities since low level, reusable requirements are already implemented by the platform.
- Similarly, blockchain platform comes bundled with a group of predefined functionalities such as storing and reading from ledger, consensus, validation, wallet, smart contracts etc.
- With smart contracts and decentralized applications, network in blockchain 2.0 provided a vision to implement decentralized autonomous organization.
- Organizations were able to raise millions through unregulated market through a method known as initial coin offering (ICO).
- The key traits that dominated this segment are smart contracts, Dapps and oracles.

# Blockchain 2.0

**Smart contracts**-It is a piece of custom written code implementing business logic. This smart contract can be deployed on all the nodes of the blockchain. A typical smart contract contains all the business rules for negotiating the terms of contract, verifying the contract followed by executing the agreed terms. This is one of the key features that made blockchain useful in many industries beyond cryptocurrencies. Smart contracts code respond to the events that get triggered based on transactions that execute.

**Decentralized applications**-It has its backend running on decentralized peer-to-peer network allowing users or front end to directly access the functionality available on the decentralized network. They have normally their own cryptographic token implemented on blockchain. E.g ETH for all applications implemented on Ethereum.

**Oracles**-Oracles provide mechanism to interact with outside world get reliable external data. Smart contracts do not communicate with oracles rather the oracles would call the methods of smart contracts with necessary inputs. The oracles may also streamline the input before sending to smart contracts. The oracles do not provide the final outcome.



# Blockchain 3.0

- Though Blockchain 2.0 provided enormous potential using blockchain platforms, it had some key issues that acted as showstoppers for mainstream adoption.
- Blockchain 3.0 platforms primarily focus on fixing these issues and making blockchain relevant and meaningful for various use cases.
  - Consensus
  - Scalability
  - Interoperability

# Consensus

- Consensus is a revolutionary mechanism introduced in bitcoin which provided a solution for finalizing a transaction.
- In blockchain 1.0 and 2.0, consensus mechanism used is proof-of-work. It refers to the class of algorithms that utilize expensive computation for solving a cryptographic puzzle.
- The time needed to solve the puzzle in bitcoin was approx. 10 min and in ethereum it is 14 secs.
- Overall a transaction can not be achieved in milliseconds, which is the requirement in most business applications.
- Blockchain 3.0 is working on a newer class of algorithms that would address this problem without compromising on the quality and security of POW algorithms.

# Consensus

- The Cardano platform is working on a proof-of-stake consensus known as Ouroboros, which they claim is the first secure peer reviewed consensus.
- POS refers to the class of algorithms that utilize the stake placed by participants by investing in cryptocurrency.
- Hedera Hashgraph is another platform. It uses asynchronous Byzantine fault tolerance (BFT).

# Scalability

- Scalability refers to the capability of the a system to handle increasing amount of work.
- Due to the delay in consensus mechanisms, blockchain networks are not able to handle more than a few transactions per second as compared to VISA network ,which can handle thousands of transactions per second.
- In bitcoin and ethereum, a transaction gets bogged during peak usage.
- Addressing consensus play major role in the resolution of the scalability problem.
- However, there are some other issues also. e.g each node in the network has to validate all the previous transactions before finalizing the new transaction.
- Blockchain 3.0 is focusing on the algorithms that would address this problem.

# Interoperability

- There is very little or no interoperability between various blockchain platforms.
- Many enterprises use different platforms, hence interoperability is crucial when enterprises try to integrate their functionalities for full scale automation.
- E.g. an insurance company selling policies on blockchain needs to integrate with payment providers to accept cryptocurrencies or with a bank for accepting fiat currencies.
- Blockchain 3.0 is trying to address interoperability by coming up with newer protocols that would allow different blockchain networks and platforms to interact with each other. It will require enormous efforts.
- As a first step, standardization is gradually introduced in the blockchain platforms.
- Blockchain platforms have started collaborating with each other and recommend adherence to each other's specifications and standards.

# Consortia

- One of the important use cases of blockchain is data sharing across organizations or enterprises. Since data is the heart of many businesses, sharing data needs proper cooperation between competing enterprises to come together for a common goal that would benefit all the stakeholders.
- However, every participant in the industry would not be ready to participate in such collaboration.
- Hence, it is a practical way to create a consortium of organizations willing to participate.
- The consortium will have representatives from each of the organizations involved and they will define the mission, drive the implementation and govern the blockchain network and standards to extract value out of blockchain technologies.
  - **Business focused consortium**
  - **Technology focused consortium**
  - **Hybrid consortium**

# Business focused consortium

- A consortium formed by organizations looking forward to making use of blockchain for business specific use cases is a business focused consortium.
- It analyses business cases for using blockchain while adhering to compliance and regulatory requirements.
- They generally forms focus groups or special interest groups to conduct detailed analysis, do proof of concepts and come with specifications as well as guidelines on how blockchain can benefit the business domain.
- Detailed analysis includes studying the impact of blockchain on regulations and can suggest amendments to the regulations, defining standards as well as best practices during implementation of blockchain.
- E.g B3i.

# Business focused consortium-examples

## B3i

- The Blockchain Insurance Industry Initiative (B3i) was formed in late 2016 as a collaboration of insurers and reinsurers to explore the potential of using Distributed Ledger Technologies within the industry for the benefit of all stakeholders in the value chain.

## HashHead Health

- Hashed Collective is a global community for healthcare organizations, consumers, entrepreneurs, developers — anyone looking to be a part of conversations at the intersection of blockchain and healthcare. It is an open, no-cost community where enthusiasts and newbies can engage with industry leaders and blockchain entrepreneurs across an array of interest areas.

## Digital trade chain

- It is created by a group of banks to harness the power of distributed ledger technology for commerce applications.

## PhUSE

- It promotes research and standardization in the area of blockchain for the pharma domain.



# Technology focused consortium

- A consortium focusing on creating generic reusable blockchain platforms is a technology focused consortium.
- It also includes representatives from various business organizations but usually has more participants from technology based organizations.
- This consortium also forms focus groups that study various technical challenges as well as business challenges in adopting blockchain. It also does various proof of concepts to understand these challenges.
- Business challenges include compliance and privacy whereas technology related challenges cover performance, scalability and inventions to emerging problems.
- Based on its analysis, it creates reusable blockchain tools and platforms.

# Technology focused consortium-example

## Hyperledger

- Hyperledger-A great example of technology based consortium, which aims to create advances across industry blockchain technologies.
- It has released various blockchain platforms,the most notable one being Hyperledger Fabric platform.
- It employs a modular architecture allowing plug and play of various components such as consensus and membership services.

## Enterprise Ethereum Alliance

- It is created to increase the adoption of ethereum in enterprises.

# Hybrid consortium

- It aims to focus on both technology and business challenges in the area of blockchain.
- This consortium does not identify or align themselves to a particular domain.
- It does have good technology standards and platform or technology ecosystem around its base offerings.

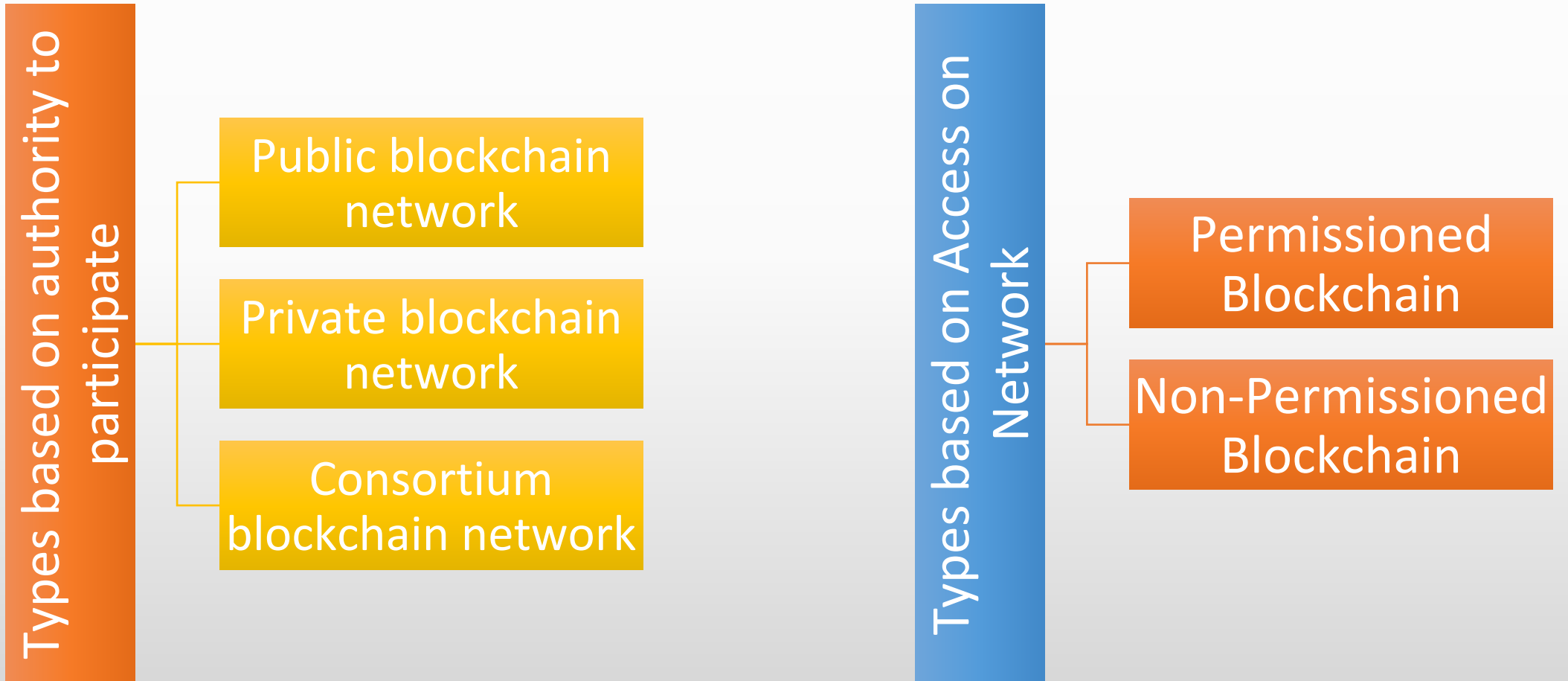
# Hybrid consortium-example

R3

- It has more than 300 firms as its members working together to build blockchain based application in industries such as finance, insurance, healthcare etc.
- R3 also have built their own blockchain platform known as Corda for business applications.

# Lecture 7

# Restrictions on sharing ledgers



# Types based on authority to participate

## Public blockchain network

- Anybody can join the network
- Anybody can participate in consensus protocol
- Uses incentive mechanism for consensus
- Anybody can read and write to the ledger
- Data is visible to all the participants

## Private blockchain network

- Limited to members of organization or entity
- Writes and consensus are controlled by organization or entity
- Members would require invitation to join the network
- High privacy
- High performance due to faster consensus

## Consortium blockchain network

- Group of parties create the network
- Super users hold the privilege to add or remove members
- Limited set of users are responsible for consensus
- Better privacy using permissions
- Better performance due to faster consensus

# Type based on access on network

## Permissioned blockchain

- Reads and writes are governed based on access permissions granted to the users.
- It falls in between public and private b. networks
- Super users hold the privilege to add or remove and grant access to members
- Limited set of users participate in consensus
- e.g Ripple

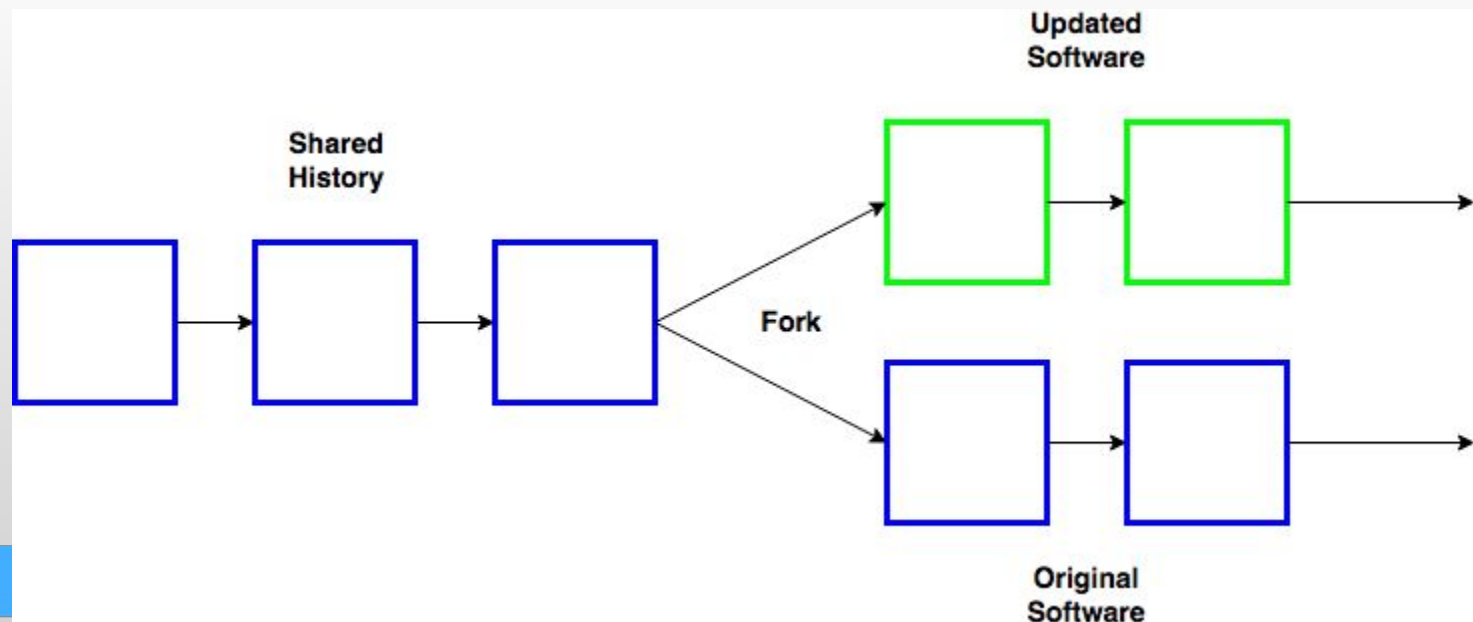
## Non-permissioned blockchain

- Inverse class of permissioned blockchain
- No single entity or group can control the network.
- It is governed by rules coded in to the blockchain network
- Anyone can join the network by running the blockchain software and can participate in consensus.
- e.g Bitcoin



# Forks

- Software fork occurs when two or more versions of software are developed separately out of single base version, creating two or more separate and independently managed source codes.
- This branching is known as forked-off version of software.



- Blockchain is decentralized application ,not controlled by single entity.
- This means that any update to the blockchain software needs agreement from all the parties running the network.
- In this case, changes must go along with the data.
- Essentially, the number of participants that agree to accept the change and take their data along decides the fate of the branch in a fork.
- That's why, in blockchain context fork refers to a software update to the blockchain software that I agreed upon by a set of participants from a network under consideration.
- This is relatively easy for private networks as organizations can take the decision to update the software.
- Even in consortium network, the software update can be performed relatively easily once all the super users or the founding members agreed to it.
- In case of public network, however it is a herculean task as getting agreement from all participants is difficult.
- A disagreement from some of the nodes shall result in the network running two versions of the software: one running with update and the other opting out of the update

# Forks

## Hard Fork

- It happens when software update to blockchain is not compatible with previous version.
- The update will result in the network splitting in two, with one group upgrading to a new version while the other group with participants without update.
- Hard fork occurs when majority of nodes agrees on the update while minority of nodes are against it.
- When network splits into two, there will be two copies of the same ledger at the time of split for each of the network.
- The nodes with new version, will have their own copy of ledger and the nodes without update will have existing copy of ledger.
- E.g Bitcoin cash allows larger blocks ,which they claim to process more transactions per second.

## Soft Fork

- It happens when software update to blockchain is compatible with previous version.
- The network will not be splitting in two, but the same network will have two versions of software.
- One group running to a new version while the other group with participants running old version.
- The new version blocks will be accepted by the nodes running old version whereas old version blocks will not be accepted by the nodes running new version.
- Bicoi's SegWit update is a soft fork that changes the way data is stored.

# Public Blockchain Environments

# Lecture 8



# Mainnet

- Mainnet refers to the live production network of a blockchain.
- The cryptocurrency used in the Mainnet possesses real value since all transactions are real transactions stored on the live ledger.
- Each and every transaction involves costs that are paid using the native currency of the blockchain network.
- Every member who solves the consensus is incentivized by payment in native coins.
- For private b.networks, Mainnet will be the production system on which real transactions would happen.
- Change management on Mainnet needs to be controlled. Changes to the mainnet need to analyse version compatibility and impact to decentralized applications that are connecting to the network.
- In case of soft fork, version compatibility of decentralized applications would be even more complicated if the user interface does not take care of version compatibility and availability of the data on the node that is connected.

# Testnet

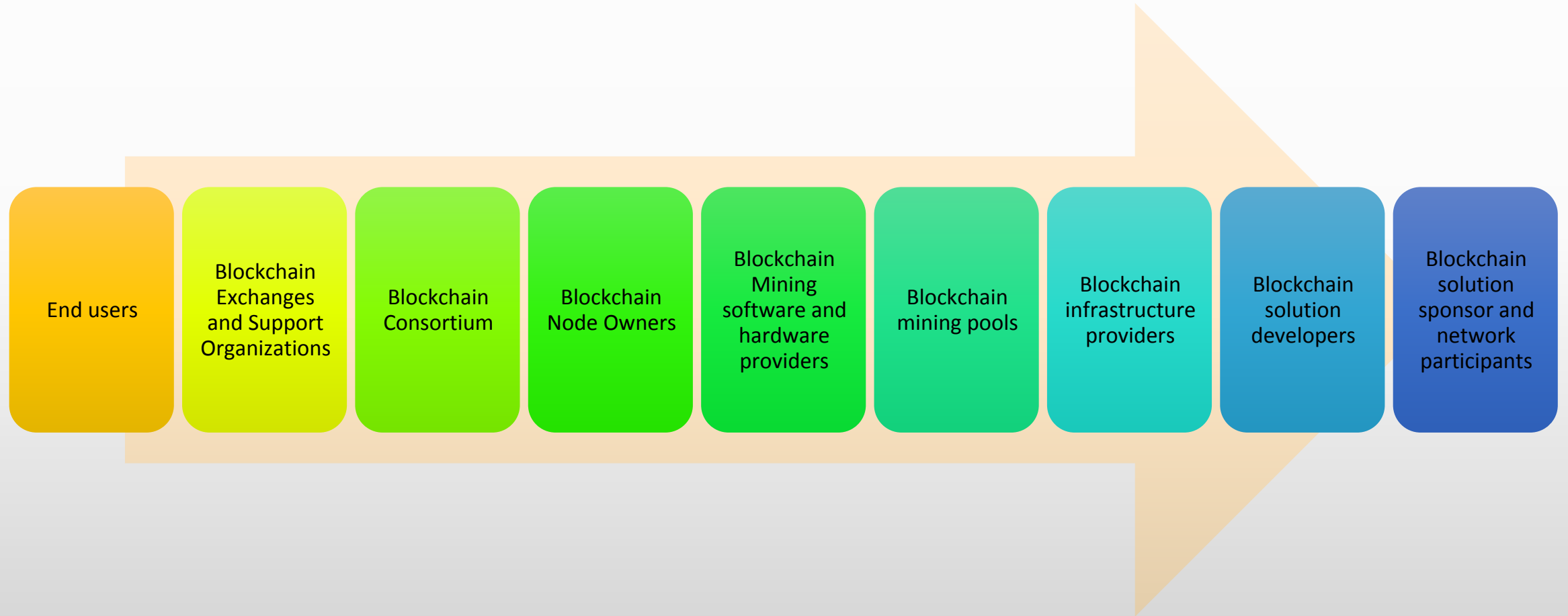
- Testnet refers to non production network of blockchain involving actual players performing activities similar to what they perform in production environment.
- It is network involving actual players for the purpose of testing.
- The cryptocurrency used in the test network does not possess any value since all the transactions are fake transactions. There is no cost involved in the transactions.
- No incentives are paid for the consensus.
- The size of the network might also be as large as production and data on Testnet can be regularly wiped off or cleaned based on the decision by all participants.
- Consensus mechanism in Testnet need not be same as that of production environment as aim is to get more testing done with least cost to providers.
- In private blockchain, it is integration testing environment where participants would validate their test cases before pushing changes to production.
- Decentralized applications also need to be connected to the Testnet to validate functionality and ensure there are no issues due to soft forking scenarios.
- Bitcoin Testnet uses proof-of-work for similar to the Mainnet.
- Ethereum has multiple Testnets viz Ropsten (proof-of-work), Rinkeby and Kovan (proof-of-authority).



# Local

- This refers to the development network.
- This can also be single node network created using simulator.
- This is required because in the process of development, changes are very frequent and might not always be working.
- It does not even make sense to even have network to perform transactions.
- A simulation is enough to validate if desired changes are working fine or not.
- A local network is simulation, not everything that works on local might work on Production or Testnet

# Types of players in blockchain ecosystem



# Players in market

# Bitcoin



Bitcoin is a digital currency created in January 2009.

It follows the ideas set out in a whitepaper by the mysterious and pseudonymous Satoshi Nakamoto. The identity of the person or persons who created the technology is still a mystery.

Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and, unlike government-issued currencies, it is operated by a decentralized authority.

Bitcoin is a type of cryptocurrency. There is no physical bitcoin, only balances kept on a public ledger that everyone has transparent access to.

All bitcoin transactions are verified by a massive amount of computing power.

Bitcoin is not issued or backed by any banks or governments, nor is an individual bitcoin valuable as a commodity.

Despite it not being legal tender in most parts of the world, bitcoin is very popular and has triggered the launch of hundreds of other cryptocurrencies, collectively referred to as altcoins.

Bitcoin is commonly abbreviated as "BTC."

Bitcoin's history as a store of value has been turbulent; it has gone through several cycles of boom and bust over its relatively short lifespan.

Bitcoin Core is the software that runs the blockchain network. Any person who uses to run a bitcoin node needs to download, install and run the Bitcoin Core software. It also contains a secure digital wallet that can be used to store, receive and send bitcoins.



# Multichain

Multichain is a platform that help to create private or consortium blockchain networks in a simple way.

It is based on blockchain protocol and software used in bitcoin.

Multichain allows permissions to be defined at the network level on who creates assets, sends assets and receives assets.

It allows mining to be performed without proof-of-work,using the concept of validations in a round robin fashion saving compute power.

Multichain provides a simple API and command line interface.

One of the key feature of Multichain is Asset.Any business entity can be represented as an asset in Multichain.

Assets can be created easily.Users can also send and receive assets.

Custom business rules can not be implemented on Multichain.

Any business rules surrounding creation and transfer of assets has to be coded outside the Multichain that is known as an off-chain code.



# Ethereum

Ethereum is a global decentralized, open-source blockchain with smart contract functionality.

Ether (ETH or  $\Xi$ ) is the native cryptocurrency of the platform.

After Bitcoin, it is the largest cryptocurrency by market capitalization.

Ethereum is the most actively used blockchain.

Ethereum was proposed in 2013 by programmer Vitalik Buterin.

In 2014, development was crowdfunded, and the network went live on 30 July 2015.

The platform allows developers to deploy permanent and immutable decentralized applications onto it, with which users can interact.

Ethereum represents generation 2.0 in blockchain evolution journey.

It provides a decentralized virtual machine, the Ethereum virtual machine which can execute scripts on an ethereum node.

These scripts are known as smart contracts.

Ethereum is not just blockchain network ,it is a distributing computing platform and operating system.

It allows users to create their own operations of any complexity they wish.



# Hyperledger

Hyperledger is an umbrella project of open source blockchains and related tools, started in December 2015 by the Linux Foundation, and has received contributions from IBM, Intel and SAP Ariba, to support the collaborative development of blockchain-based distributed ledgers.

Hyperledger is an open source community focused on developing a suite of stable frameworks, tools and libraries for enterprise-grade blockchain deployments.

It serves as a neutral home for various distributed ledger frameworks including Hyperledger Fabric, Sawtooth, Indy, as well as tools like Hyperledger Caliper and libraries like Hyperledger Ursa.

Hyperledger Fabric is intended as a foundation for developing applications or solutions with a modular architecture.

Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play.

Its modular and versatile design satisfies a broad range of industry use cases. It offers a unique approach to consensus that enables performance at scale while preserving privacy.



# R3 Corda

Corda is a permissioned blockchain platform that powers DLT applications that enable businesses to transact directly and in strict privacy with one another.

Though origin of Corda was driven by the requirements of financial industry ,it has wider applicability across different industries and use cases which require shared ledger.

Corda's design is different from a traditional blockchain system as it does not use a chain of blocks linked by hash to store the data.

However,it uses unspent transaction output(UTXO) model to structure and validate transactions.

The fundamental building block in Corda is known as "State Object", which represents a specific instance of a specific real world contract or a section of it. Transaction validation services are provided by special nodes on Corda network known as notaries.

Ledger visibility in Corda is controlled and confined to a group of concerned parties. In this way,it ensures strict privacy.

# Ethereum Quorum

Ethereum Quorum is a permissioned implementation of Ethereum, focusing on data privacy.

It is software fork of Ethereum and maintained in line with Ethereum releases.

On E.Q,private transactions and private contracts are implemented with encrypted message exchange.

As it is focused only on enterprise use cases, it offers alternatives consensus mechanism such as Raft consensus and Istanbul BFT.

In Ethereum,node permissions are supported using smart contracts,allowing only known parties to join the network.

With better choices of consensus protocol,it offers higher performance compared to Ethereum public blockchain.

# Other blockchain networks or platforms

**Ripple**-Ripple is a payment protocol for Real Time Gross Settlement (RTGS) system, currency exchange and remittance network. Ripple is a blockchain-based digital payment network and protocol with its own cryptocurrency, XRP.



**NEO**-NEO is a blockchain platform and cryptocurrency. It is also referred to as "Ethereum of China". It focuses on digital assets, digital identity and smart contracts to create a smart economy.

**Hyperledger Sawtooth**- Hyperledger Sawtooth is an enterprise blockchain platform for building distributed ledger applications and networks. The design philosophy targets keeping ledgers distributed and making smart contracts safe, particularly for enterprise use. It enables creation of both permissioned and non-permissioned networks.



- **Cardano**- It is also a blockchain platform and cryptocurrency. Cardano is developing a smart contract platform that seeks to deliver more advanced features than any other existing protocol. Their algorithm, Ouroboros, is claimed to be the first provably secure proof-of-stake algorithm that is peer reviewed by academics. Cardano can be classified as Blockchain 3.0 technology since its primary aim is to address the shortcomings of Blockchain 2.0 technologies.



- **Hedera Hashgraph** -It is a distributed ledger technology using graph, such as structure, for the network. It uses asynchronous Byzantine Fault Tolerance for consensus and gossip protocol for communication. It can be classified as Blockchain 3.0 technology.

# Thank you

# Lecture 8

# **FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGIES (ITUA40181B)**



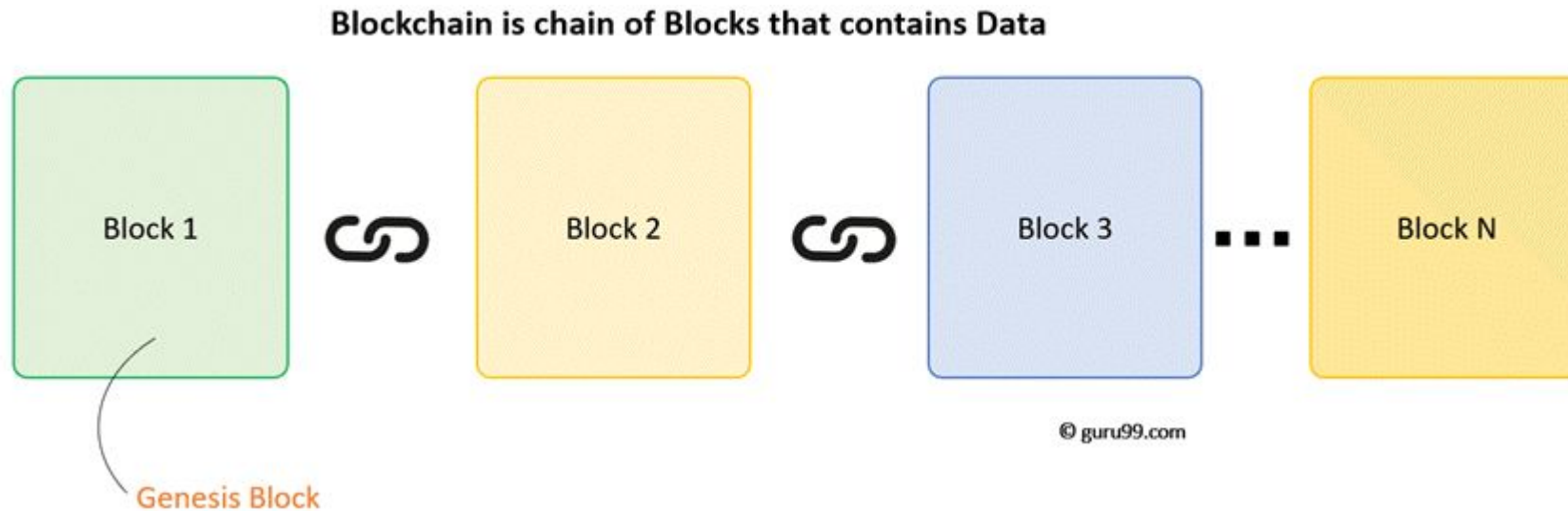
# Unit II

# Blockchain Concepts

Dr. Priya M Shelke

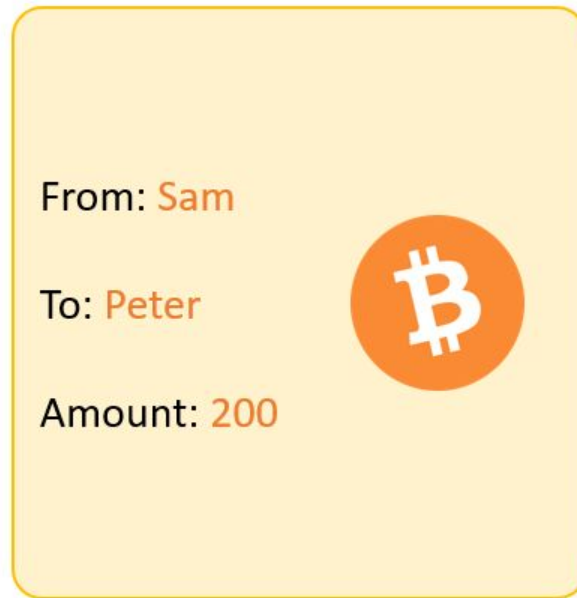
[priya.shelke@viit.ac.in](mailto:priya.shelke@viit.ac.in)

# Chaining of blocks



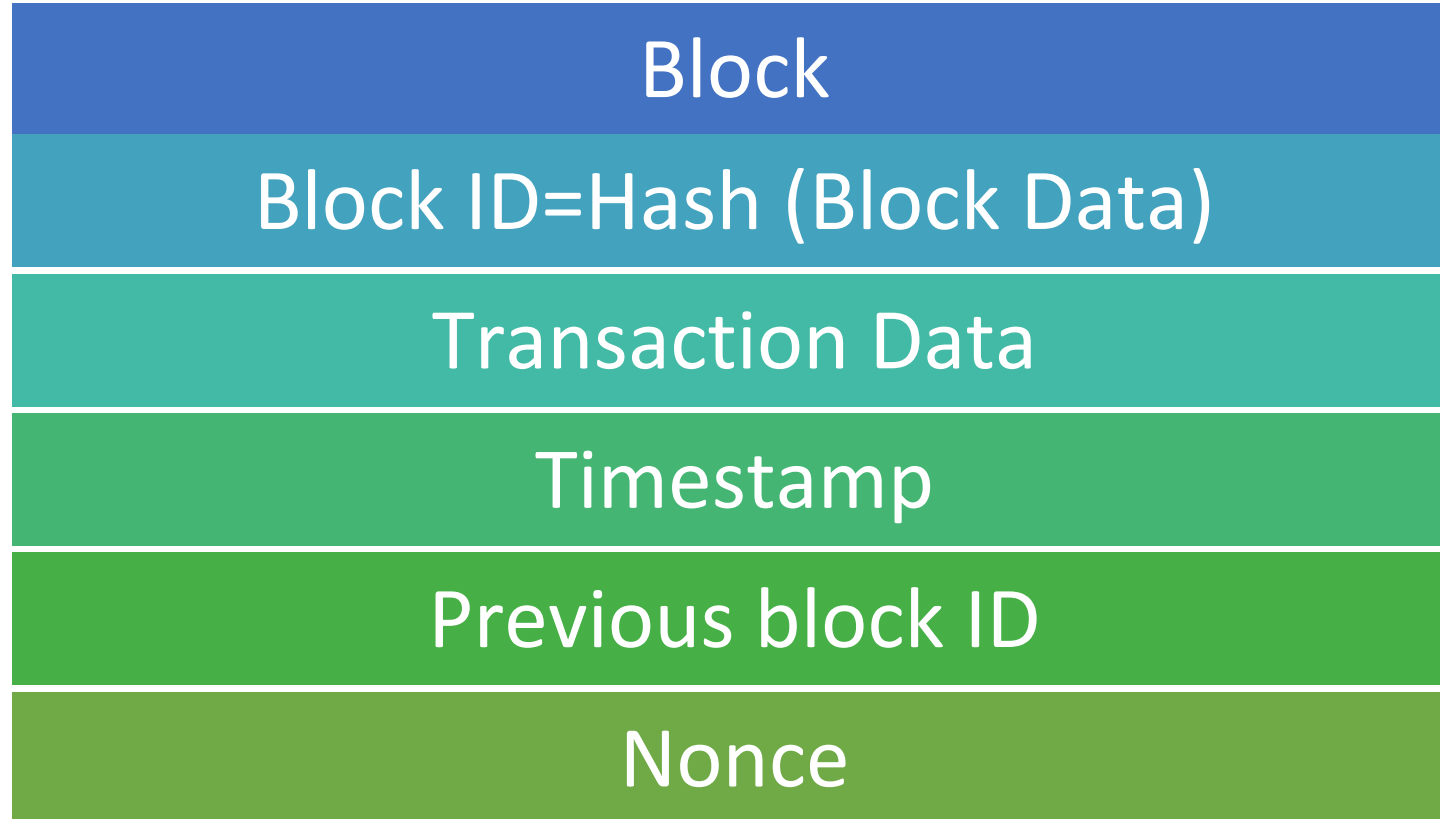
- A Blockchain is a chain of blocks which contain information.
- The data which is stored inside a block depends on the type of blockchain.
- The first block in the chain is called the **Genesis block**.
- Each new block in the chain is linked to the previous block.

For Example, A Bitcoin Block contains information about the Sender, Receiver, number of bitcoins to be transferred.



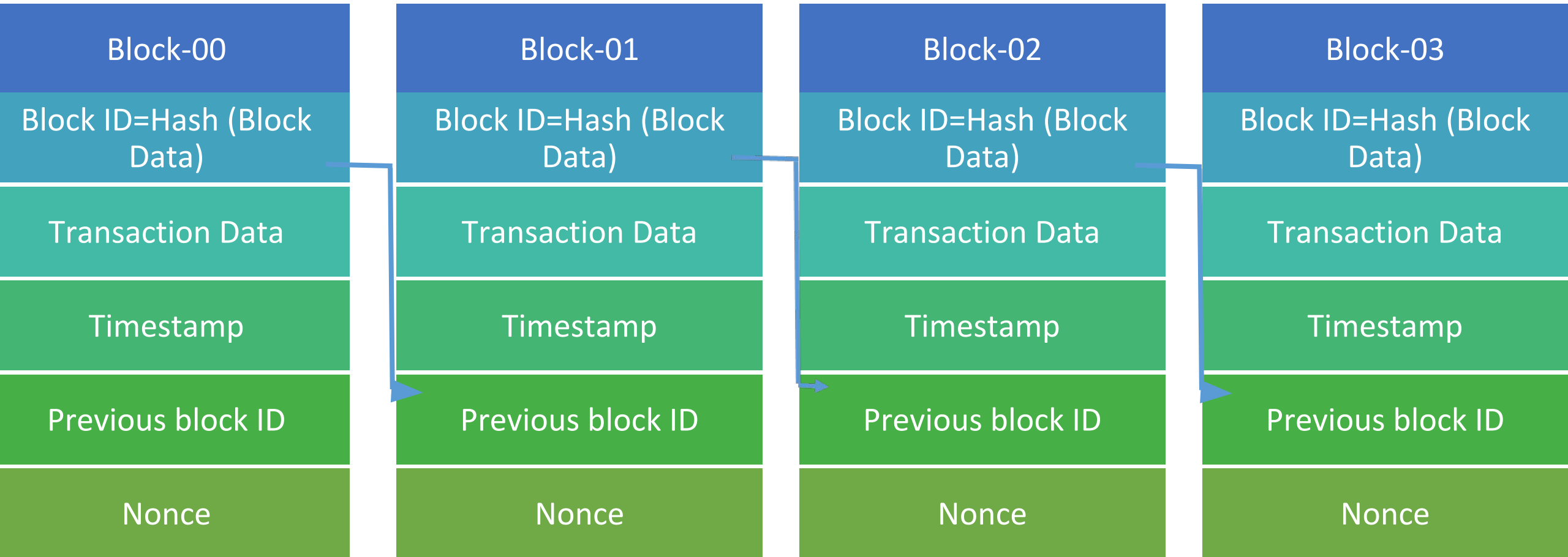
**Bitcoin Block Example**

# Sample structure of block



- Capture the data in fixed size sets (say 1 KB each), called as blocks.
- These blocks will get unique identifier based on the contents of data.
- These identifiers are created using hashing mechanism.
- Each block shall have four sections: identifier, data, timestamp and identifier of previous block.

# Chaining of blocks



# Chaining of blocks

- Logically, the first block does not contain the pointer since this one is the first in a chain.
- The 1<sup>st</sup> block has no predecessor. Hence, it does not contain hash of the previous block. It is called as *Genesis block*.
- In the beginning, we will create first block: BLOCK-01
- For this block, we will initialize “the identifier for the previous block” to zeros and the “timestamp” is set to current timestamp.
- This block does not get confirmed till it gets enough data i.e. (1 KB) that it can hold.

- Whenever 1 KB data is confirmed, we update “**data**” of BLOCK-01 to received data.
- The identifier of BLOCK-01 will be created using contents of block including “**data**”, “**timestamp**” and “**previous block identifier**” of BLOCK-01.
- As BLOCK -01 is confirmed, the second block (BLOCK-02) is created with “previous block identifier: set to identifier of BLOCK-01.
- The process keeps repeating many times as required.
- There is potentially going to be a final block within the blockchain database that has a pointer with no value.



# Modifying contents of block

- Suppose there is chain of 10 blocks.
- Some malicious user try to update contents of BLOCK-07->will impact on its identifier->require to change identifier of BLOCK-08->will need to change identifier of BLOCK 09 and 10 as well.
- So, deeper the block in the chain, more changes are required to update it.
- All this is possible because of the technique which creates identifiers based on contents of data.
- This technique is called as cryptographic hash functions.

# A MUST MUST MUST video to start

[https://youtu.be/\\_160oMzblY8](https://youtu.be/_160oMzblY8)

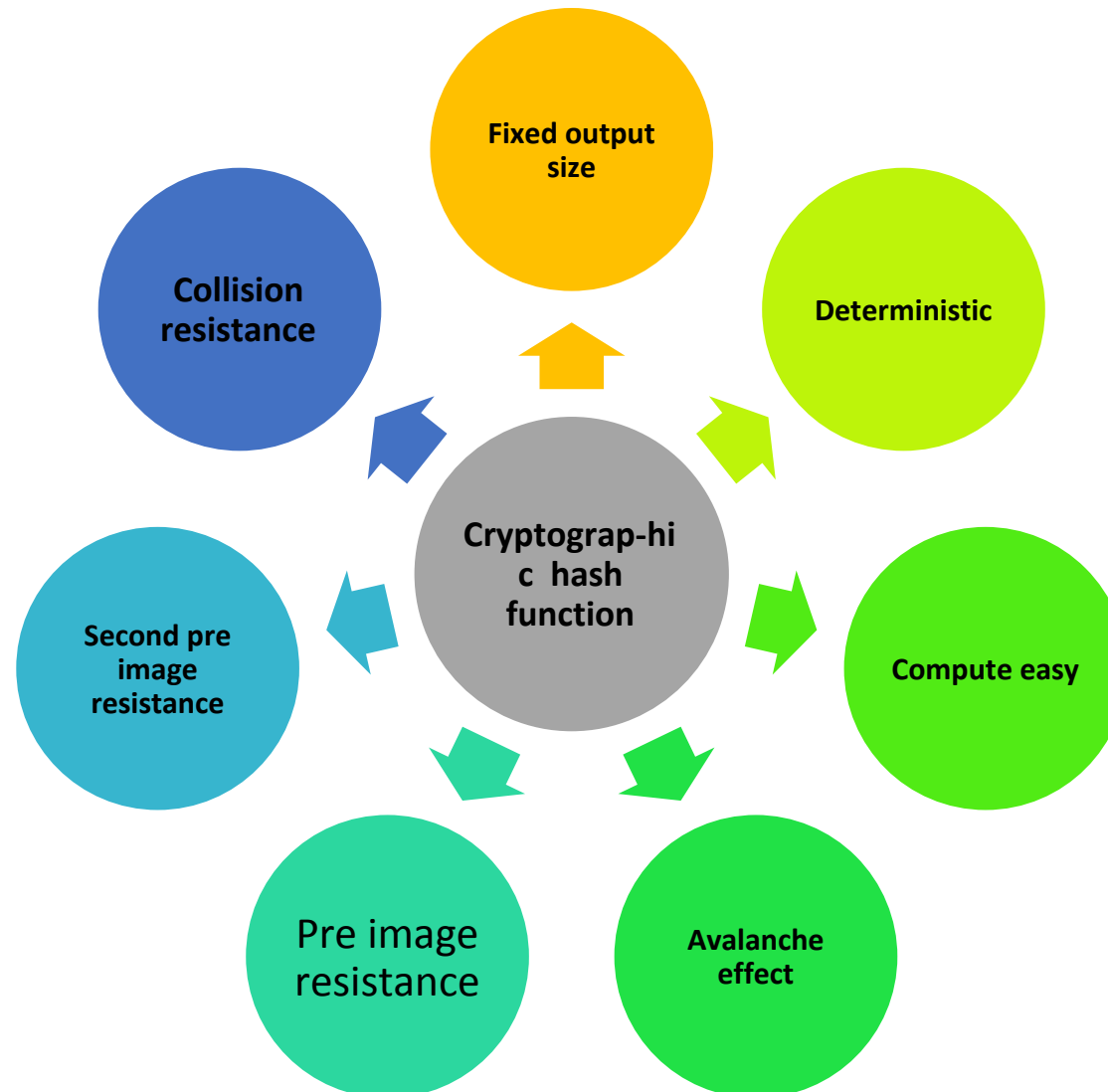
<https://andersbrownworth.com/blockchain/hash>

# Lecture 9

# Hashing

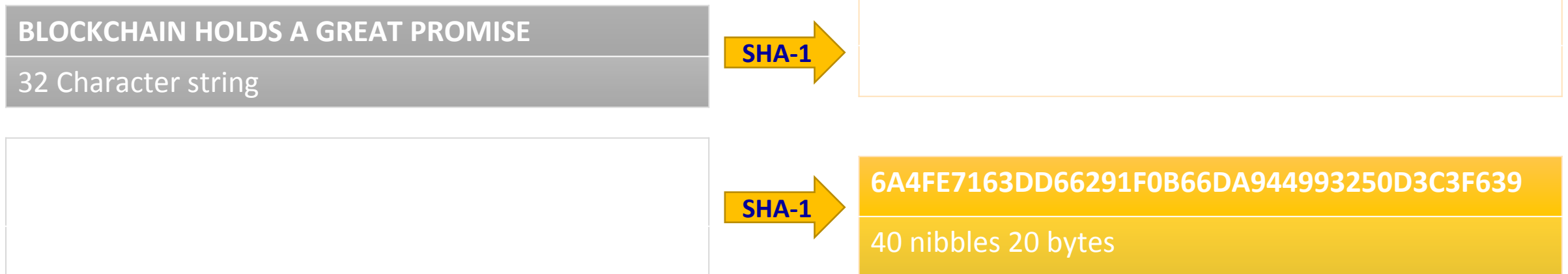
- Cryptographic hash functions are one of the key components of blockchain.
- These are part of building block functions which provides security, privacy and consensus on blockchain platform.
- These functions are mathematical algorithms used to perform required conversion.
- Different types of Cryptographic hash functions are available e.g Message Digest algorithm(MD5),Secure Hash algorithm(SHA)

# Characteristics of Cryptographic Hash Functions



# Fixed output size

- Usually, if the size of input changes then size of output changes. E.g Compression
- However, in case of cryptographic has functions, output string size remains same irrespective of input string size.  
(<https://passwordsgenerator.net/sha1-hash-generator>)



# Deterministic

- If the input is same, the output will always be same.
- If the function is applied on the same input any number of times, the resultant answer will always be same.
- If we apply SHA-1 on “BLOCKCHAIN HOLDS A GREAT PROMISE” any number of times, every time output generated will be “82F9EBDDEF5D1299B0B5C61DE0E245ACB2603160”.
- This characteristic helps them to be a very good candidate to be part of proof-of-work consensus mechanism in the blockchain.

# Compute easy

- Creating hash value is not compute intensive
- It does not need special hardware and it can be completed reasonably fast and not hold the end user.
- This has made these functions popular for signature validation ,consensus scenarios in the blockchain.



# Pre-image resistance

- It is not computationally easy to derive input for a given output.
- Say,  $H1 = \text{hash}(\text{string } 1)$
- If  $H1$  is given, it is not computationally easy or practical to find string1.
- It is possible but just not easy.
- The stronger the algorithm, the more computation it may require and it may have better pre-image resistance.
- Next, even if two characteristics are similar to pre image resistance, they are not the same.
- It is not easy to find source based on data, making these a kind of one way function.

# Second pre-image resistance

- It is possible to find another input that can give the same hash value as a given input.
- Let's take String1 and  $H1 = \text{hash}(\text{String1})$ .
- It is not easy to find another string (String2) such that  $\text{String1} \neq \text{String2}$  and  $H1 = \text{hash}(\text{String2})$ .
- To be clear, it may not be impossible, but it will definitely not be easy to do so.

# Collision Resistance

- It is not easy to derive two input values for a hash function such that output value is same for both the input values.
- If two input maps to same output, then the function is said to have collision.
- It is not that collision might not exist, just that probability of occurring that collision is very less.
- So, hash algorithm, HASH1 is said to not have collision resistance if you can find two strings, say S1 and S2, such that  $S1 \neq S2$  and  $HASH1(S1) = HASH1(S2)$ .
- It is different than second pre-image resistance as here only hash function is given while input strings can be anything.
- In second pre image resistance one input string is given.

# Avalanche Effect

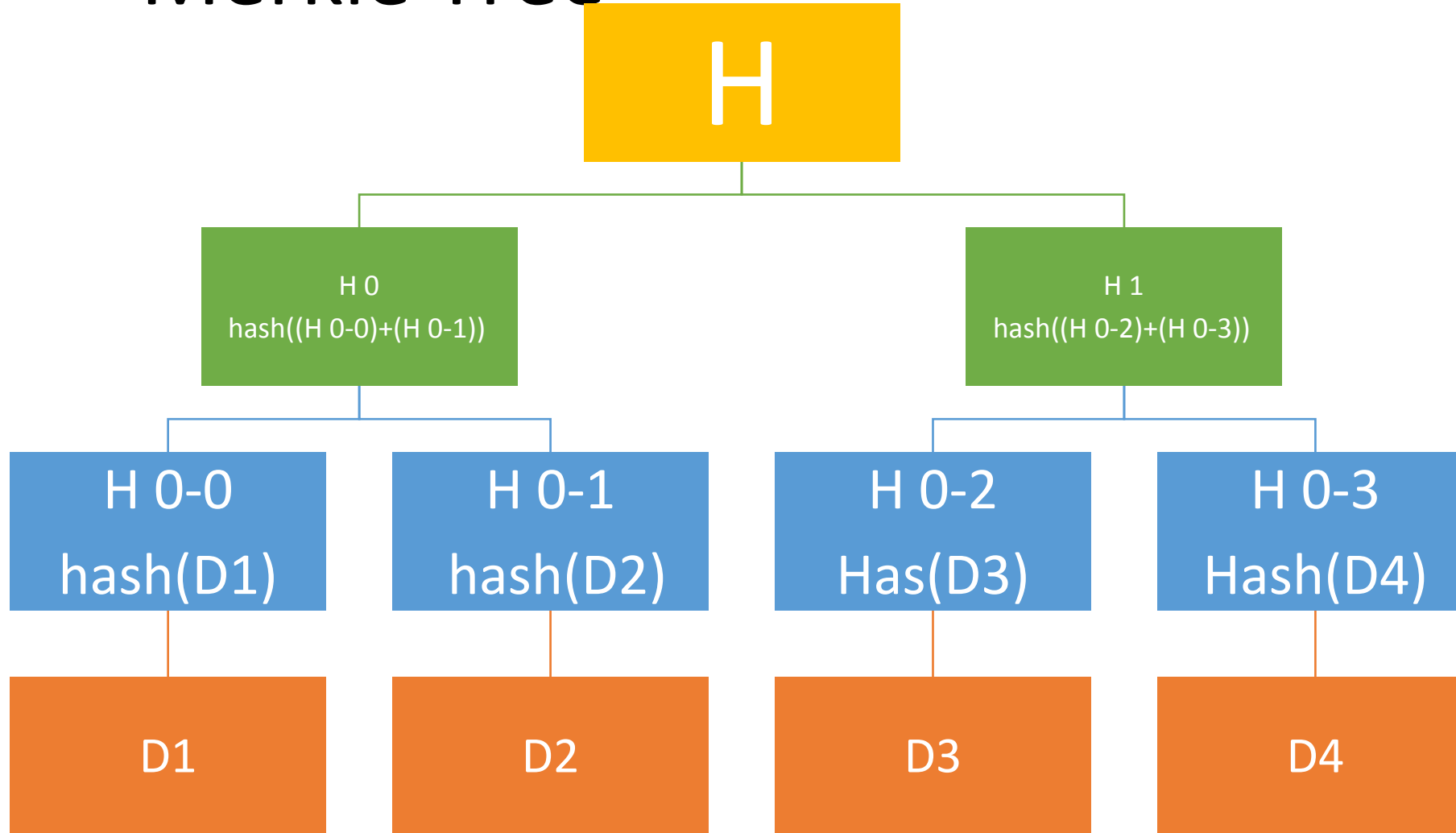
- A small change in input causes a large change in output.



# Variants of SHA

- All these characteristics make hashing a very useful tool in the context of blockchain.
- SHA is one of the ways in which hashing can be done.
- There are various variants of SHA such as SHA128,SHA256,SHA512 etc.
- Here,the numbers at the end inform about the length of output.

# Merkle Tree



- Merkle tree also known as hash tree is a data structure used for data verification and synchronization. It is a tree data structure where each non-leaf node is a hash of its child nodes.
- All the leaf nodes are at the same depth and are as far left as possible.
- It maintains data integrity and uses hash functions for this purpose.

# Merkle Tree

- An input of data broken up into blocks labeled Data1 though Data4.
- Each of these blocks are hashed using some hash function.
- Then each pair of nodes are recursively hashed until we reach the root node, which is a hash of all nodes below it.
- The hash value at root node is called as Merkle root.
- When data is shared among parties, data is shared from regular channels and Merkle root is shared from secure channel.
- Intermediate hash values can be shared from regular or secure channels as per requirements.

# Merkle Tree

- As data starts coming in, the verifier can verify if the data is valid by calculating hash value of the data received and comparing it with the hash value received for that segment.
- After the entire document is received, merkle root is compared with the merkle root received from the secure source.
- If data is manipulated in the process, then value of hash and in turn merkle root would change and this will help verifier to check authenticity of the data.



# Lecture 10

# Consensus

- Decision making process where participants agree on decisions of creating a block is called as *consensus*.
- There are various types of consensus mechanisms in the blockchain world.
- Consensus mechanisms try to lay out various principles for seeking the agreement.

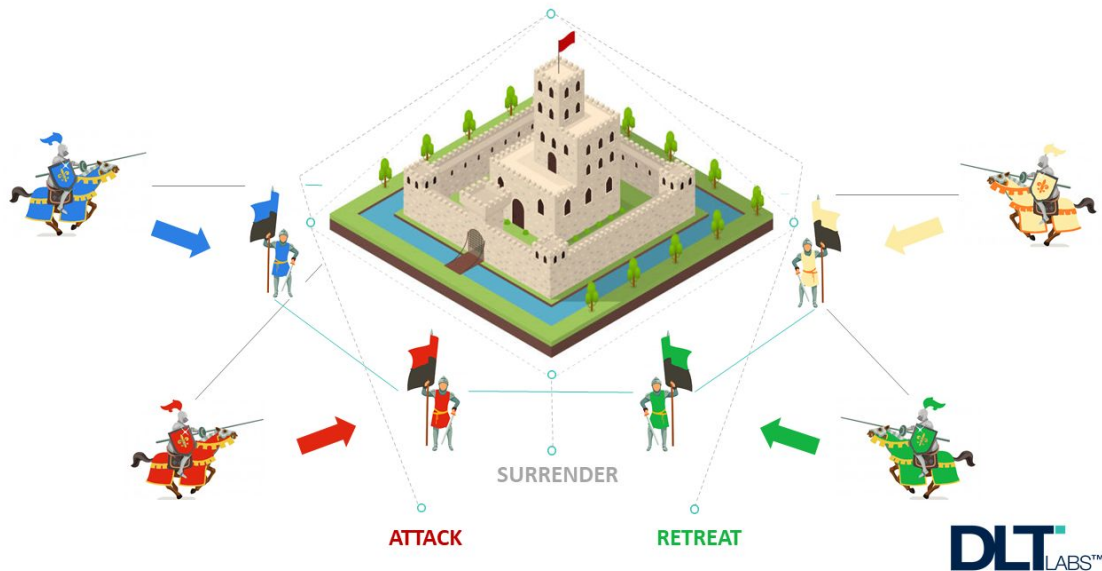
# The consensus problem

- An algorithm achieves consensus if it satisfies the following conditions:
  - Agreement- All non faulty nodes decide on the **same** output value
  - Termination- All non faulty nodes eventually decide on the **some** output value

# History of consensus mechanism

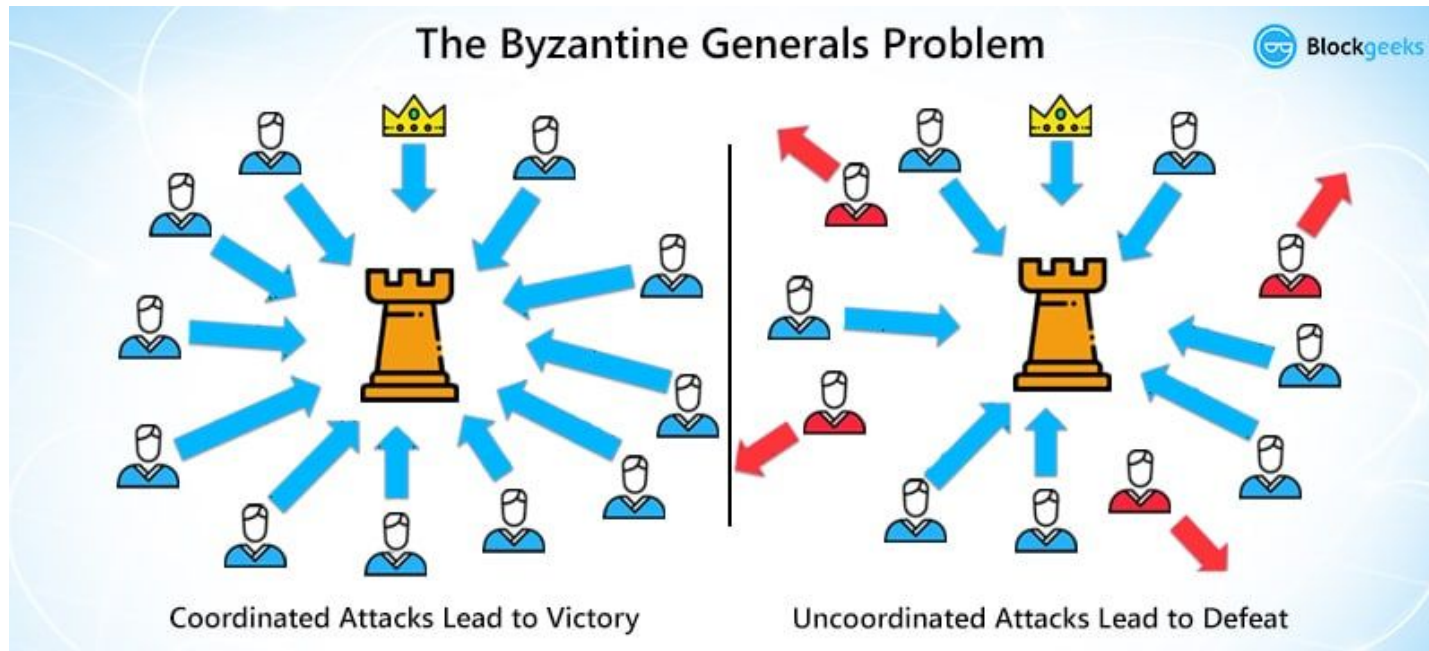
# Byzantine General's Problem

- BGP discusses a scenario where participants must decide in unison to agree or disagree on a decision, otherwise it is collective loss for all participants.
- The challenge to be solved is that if one or more participants are not reliable, then how can entire collection protect themselves from catastrophic failure.



- Four generals plan to attack a fort.
- The conquest requires all generals to put on concerted effort.
- If all attack together, all will win; If all stay put, status quo is maintained.
- If all do not attack together, then only those who attacked will be killed.
- Generals can send messages through messengers but messengers might get hacked or might get changed.

# Byzantine General's Problem



- Every morning, the challenge is for all four generals to decide if they shall attack or stay put.
- The decision by individuals may lead to win or catastrophe.
- Some solutions to the problem can be appointing one of the generals as “ultimate command of campaign”, coding messages and decision being taken based on messages from all assuming not all messages would be hacked etc.
- No solution exists if less than or equal to  $\frac{2}{3}$  of generals are loyal

- In blockchain, the problem is very similar since the participants are peers.
- The decision in case of blockchain is to agree on data to be inserted and create the block of data.

# Proof-of-Work

- Proof of Work(PoW) is the original consensus algorithm in a blockchain network.
- The algorithm is used to confirm the transaction and creates a new block to the chain.
- The idea here is participants should do certain activity and show a proof that it is done.
- All other participants shall be able to verify easily that the activity has happened based on some evidence.
- In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network.
- The process of competing against each other is called mining.
- As soon as miners successfully created a valid block, he gets rewarded.
- The most famous application of Proof of Work(PoW) is Bitcoin.

# Proof-of-Work

- Producing proof of work can be a random process with low probability.
- When a block is to be created, all participants are required to add extra bytes to the block called *nonce* such that hash of the block begins with zeros.
- As it is not easy to predict what hash of block would be, it requires a lot of trial and error to identify hash value that satisfies additional condition such as three leading zeros.
- At the same time, as cryptographic hash functions are compute easy, it is very easy to validate if hash of a given string is valid as everyone can run hash function for the confirmation.
- With all participants already having data, if all are given nonce value by the puzzle solver, all can validate independently that the puzzle solver has really done “work” to get a valid nonce.
- The main working principle of proof of work is a mathematical puzzle which can easily prove the solution.
- Proof of work can be implemented in a blockchain by the Hashcash proof of work system.



# Contd...

- In the puzzle game, bitcoin software creates a challenge, and there is a game begins.
- This game involves all miners competing against each other to solve the challenges, and this challenge will take approximately 10 minutes to be completed.
- Every single miner starts trying to find the solution to that one Nonce that will satisfy the hash for the block.
- At some specific point, one of those miners in the global community with higher speed and great hardware specs will solve the cryptography challenge and be the winner of the game.
- Now, the rest of the community will start verifying that block which is mined by the winner.
- If the nonce is correct, it will end up with the new block that will be added to the blockchain.
- The concept of generating a block provides a clear explanation of proof of work(PoW).

# Contd...

- PoW gives equal opportunity for all participants; every participant gets equal chance to prove that they have done the work as long as they have invested some efforts.
- Blockchain networks that uses PoW try to incentivize by rewarding those who put more efforts and are able to solve puzzle.
- The challenge with PoW is that it is extremely resource intensive, a hash puzzle can be solved with Brut force only.
- It hampers first rationale of providing equal opportunity to all.
- With more rewards for more efforts, those having higher computing gets rewarded.
- This has caused more than 10 mining pools/groups winning the reward more than 70% time.
- This also creates a situation known as 51% problem where a single participant may consistently reap the reward by solving the puzzle.

# Contd...

- It also makes chain susceptible to other issues such as finality inversion, invalid block finalization, liveness denial and censorship.
- With very few participants consistently taking the decision, a single hacker needs to get control of just few players to seek the control of entire system.
- This really defies
  - Finality inversion- An already finalized block may be changed by a selected few.
  - Invalid block finalization- The block that is not available or incorrect gets finalized.
  - Liveness denial- Participants can not allow any blocks to be mined.
  - Censorship- When cartel denies or deprioritizes creation of blocks from certain sources.

# Proof-of-Stake

- PoS tries to take into account realities on ground that participants can have skewed computation capacity.
- Proof of Stake (PoS) is a type of algorithm which aims to achieve distributed consensus in a Blockchain.
- This way to achieve consensus was first suggested by Quantum Mechanic here and later Sunny King and his peer wrote a paper on it. This led to Proof-of-Stake (PoS) based Peercoin.
- A stake is value/money we bet on a certain outcome. The process is called staking.

# What is PoS?

- As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it.
- Then, an algorithm chooses from the pool of candidates the node which will validate the new block.
- This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.
  - **Coin-age based selection:**
    - The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.
  - **Random Block selection:**
    - The validator is chosen with a combination of 'lowest hash value' and 'highest stake'. The node having the best weighted-combination of these becomes the new validator.

# Lecture 11

# PoS Workflow

- Nodes make transactions. The PoS algorithm puts all these transactions in a pool.
- All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like 'coin-age' or 'randomized block selection' to select the validator.
- The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can 'OK' the new block.
- If the block is 'OK'-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block's has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
- If the block is not verified by other nodes on the network, the validator loses its stake and is marked as 'bad' by the algorithm. The process again starts from step 1 to forge the new block.

# Features of PoS

- **Fixed coins in existence:** There is only a finite number of coins that always circulate in the network. There is no existence of bringing new coins into existence (as in by mining in case of bitcoin and other PoW based systems). Note that the network starts with a finite number of coins or 'initially starts with PoW, then shifts to PoS' in some cases. This initiation with PoW is meant to bring coins/cryptocurrency in the network.
- **Transaction fee as reward to minters/forgers:** Every transaction is charged some amount of fee. This is accumulated and given to the entity who forges the new block. Note that if the forged block is found fraudulent, the transaction fee is not rewarded. Moreover, the stake of the validator is also lost (which is also known as slashing).
- **Impracticality of the 51% attack:** To conduct a 51% attack, the attacker will have to own 51% of the total cryptocurrency in the network which is quite expensive. This deems doing the attack too tedious, expensive and not so profitable. There will occur problems when gathering such a share of total cryptocurrency as there might not be so much currency to buy, also that buying more and more coins/value will become more expensive. Also validating wrong transactions will cause the validator to lose its stake, thereby being reward-negative.



# Advantages of PoS

- **Energy-efficient:** As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved( as in case of Proof-of-Work system) thus saving the energy.
- **Decentralization:** In blockchains like Bitcoin(Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system(like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.
- **Security:** A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

# Weakness of a PoS

- **Large stake validators:** If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.
- **New technology:** PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.
- **The 'Nothing at Stake' problem:** This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

# PoS

- **Blockchains using Proof-of-Stake**

- Ethereum(Casper update)
- Peercoin
- Nxt

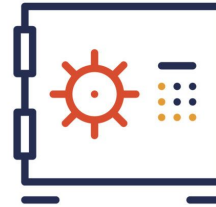
- **Variants of Proof-of-Stake:**

- Regular Proof-of-Stake – The one discussed in this article.
- Delegated Proof-of-Stake
- Leased Proof-of-Stake
- Masternode Proof-of-Stake

# PROOF OF WORK **vs** PROOF OF STAKE



The miner gets block rewards based on the amount of work they have done.



A new block creator is selected based on the number of coins they hold.



Miners who solve the blocks' problem first gets the reward.



POS has no concept of rewards. Miners only take transaction fees.



Miners in mining pools work in a group to increase efficiency.



POS is decentralized and is very cost-effective.

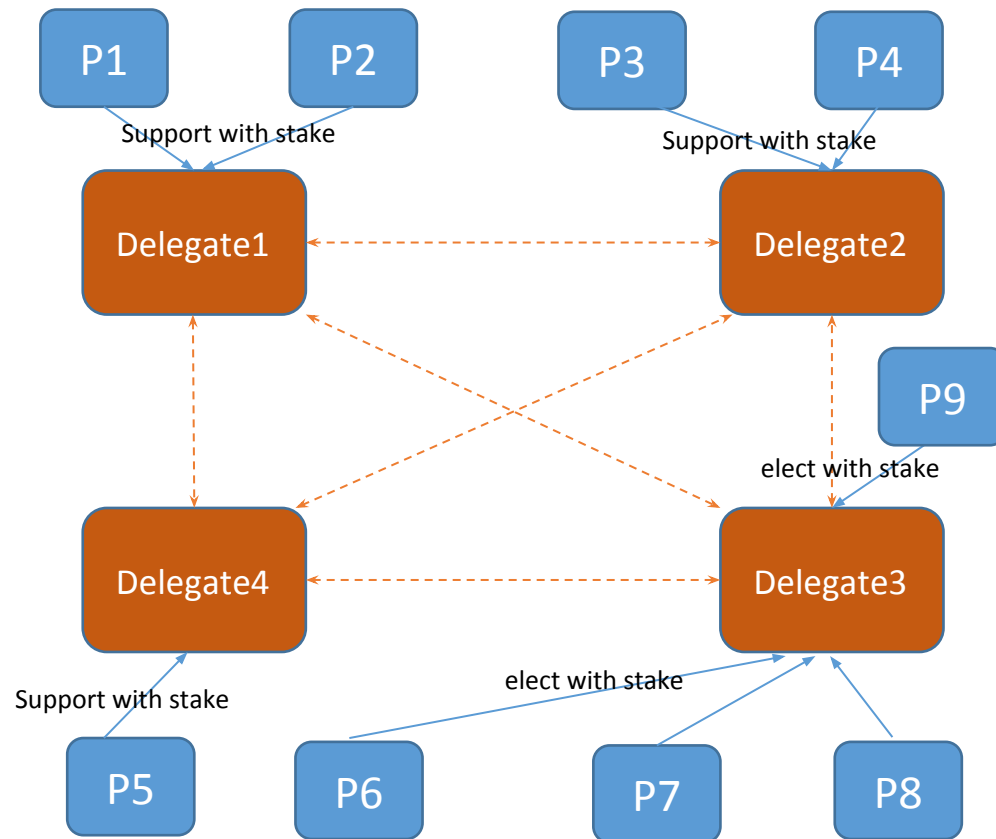
# Delegated-Proof-of-Stake

- Delegated Proof of Stake (DPoS) is a popular evolution of the PoS concept, whereby users of the network vote and elect delegates to validate the next block.
- Delegates are also called witnesses or block producers.
- Using DPoS, you can vote on delegates by pooling your tokens into a staking pool and linking those to a particular delegate.
- You do not physically transfer your tokens to another wallet, but instead utilize a staking service provider to stake your tokens in a staking pool.

# Delegated-Proof-of-Stake

- A limited number of delegates (most protocols choose between 20 and 100) are chosen for each new block, so the delegates of one block might not be the delegates of the next.
- Elected delegates receive the transaction fees from the validated block, and that reward is then shared with users who pooled their tokens in the successful delegate's pool.
- The more you stake, the higher a share of the block reward you receive. The rewards are shared based on each user's stake; so if your stake represents 5% of the total staking balance, you would receive 5% of the block reward.

# Delegated-Proof-of-Stake



- All participants have same base data
- Participants support smaller set of selected delegates or elect smaller set of elected delegates with stake
- A smaller set of delegates take turns in proposing and validating the block each has to lock a stake
- Delegates put a bet on data block to be added and vote. Weight of vote depends on size of bet and support delegates have.
- Weighted votes decides what block will be added and participants are rewarded in proportion to bet.

# Advantages

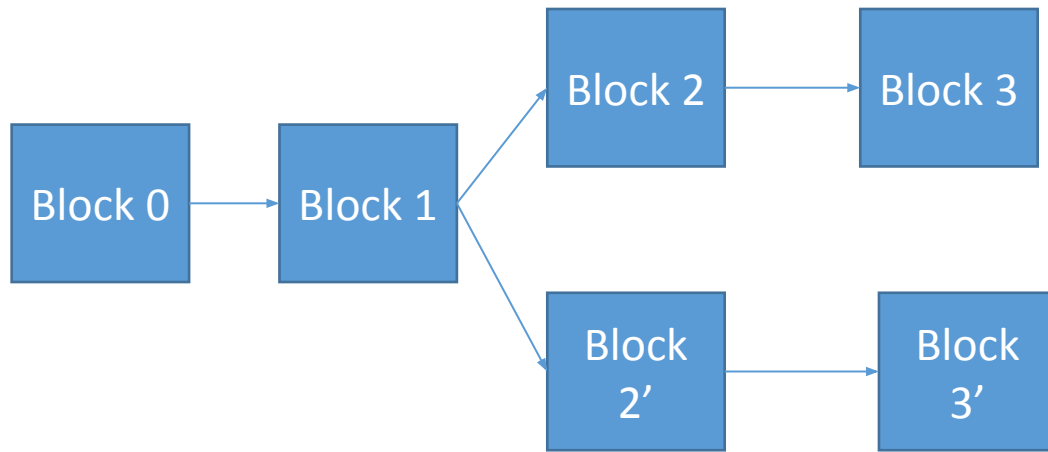
- DPoS blockchains have good protection from double-spending.
- DPoS is more democratic and financially inclusive due to lesser staking amount required by a user/node.
- DPoS provides more decentralization as more people take part in the consensus due to low entry threshold.
- DPoS doesn't require lots of power to run network, which makes it more sustainable.
- Transactions in DPoS is not dependent on computing power required to run network, hence it is more scalable.
- DPoS separates election of block producers from block production itself which opens door for more creative models to solve both problems in isolation.
- DPoS method provides foundation for implementing interesting governance models in blockchain applications. In a sense, it forms a kind of democracy.



# Disadvantages

- Effective operation and decision making of network requires delegators to be well informed and appoint honest witnesses.
- Limited number of witnesses can lead to centralization of network.
- DPoS blockchain is susceptible to problems of weighted voting. Users with smaller stake can refuse from taking part in votings after considering that their vote is insignificant.

# Nothing at stake problem

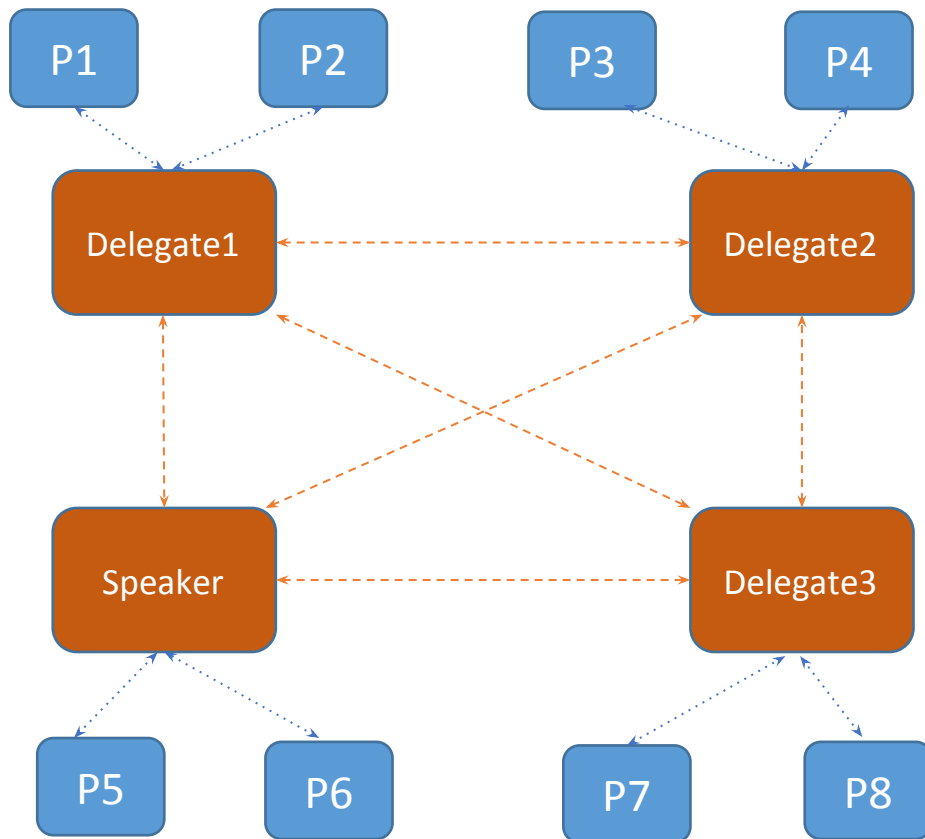


- Block 0 and block 1 were added to chain through consensus.
- While creating Block 2, two blocks Block 2 and Block 2' were proposed by the participants.
- Ideally, each participant is supposed to bet on only one block and the block that gets a greater weighted vote is supposed to win.
- While this is true, nothing prevents a participant or more from betting on both blocks equally.
- Not only that, participants can keep voting on subsequent blocks on both chains equally, which leads to hard fork.
- In case of forking, two parallel chains start forming.
- If participants bet on both the chains, they will get rewarded for one of the case anyway.
- It is known as nothing at stake problem where participant do not loose anything for supporting or performing malicious activity.
- Casper protocol tries to solve this where participant will need to pay penalty of stake that they have placed for transaction.

# Byzantine Fault-Tolerant mechanisms

- Byzantine Fault Tolerance is more a property of the system than just a consensus mechanism.
- There are three prominent variants.
  - Practical Byzantine Fault Tolerance (pBFT)
  - Delegated Byzantine Fault Tolerance (dBFT)
  - Federated Byzantine Fault Tolerance (FBA)

# Byzantine Fault-Tolerant mechanisms



- All participants have same base data. Participants can send request to the network.
- One of the delegate is chosen as a speaker. Different in each round, delegates are participants with better compute power
- Speaker creates a block and proposes it to delegates.
- Delegates validates the block. If  $2/3^{\text{rd}}$  delegates accept the proposed change, then it is accepted.
- All participants gets information as it gets confirmed.

# Byzantine Fault-Tolerant mechanisms

- Not every participant needs to have special hardware. Those who have it are called delegates.
- The system appoints a speaker among delegates.
- The speaker is supposed to be different in each transaction cycle, usually it is created in a round robin fashion.
- From the data, that is received from the participants, block is formed by the speaker.
- The speaker then publishes the block to all the delegates.
- The delegates validate the block and when  $2/3^{\text{rd}}$  of delegates send confirmation to the speaker, block is finalized.
- This makes BFT non forking as results are finalized once confirmed and there are no alternates possible.
- If the speaker is compromised, then  $2/3^{\text{rd}}$  of delegates will not agree on the proposal of the speaker.
- If some of the delegates are compromised and they send invalid confirmation, then they will be ignored as  $2/3^{\text{rd}}$  of the delegates who are not compromised will not send the confirmation.

# pBFT

- In pBFT membership list needs to be confirmed beforehand.
- This makes it challenging to use in public networks where the membership list is dynamic and always changing.
- Since agreements require multiple communication rounds, pBFT is communication heavy.
- This approach works in private and permissioned blockchain much better.
- E.g Hyperledger

# dBFT

- Special nodes in dBFT delegates are known as consensus nodes, while regular nodes are known as candidate nodes.
- dBFT has preselected consensus node.
- It helps to achieve very high transaction rates.
- E.g Network NEO implementing dBFT claims to achieve 10,000TPS.

# FBA

- FBA does not need network to be permissioned and private.
- It has limited set of delegates that take care of consensus.
- This set is supported by rest of the participants.
- The main difference is in the approach with which delegates reach consensus.
- Each delegate makes a choice for quorum slice, which is a rule about a smaller group that the delegate believes is enough for it to make a decision.
- E.g incase of international transaction, the bank delegate node might have a rule that it needs confirmation from at least two banks of origin and deposit countries.
- This gives dynamism as well as openness while achieving better performance and lesser compute needs.



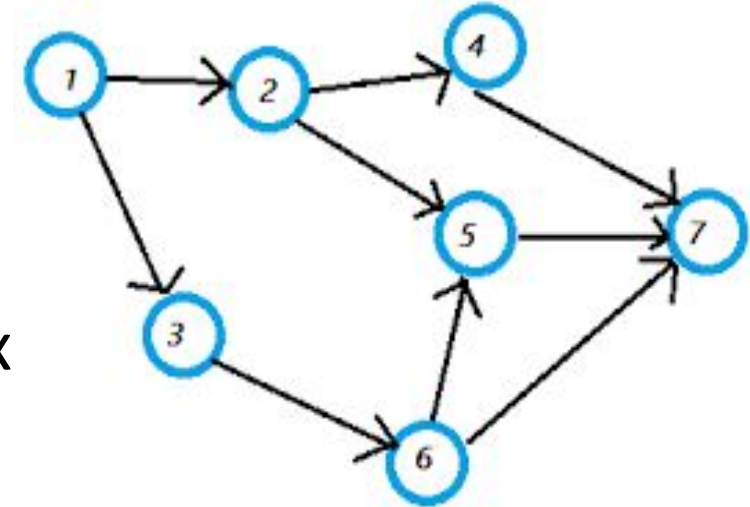
# Advantages of BFT

- BFT algorithm do away with resource wastage of PoW and at the same time they improve upon performance significantly.
- BFT also can function in permissioned, semi-permissioned and private networks.
- BFT also not require cryptocurrency available out of the box to function and this makes it very useful in blockchain networks that aim to log information onto ledger than be mechanism to trade cryptocurrencies.

# Lecture 12

# Directed Acyclic Graphs

- This mechanism uses directed acyclic graph data structure.
- The graph has nodes or vertices connected by edges or links.
- In case of directed graphs, edges have directions specified that can be considered as a path from one vertex to another.
- In case of acyclic graphs, there is no path from a vertex to itself that is going through another vertex/vertices.
- Basically, in case of DAG one can not form Cyclic loops.



- Hedera Hashgraph is an enterprise-focused public Distributed Ledger Technology (DLT) that utilizes a Directed Acyclic Graph (DAG) for its architecture instead of a blockchain.
- Hedera Hashgraph is a DLT service provider with built-in centralized control levers and client optimization. It has proven attractive to enterprises seeking to harness some of the functionalities of blockchain technology without fully committing to decentralization. However, Hedera Hashgraph's patented, for-profit gossip protocol, closed developer loop model, and limited decentralization have been criticized for a lack of transparency and equitability by some blockchain idealists.

# Proof-of-Capacity

- Proof of Capacity, also known as Proof of Space, Proof of Storage is an extremely intriguing consensus algorithm.
- To verify transactions, Proof of Capacity uses hard drives and storage.
- This approach provides a much cheaper and greener, thus more efficient and viable source of block verification.
- One live implementation of PoC, or PoSpace, is [Burst Coin](#).
- PoC miners use a 2 step system — plotting and mining.
- Plotting consists of creating a random solution, known as a plot, through the Shabal cryptographic algorithm and storing it on a miner's hard drive.
- Mining consists of miners reaching the solution, and whoever reaches it first, gets to mine the next block.

# Other Consensus mechanisms

- Proof-of-Activity-Proof-of-Activity (PoA) is a blockchain consensus algorithm that facilitates genuine transactions and consensus amongst miners. That is a consensus algorithm combining proof-of-work and proof-of-stake. This consensus algorithm is designed to prevent attacks on the underlying Blockchain.
- Proof-of-Importance-Proof of importance (PoI) is a cryptocurrency term defined as a blockchain consensus technique – essentially, proof of importance works to prove the utility of nodes in a cryptocurrency system, so that they can create blocks. In cryptocurrency jargon, proof of importance (POI) is a system used to determine which users are eligible to perform the calculations necessary to add a new block of data to a blockchain and receive the associated payment. A proof of importance algorithm prioritizes miners based on the number of transactions in the corresponding cryptocurrency that they perform. The more transactions are made to and from an entity's cryptocurrency wallet, the higher that entity's chances of being given mining projects are.
- Proof-of-Contribution
- Paxos and Raft

# Proof-of-elapsed time

- Also known as PoET.
- The algorithm is used mostly in permissioned blockchains like Hyperledger Sawtooth (in addition to PBFT). PoET uses a lottery-style random selection to select the node that is going to win the new block.
- PoET started to be used in Hyperledger Sawtooth in 2016/2017, introduced by Intel. The “miners” must first join the network, gaining a membership certificate. Once they are in the network, the nodes need to wait a certain amount of time that is randomly decided. The miner must wait at least the amount of time that was defined before starting mining a new block into the blockchain. In PoET, the miner that has the shortest amount of time is elected to do the block mining that round. The system tends to be fair and choose miners with a good degree of randomness. It doesn’t require much electricity consumption and miners can “go to sleep” while they wait for their turn.

# Proof-of-Burn

- Invented by Iain Stewart, Proof of burn is an experimental consensus mechanism and a fascinating concept: Slimcoin, a defunct cryptocurrency used to use it. Proof of burn aims to provide a very different incentive mechanism for nodes to participate in validating transactions.
- Proof of burn can be seen as precisely the opposite of what the Central Banks do: it destroys currency instead of printing it.
- Instead of “burning” electricity and hardware like proof of work does, proof of burn just burns its own coins to provide an incentive for nodes to be good actors in the blockchain.
- Proof of burn miners needs to send a number of coins to an unspendable address(blockchain address with no private keys). When coins are sent to this unspendable address, they are not really destroyed or burned. They simply fall into a black hole and can no longer be spent or accessed. Many other cryptocurrencies or tokens use the same concept in order to decrease the supply.
- Back to proof of burn, the more coins they send to burn, the higher the probability of being chosen by the algorithm to mine a block. They receive a reward if they validate transactions and mine a block correctly. If not, they just simply burned the coins and wasted money.
- Miners are randomly chosen according to the number of coins they sent to burning
- Burning more coins translates to more commitment, thus higher the chances of being selected as a miner (just like spending more electricity on proof of work increase the chances of mine a block)
- Burned coins are lost forever, locked in a burn address



# The Proof-Of-Authority

- The Proof-Of-Authority (PoA) is a consensus method that gives a small and designated number of blockchain actors the power to validate transactions or interactions with the network and to update its more or less distributed registry.
- Proof-of-Authority (PoA) is a new consensus algorithms family that provides high performance and fault tolerance. In PoA, rights to generate new blocks are awarded to nodes that have proven their authority to do so. To gain this authority and a right to generate new blocks, a node must pass a preliminary authentication.
- Proof of Authority (PoA) is a modified form of Proof of Stake (PoS) where instead of stake with the monetary value, a validator's identity performs the role of stake. In this context, identity means the correspondence between a validator's personal identification on the platform with officially issued documentation for the same person, i.e. certainty that a validator is exactly who that person represents to be.

# Proof of contribution

- It aims to incentivize donating compute time for large data research programs.
- End users who donate compute time are rewarded with tokens.
- These are very useful where compute can be divided into large number of parallel functions
- These mechanisms are not for regular use cases and in cases where problems cannot really be split into parallel computational tasks.

# Proof-of-Brain

- It aims to give authority of consensus and rewards for contribution to end users.
- The idea is to build consensus based on how many likes or reviews end user gives to the content.
- The basic principle here is of crowdsourcing or crowd wisdom.
- Proof-of-Brain is useful in case there is no firm information source and when the probability of the crowd being right is high.
- Tokens are generated at a fixed rate and distributed to participants.
- Actors include creators of social content and curators for these tokens.
- The downside is that use cases need to incentivize truthfulness and there is also some probability that the information captured is invalid or manipulated by the crowd with hidden intentions.

# Paxos and Raft

- Paxos and Raft are two distributed consensus mechanisms that help implement BFT consensus even if some of the nodes are not alive and connected.
- In case of Paxos, the nodes are classified into three roles. The proposer node proposes a value for acceptance. The acceptor nodes accept proposed value from proposers based on rules that are based on indexes of values that are accepted across the network.
- Paxos is relatively complex mechanism.
- Raft tries to simplify the overall mechanism by keeping only two roles-leaders and followers.
- Leaders can be chosen in round robin fashion, lottery or other mechanism and participate in building consensus.

# Lecture 13

# Mining and finalizing blocks

- In case of blockchain network, consensus decision is about composing a block.
- The transaction data is received by the network participants and each of the node tries to ensure that the transaction data they have received is included in the blocks.
- While participant nodes try to compose the block, they also communicate the transactions to each other.
- In this manner, each of the participants have their own block composition that they want to all participants to agree on.
- Various consensus mechanisms help in decision-making, which a participant's block is to be accepted by the network.

# Mining and finalizing blocks

- In case of public blockchain network that supports cryptocurrencies, transactions that perform exchange of currencies form data that is to be put in the block.
- The currencies are called Tokens. One token is a unit of currency say, a dollar, a pound, a rupee etc.
- While consensus help in selection of the participant whose block is to be added to the network ,it also involves reward for the effort.
- A participant that is investing efforts in creation of the blocks is helping the network sustain itself and so this participant will be incentivized.
- Part of this incentive comes in the form of fees that the participant charges to individuals who are performing transactions.
- While fee is a good incentive, it just incentivizes addition of transaction to the chain;thus efforts required to create the block that are agreed on by all the network participants also shall be incentivized.

# Mining and finalizing blocks

- This is done by creating new money in the network and giving it to the participant whose block is added to the network.
- The process of creation of the new token and allocating it to the participant whose block is accepted by all participants is called *mining*.
- Participant nodes that participate in mining are called as *miners*.
- Mining help the network sustain itself by rewarding participant that put efforts, defines a consistent way in which new tokens are added to the pool and establishes immutability of the transactions



# Mining and finalizing blocks

- The mining process is much more complicated than just reaching consensus and sharing blocks.
- All participant nodes are getting transaction in parallel; each want transaction they have received to be included in the next block, each one sharing transaction they have received with everyone and at the same time, each participant is also trying to create the new block.
- To implement this, transactions are first placed in something called *mempool*.
- When a transaction is received by the network but it is not accepted in a block that is agreed by participants, it is called *unconfirmed transaction or pending transaction*.
- Mempool is a transient place where transactions are placed before their confirmation. Mempool is the location of unconfirmed transactions.

# Mining and finalizing blocks

- Once a transaction is placed in a block that is accepted by all participants on the ledger it is called *confirmed transaction*.
- Unconfirmed transactions can stay in mempool for long time.
- Transactions that offer good fee are picked up by miners earlier as compared to transactions that offer lesser fee.
- For this reason, transaction can remain unconfirmed for really long time.
- This also create situation where end users need to wait for a certain time to know if the transaction has been accepted or rejected.
- Mempool is involved concept and some of the participant might form forks where multiple chains start growing in a single network.
- Blockchain protocol implements checks, incentives and mechanism to ensure that such scenarios are managed and governed and do not create significant damage.
- E.g keeping block confirmation time to 10 min and participant losing stake for undesirable behavior and rewarding for desirable behavior through mining rewards.

# Mining and finalizing blocks

- The fact that transaction do not get confirmed on some of the blockchain networks immediately creates two scenarios.
- In first scenario after transaction is submitted to the miner, there is a probability that the transaction is picked up and placed in a block.
- In the second scenario, there is surety that if transaction is accepted by the miner, then it will be placed on a block.
- The confirmation about transaction submitted by the participant to be accpeted on immutable ledger chain is called *finality*.
- Finality helps ascertain the rate at which transaction become final on the network.
- It can be decision about how much time one should wait before next retry or purchase on the network.
- Finality is not the property of the network, but of consensus mechanism.

# Mining and finalizing blocks

Probabilistic finality-There is chance or probability associated with the transaction being added to the ledger post as it is received by the minor. Here, if a sufficient number of validating participants have agreed to include the transaction on the block, then chances of reversal will be very less as validating participants also lose because the block they have agreed to is not getting confirmed. It is the property of PoW, PoS and dPoS.

The special scenario in prob. Finality where sufficient number of validators have confirmed validity of the block and in turn inclusion of transaction in the block is called as economic finality

Absolute finality—Also called as immediate finality. If the miner receives the transaction, it will definitely be added to the network. dBFT, pBFT supports it.

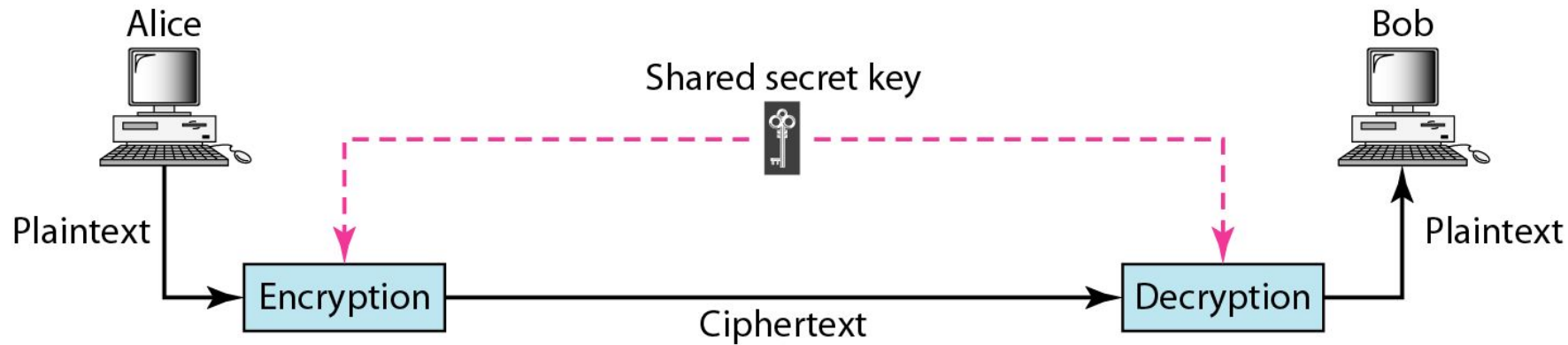
# Currency (Tokens)

- When assets get transacted on blockchain network they are given digital identities, called tokens.
- A token that is interchangeable (any one token can be replaced by other) is called fungible token. E.g. currency tokens
- E.g. If I have 100 dollars, it is immaterial if I have five 20 dollar bills, twenty 5 dollar bills or 100 dollar coins.
- A token that is not interchangeable (we need to individually identify asset and one asset can not be replaced by another even if of same value) is called non fungible tokens.
- Most physical entities that are tracked through transactions become non fungible.
- Asset in itself is non fungible, but how it is being tracked and the purpose behind use of blockchain really makes it fungible or non fungible on that blockchain.
-

# Security on Blockchain

- Security is implemented at various stages-at storage,at transport and at end compute level.
- Cryptographic functions are used for encryption and decryption at right levels.
- Blockchain framework utilize Public Key Infrastructure (PKI) in various forms to implement security.

# Symmetric-key cryptography



In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption).

The key is shared.

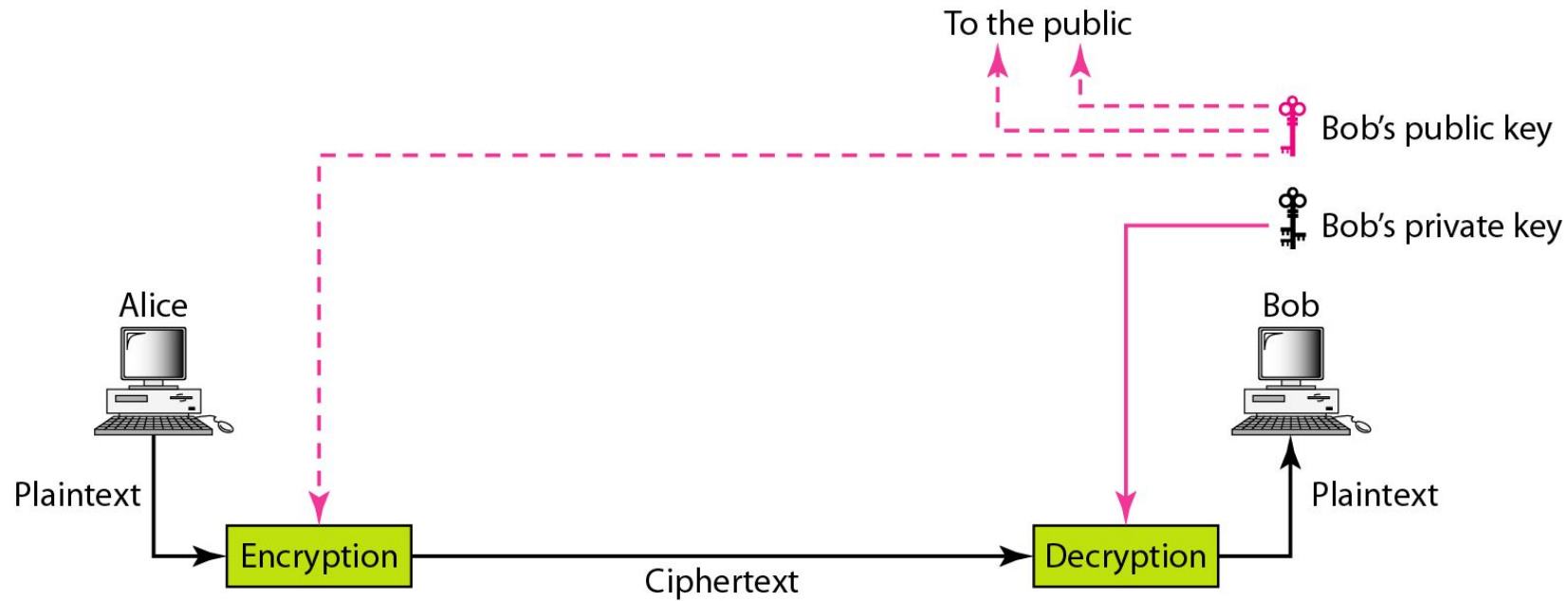
Algorithm: DES, 3DES

# Symmetric-key cryptography

- Advantages:
  - Simple
  - Faster
- Disadvantages:
  - Key must exchanges in secure way
  - Easy for hacker to get a key as it is passed in unsecure way.



# Asymmetric-key cryptography

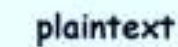


*An asymmetric-key (or public-key) cipher uses two keys: one private (To decrypt data) and one public (To encrypt data).*

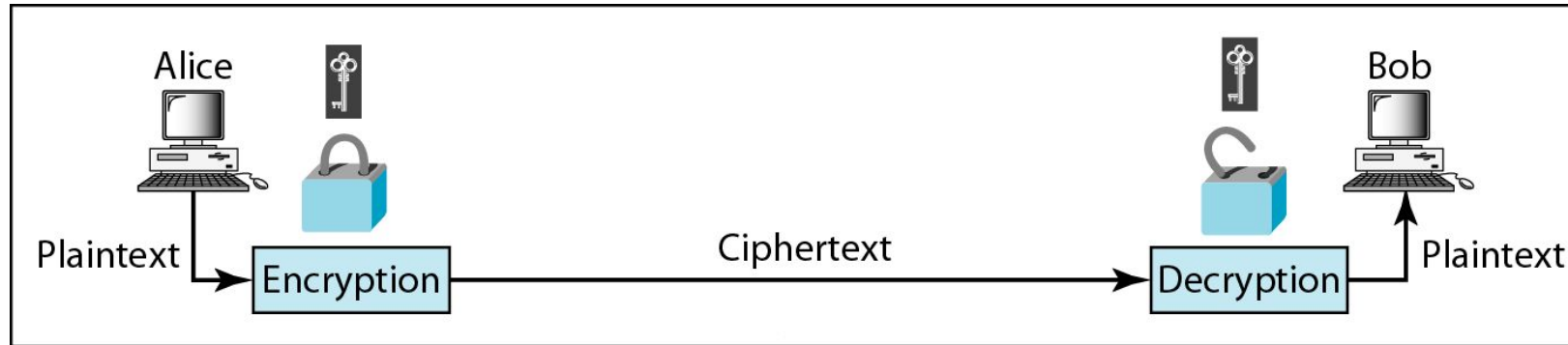
- Asymmetric encryption use two keys:
  - Public Key - to encrypt the data
  - Private Key - to decrypt the data
- These keys are generated together.
- The Public key(s) is distributed freely between the sender and receiver.
- The other is named as Private Key and it is kept hidden.
- The Private Key is only used for Decryption and will not be shared between the sender and receiver.
- RSA, Digital Signature Algorithm, Diffie-Helman

# Asymmetric-key cryptography

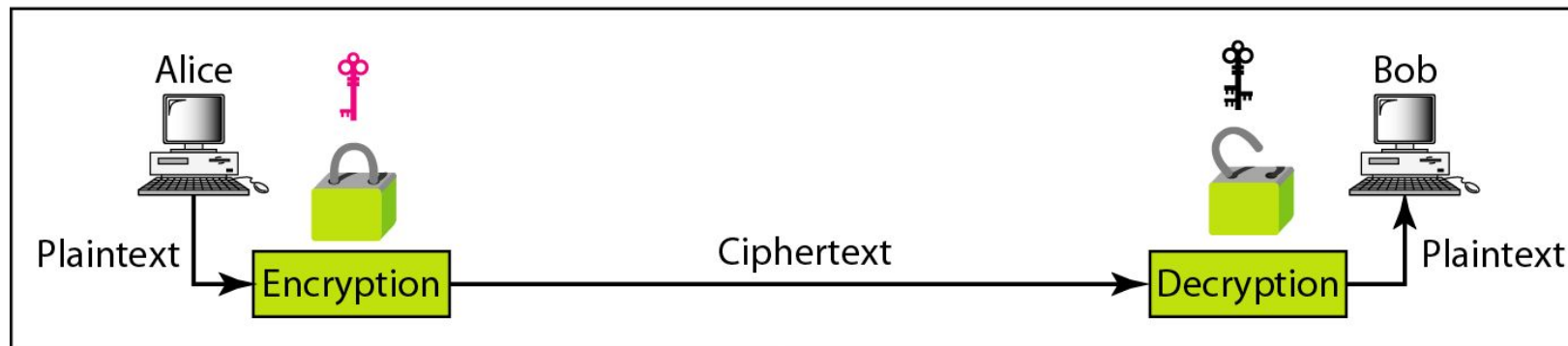
- Users get the Key from a Certificate Authority
- Advantages
  - More Secured
  - Authentication
- Disadvantages
  - Relatively Complex



# Comparision



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

# MERITS & DE-MERITS

- Merits:

- ❖ Two parties **don't need to have** their private keys **already shared** in order to communicate using encryption.
- ❖ **Authentication** and **Non-Repudiation** are **possible**. (Authentication means that you can encrypt the message with my public key and only I can decrypt it with my private key. Non-repudiation means that you can "sign" the message with your private key and I can verify that it came from you with your public key.)

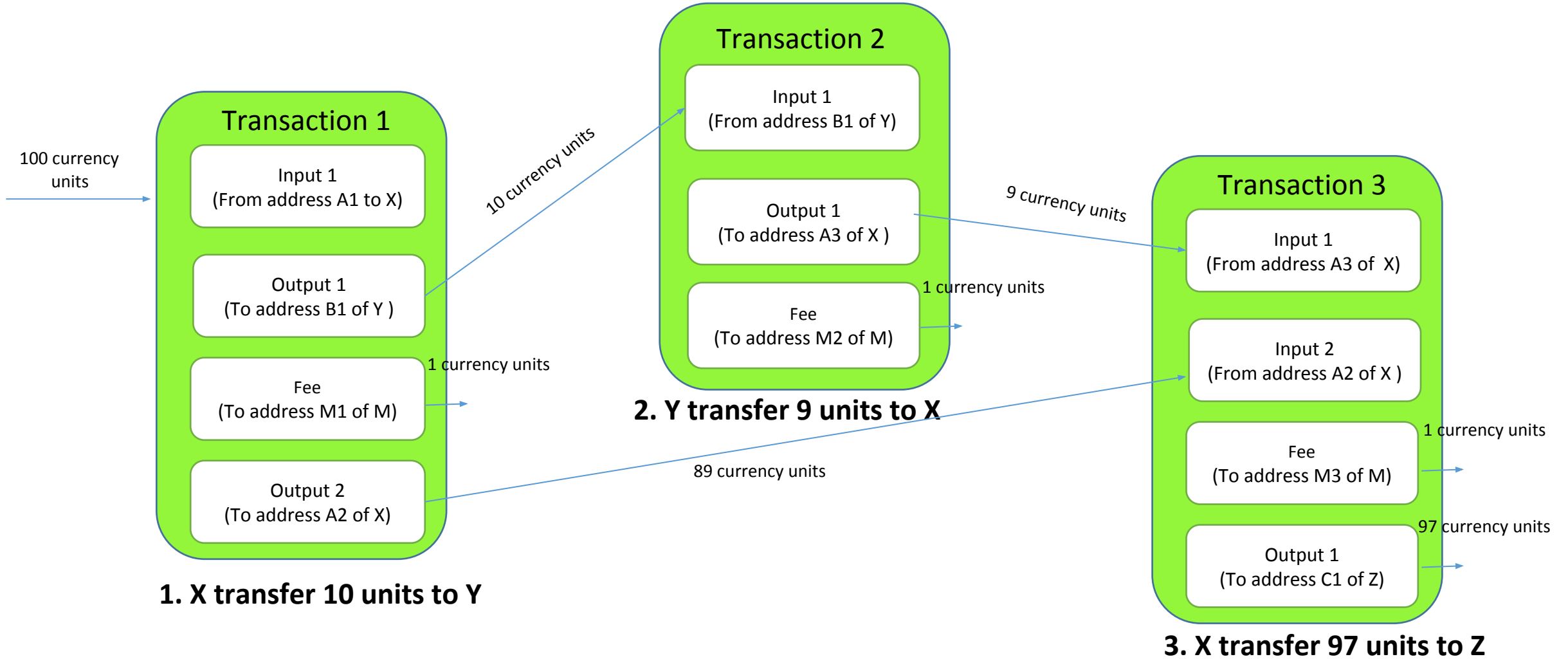
## De-Merits:

- ❖ Asymmetric Encryption algorithms are comparatively complex.
- ❖ Time consuming process for Encryption and Decryption.

# Data storage on Blockchain

- Storage of transactions needs to be optimized for consensus, information sharing and storage.
- With all participants receiving copy of data, privacy of information stored along with it is also important factor.
- Generally, there are two models in which transaction data is stored and processed.

# UTXO (Unspent Transaction Output )Model





# UTXO (Unspent Transaction Output )Model

- Each transaction has input addresses and output addresses which belong to individual.
- In this method, account balance is not stored explicitly on the chain.
- Each time transaction needs to be created, all the UTXOs from all the addresses need to be consolidated to feed as input to subsequent transactions.
- This is done by off chain utilities called *wallets*.
- The biggest advantage of the UTXO model is that transactions cannot be replayed on chain as each transaction needs output from a previous transaction as input.
- Even if transaction is of same amount, the output address will change while creating the similar transaction. This also helps create transactions in parallel improving capability.
- This approach provides improved privacy as multiple addresses are used by each user's transaction outputs.
- The challenge is in difficulty in performing complex computations.
- Also, for the end users ,to off chain computations on wallet is required for them to give a view on their spending capacity.
- Bitcoin used this approach.

# Lecture 14

# Global State Model

- The Global state model records the transactions and stores the impact of the same outside the transaction.
- Each transaction is recorded between accounts and the result is aggregated.
- For platforms that support currency at platform level such as Ethereum, aggregation is done at user accounts.
- In this model, both transactions and state of the account need to be stored at each node.
- As implementation, each node push transactions on to the block and there is an impact of these transactions on to the account states.
- This impact needs to be stored separately on the nodes.
- Ethereum manage this through EVM. It introduces additional layers between storage to manage state, transactions and transaction receipts.
- Unlike the UTXO model, where wallets that are connected to nodes take care of aggregation, in global state model, the information is stored as part of global state and is shared with all participants.
- This global state is known by different names in different platforms such as a world state in Hyperledger, account in Ethereum etc.

# Global State Model

- The Global state model provides easy to consume interface and information
- Reduces design and development complexity
- Allows developers to focus on use cases more than technicalities.
- Performance to extract global state is little better –but needs to consume network and processing resources to prepare and sync up the global state.
- Detecting transaction replay is quite challenging-No easy way to detect differences between two same amount-same party transactions.
- Bulk transaction processing is little better
- Not easy to issue parallel transactions from a single account. This is because not all blockchain platforms accept and finalize transactions asynchronously . Some uses separate databases to store global state.
- E.g Hyperledger allows use of levelDB or CouchDB and Ethereum state tier stores information in name-value pairs.

# Global State Model

- While blockchain is a shared ledger, by design it is not used for storing large amounts of data.
- Decentralized storage technologies, such as IPFS (Interplanetary File System) can be a solution for more data storage requirements.
- One of the concerns on data storage on blockchain is that ledger data keeps growing. This ever-increasing data store is a concern to participants and has significant performance, processing and cost implications.
- To alleviate these issues, the platform allows participants to be of different processing capacity to allow only transaction reads or transaction updates.
- Platforms also allow to purge or prune the ledger data store.

# Wallets

- On blockchain information is shared with all nodes, however individual identity information is not captured by any of the nodes to avoid privacy breach. Information that is captured also needs to be secured during transit and at rest.
- Wallets help to achieve these by storing three data items-private key, public key and wallet address.
- Wallet address establishes identity of the wallet with blockchain network.
- Wallets are analogous to a bunch of keys that are used to sign the transactions and receive transaction outputs.
- Wallets do not store cryptocurrency.
- Wallets are utilities that assist end users to interact with the blockchain network.
- UTXO model wallets help aggregate transaction outputs so that an end user understands his/her current spending capacity.
- In global state model wallets help manage accounts and balances.

- In reality, crypto wallets don't store the currency but act as a tool of interaction with blockchain, i.e., generating the necessary information to receive and send money via blockchain transactions.
- The information comprises pairs of private and public keys. Based on these keys, an alphanumeric identifier called address is generated.
- In essence, this address specifies the location to which coins can be sent to the blockchain. The address can be shared to receive funds, but private keys are to be never disclosed.
- The private key can be used on any wallet for accessing the cryptocurrency.
- As long as the private key is known, funds are accessible on any device. Also, coins are just transferred from one address to another, never leaving the blockchain.

# Wallet address generation in Bitcoin





# Wallet types

Deterministic wallets-  
Randomly generated private keys based on seed words  
Sequential Wallets  
Hierarchical Wallets

Non-Deterministic wallets

# Cryptocurrency wallets--Simplified

<https://youtu.be/d8lBpfs9bf4>

# Wallet types

Hot wallets -are connected to the Internet and thus are less secure and pose more risks but are user friendly, are more likely to be used for daily transactions, are easy to set up, and the funds are quickly accessible. Traders conveniently use them.

Cold wallets are stored offline and don't require internet connectivity. Thus, improved security and less risk. Used for more long-term holdings, are hack resistant, and thus the cold storage is suitable for HODLers. As a protection method, only a small percent is stored in hot wallets while being able to trade directly from their cold storage devices.

# Wallet types

Hardware wallets -are hardware devices that individually handle public addresses and keys. It looks like a USB with OLED screen and side buttons. It is a battery-less device and can be connected to PC and accessed by native desktop apps. It cost up to 70-150 dollars, but it is worth it. They have received a mixed response. They are more secure than hot wallets and user-friendlier than paper wallets but less than web and desktop wallets. They are available in different forms and offer reasonable amounts of control. They are difficult for beginners to use when the investment is significant. Most popular hardware wallets are Ledger Nano S and Trezor.

Paper wallets-It is a physically printed QR coded form wallet. Some wallets allow downloading the code to generate new addresses offline. They are not prone to hacks, but the number of flaws has made them dangerous. A major flaw is not being able to send partial funds. Thus, it can't be reused. They were used to be very popular for cold storage, but not after hardware wallets came onto the scene. All in all, if stringent security precautions are taken, then paper wallets can be set up.

# Wallet Types

**Desktop wallets**-These are installable software packs available for operating systems and are becoming serious with time. Anti-virus is required because a system connected to the Internet poses fundamental security issues. Instead of keeping cryptos on an exchange, desktop wallets for bitcoins should be used. They are the third most secure way to store cryptocurrencies and the best method for cold storage in a completely clean system. They are easy to use, give privacy, anonymity, and involve no third party. Regular backing up of the computer is needed. Popular desktop wallets are Exodus, Bitcoin core, Electrum, etc.

**Mobile wallets**- are just like desktop wallets made for smartphones. They are quite convenient as it uses QR codes for transactions. They are suitable for daily operations but are vulnerable to malware infection. Encryption of mobile wallets is necessary. They are practical and can be used on the go but open to viruses. Some mobile wallets are Coinomi and Mycelium.

**Web wallets**-These wallets are accessed by internet browsers. The private keys are held in some web wallets and are prone to DDOS attacks. They can be hosted or non-hosted. Non-hosted is preferred as funds are always in control. They are the least secure wallets. They are not the same as hot wallets. They are ideal for small investments and allow quick transactions. Some of these are MetaMask and Coinbase.

# Lecture 15

# Smart Contracts

- Smart contracts provide a way to store certain data and/or execute certain code on blockchain platforms, which can be initiated based on certain conditions.
- On Hyperledger platform, this is called chaincode.
- Smart contract runs on all nodes of blockchain network.
- When a smart contract is deployed, similar transactions get propagated on all nodes of the blockchain and smart contract also gets propagated.
- When a node is down for a while and comes back online, the ledger syncs up and all the smart contracts would run in sequence.
- Smart contracts once deployed can run or fail, they can not be killed or cancelled.
- They do not have standard output such as sysout or stdout. It makes challenging to debug smart contracts.
- They cannot interact with non blockchain systems through synchronous calls.
- They also do not have the capacity to store large amount of data.
- Each blockchain platform supports different programming languages.

# Smart Contracts

- To consolidate the information from outside the blockchain and connect with smart contracts specialized constructs e.g *oracles* are used.
- Oracle is a routine that executes outside the blockchain, consolidates information from multiple sources and pushes the information to smart contracts.
- Oracles are usually server side scripts listening to requests and invoking appropriate blockchain transactions.
- They need to manage security while interacting with blockchain.
- Blockchain smart contracts also need to ensure that information acceptance is appropriately decentralized so that it should not be possible for certain set of oracles to disproportionately influence transaction results.



# Peer-to-Peer Network

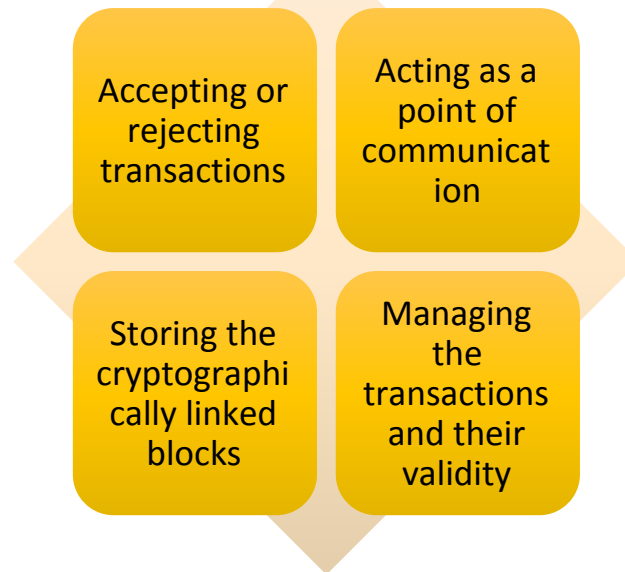
- In Peer-to-Peer network, all participating systems are of equal authority or status.
- All participants can act as client as well server to each other.
- It is not mandatory that all are physically connected to each other but all can communicate.
- Here, Security is major concern.-Compromising of one node
- In Blockchain ,all participants are peers with equal privileges.

# Blockchain nodes

## What are Nodes?

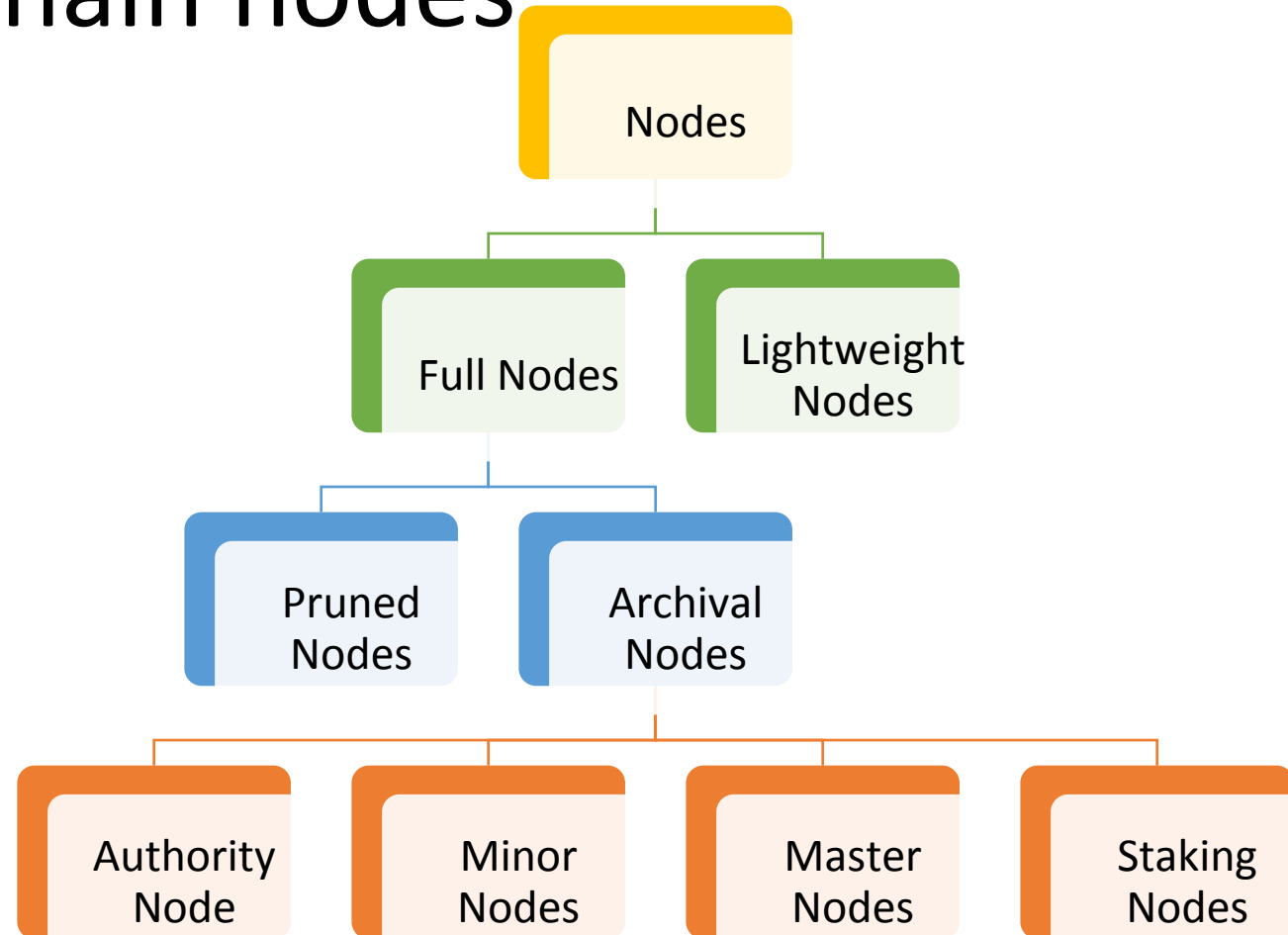
Nodes are the electronic devices connected to the network and possessing an IP address. Generally, nodes are the communication endpoints which means that any user or application that wants to interact with the Blockchain does so through nodes. Therefore, nodes are also a point of communication redistribution.

## What does a Blockchain node do?



# Types of blockchain nodes

- While it is true that all nodes in blockchain are peers, not all participating nodes have capability or intent to perform all the functionality to perform all the activities and transactions on nodes.
- Based on the capability of the nodes to perform transaction or activities on blockchain nodes, these can be classified in different ways.



### Full Nodes

*Full nodes act as a server in a decentralized network. Their main tasks include maintaining the consensus between other nodes and verification of transactions. They also store a copy of the blockchain, thus being more secure and enable custom functions such as instant send and private transactions.*

*When making decisions for the future of a network, full nodes are the ones that vote on proposals. If more than 51% of them don't agree with the proposition, it gets skipped. In some cases, this can lead to a hard fork in which the community cannot agree on a certain change and thus go their separate ways, creating two chains. The most well-known example of that happening is the [Bitcoin Cash Fork](#).*

### Lightweight Nodes

*Another type of blockchain nodes, used in day to day crypto operations, is the lightweight node or Simple Payment Verification (SPV) node. You've probably come across it already, but you're most likely familiar with the "light wallet" definition.*

*These types of nodes communicate with the blockchain while relying on full nodes to provide them with the necessary information. As they don't store a copy of the chain, they only query the current status for which block is last, and broadcast transactions for processing.*

*Having in mind the above features, it's clear to see that running SPV node doesn't require many resources, but it does sacrifice security for the sake of convenience.*

### **Pruned nodes**

*The specific characteristic here is that it begins downloading blocks from the beginning and once it reaches the set limit, deletes the oldest ones, retaining only their headers and chain placement. For example, if you set a size limit of 550MB, you will store all the latest blocks that can fit in that hard drive space, but in order to get to that state, you would first have to go through the entire blockchain to validate all those previous blocks.*

*Pruned nodes are considered full nodes and thus can also verify transactions and be involved in the consensus.*

### **Archival nodes**

*Archival full nodes are what most people refer to when talking about full nodes. They envision a server which hosts the full blockchain in its database. As I already shared with you above, their main task is to maintain consensus and validate blocks. The difference between pruned and archival node is one – the amount of hard drive space they take up on your server or PC.*

*Archival nodes can be divided into a couple of subtypes – those that can add blocks to the blockchain and ones that are unable too.*

# Miners (Mining Nodes)

- Miners are actually nodes (either full or light ones) which aim to prove that they've completed the required work to create a block. Hence the consensus name Proof of Work. To complete the task, as I mentioned above, miners need to either be an archival full node themselves or receive data from other full nodes on the network to know the current status of the blockchain and the required parameters for the next block in line.
- Participants in the process employ hardware components (be that CPUs, GPUs or ASICs) to solve a cryptographic problem. The first person to complete the task broadcasts his results to the network so it can be verified by full nodes and once consensus is achieved – he is granted the right to add a block to the existing blockchain. For their work, miners are rewarded a pre-defined amount of coins in addition to any transaction fees for the block. This set reward amount is called coinbase or a coinbase transaction. Considering it's the first transaction in the block, it's free of charge, as the miner himself created the block and included it.

## Pros

- Easy to understand and follow concept of proving your involvement
- Opportunity to work in tandem with others and increase the rate of receiving rewards

## Cons

- The process of mining consumes a lot of electricity and is thus wasteful
- In the case of ASICs – equipment producers are near monopoly (Bitmain)
- High initial cost and uncertainty of ROI

# Stakers (Staking Nodes)

- Staking can be compared to having a traditional fiat money deposit. You buy coins and hold them, while in return you receive an interest back as a reward. While there are different takes on the Proof of Stake consensus mechanism, the main characteristic is that earning money can be compared to participating in a lottery. Staking is a game of chance, which while with a lower barrier to entry, offers less certainty compared to mining and can be confusing at times.
- The end goal is to determine, based on a pre-defined set of rules and luck chance factored in, who will be next to create a block and get rewarded. Factors include coin age (how long you've had your coins), how many you have and their ratio to available ones in the network. In staking, you don't need any expensive machinery, you only keep your crypto wallet online 24/7, which can be done with a device like the Raspberry Pi.
- To be able to stake, you will need to become a full archival node, i.e. download the core wallet for the coin and keep the entire blockchain on your device.

## Pros

- The barrier to entry is low and coins can be easily bought
- Low energy consumption

## Cons

- Luck-based rewarding system
- Solo endeavor, due to lack of transparency in staking pools

# Authority Nodes

- The blockchain nodes all can join a network and perform their tasks without anyone giving them permission. That is the essence of a blockchain – its decentralized nature. Unfortunately, there are few drawbacks to this approach and the solution involves employing some level of centralization to gain benefits like increased speed. Consensus algorithms include Delegated Proof of Stake, Delegated Byzantine Fault Tolerance, Proof of Authority and others.
- Networks that make use of such algorithms need to define a fixed number of authority nodes. How many and who they'll be is voted on by the community or defined by the development team. The task of these nodes is, as with full nodes, is to create and validate blocks, while at the same time distributing information to users on the network. All participants, not chosen to be an authority node, will be running lightweight nodes (light nodes) which depend on the broadcasted data to be able to operate on the blockchain.

## Pros

- Increased speed of transactions
- No storage requirements, you can use your mobile device as a wallet
- Easier to upgrade the network and hold developers accountable

## Cons

- Lower levels of trust, due to centralization
- Vulnerable network as it can be attacked more easily



# Masternodes

- Compared to full nodes, masternodes themselves cannot add blocks to the blockchain. Their only purpose is to keep a record of transactions and validate them. Whether it will be miners or stakers, they're the ones writing blocks on the blockchain. An added benefit, however, is that by running a masternode, you not only secure the network but can earn a share of the rewards for your services.
- To establish a masternode, you will need to lock away a certain sum of funds as collateral. You are expected to be online 24/7 and hosting on a Virtual Private Server is considered good practice.

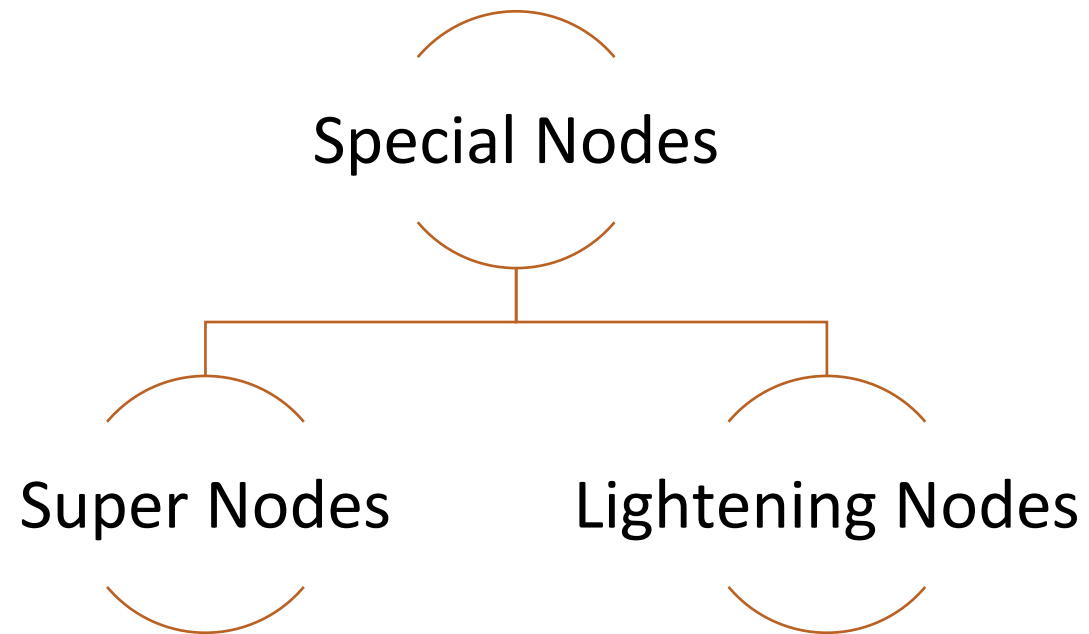
## Pros

- Beneficial for the network while also rewarding
- Great source of passive income
- Not too expensive to maintain

## Cons

- Requires large initial investment
- The setup process is not that straightforward

# Special Nodes



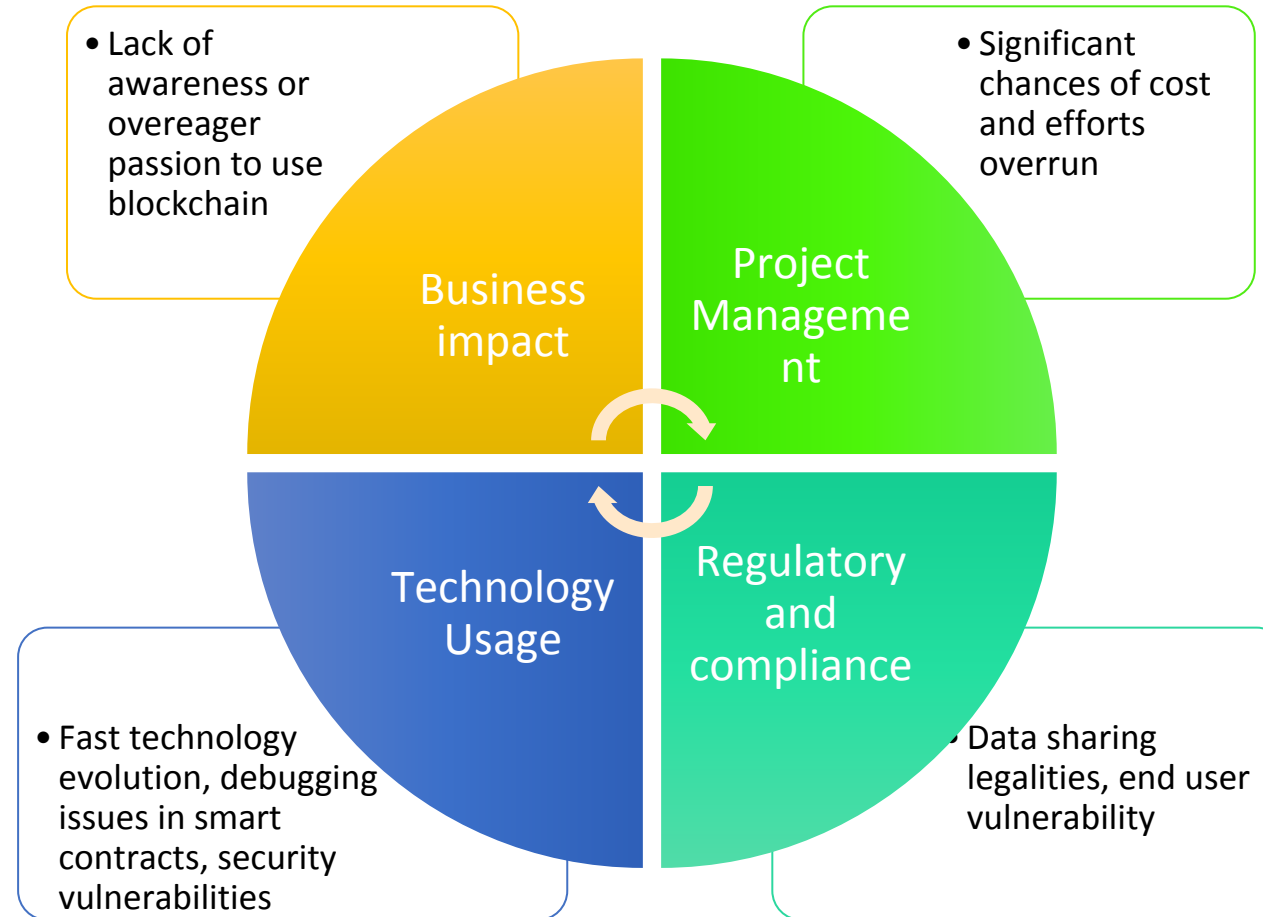
### Super Nodes

*Specific to some Blockchains, super nodes are created to carry out some special tasks. For instance, implementing a [blockchain protocol](#) change or maintaining the Blockchain rules is done by a super node.*

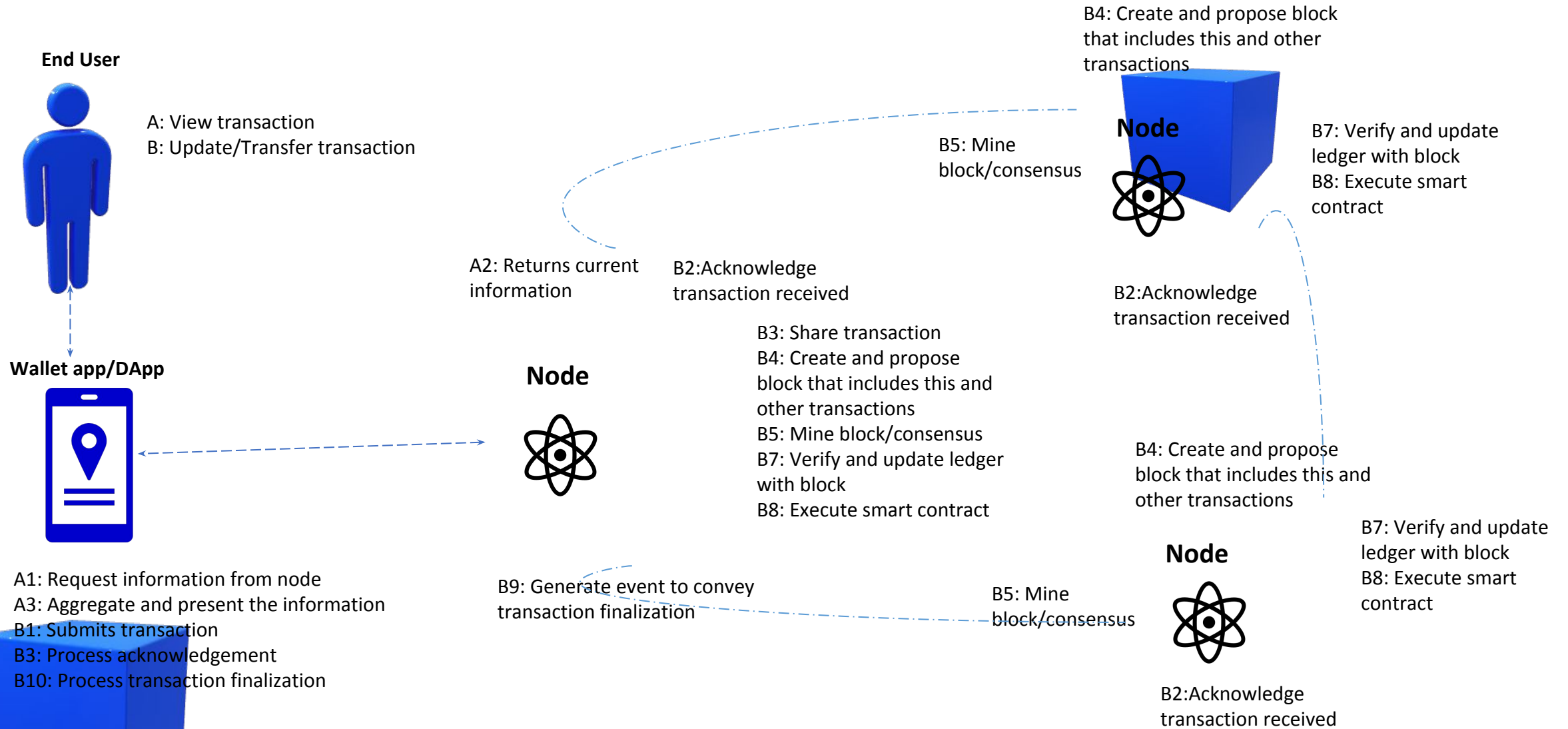
### Lightning Nodes


*Congestion in a Blockchain network is a common situation that leads to delayed transactions. This is what led to the creation of lightning nodes. These nodes create a separate network with a user and the transactions are pushed to the main Blockchain. This allows the transactions to be instantaneous and also reduces the cost of transactions as the load on the network is reduced.*

# Risks associated with blockchain solutions



# Lifecycle of blockchain transaction



***Thank you*** 

# Lecture 17

# Unit III

## Architecting Blockchain Solutions



# Obstacles for use of Blockchain

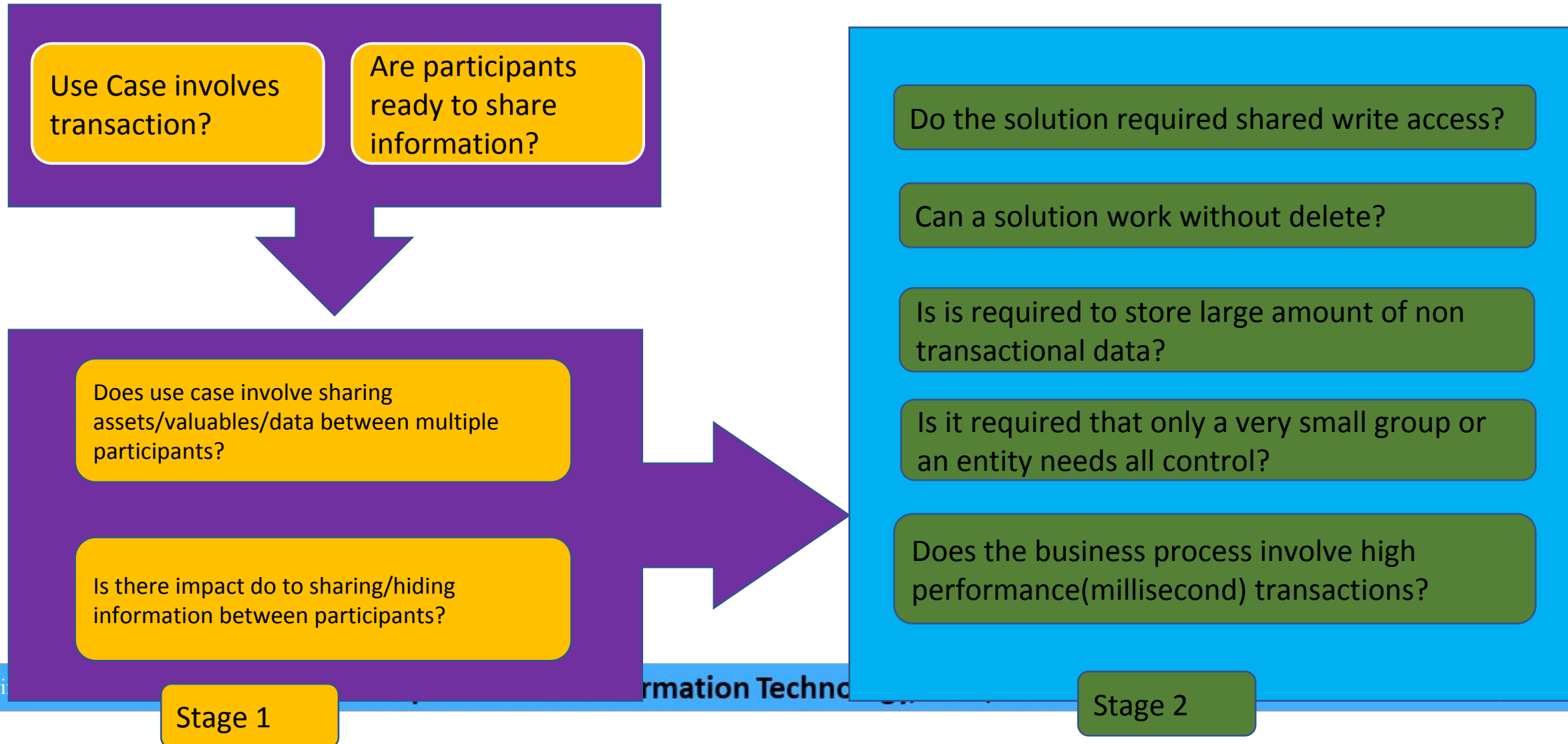
Collaboration between competing stakeholders

Change in business process

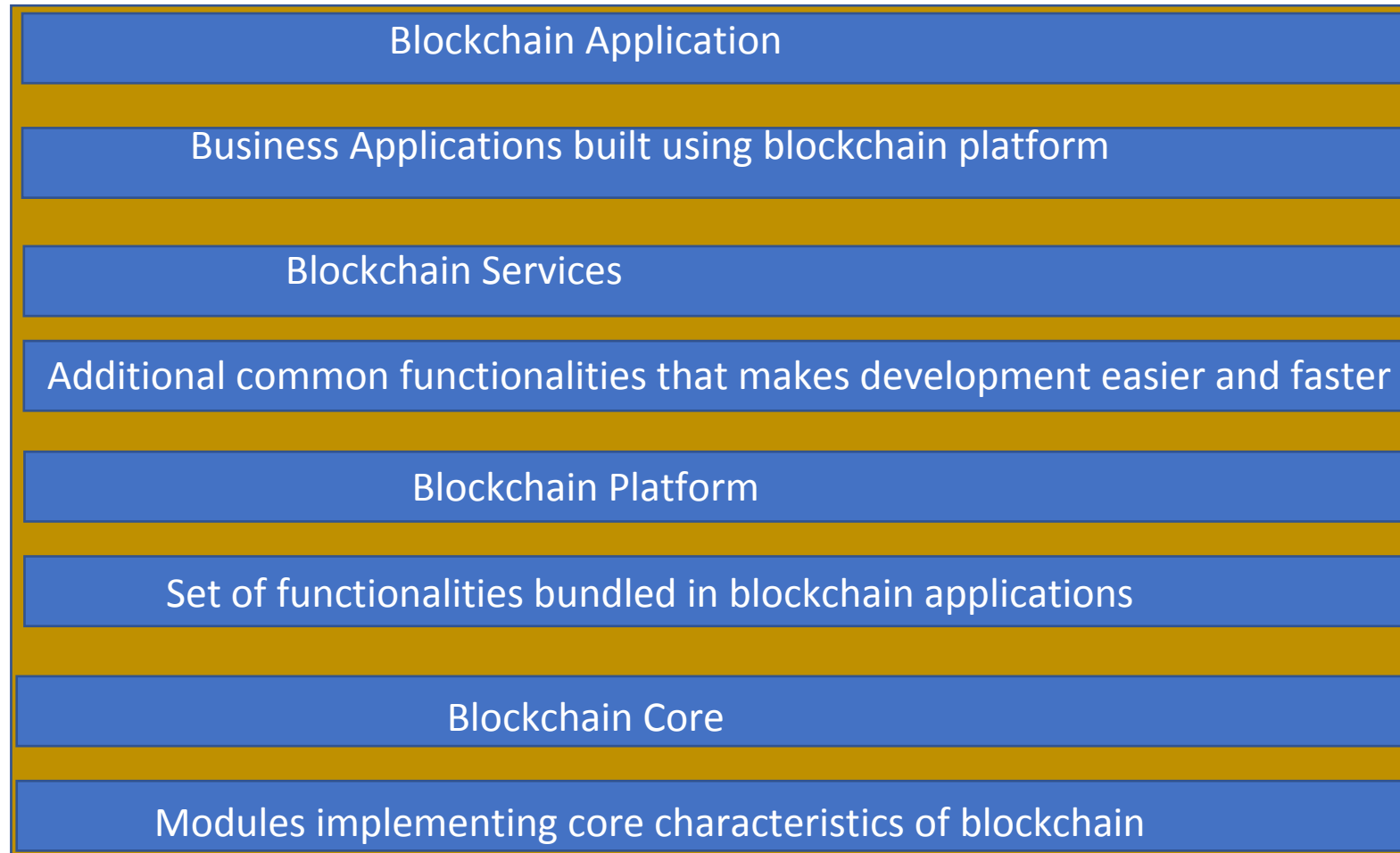
Cost of implementation

Time-to-Market is high

# Blockchain Relevance Evaluation Framework

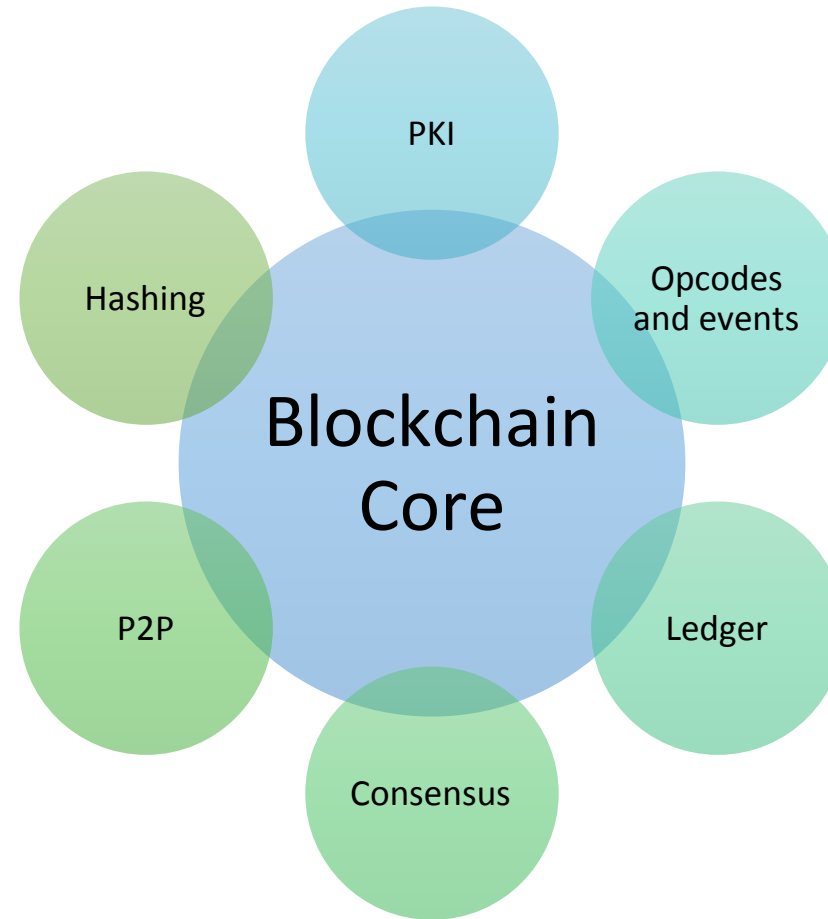


# Blockchain solution reference architecture

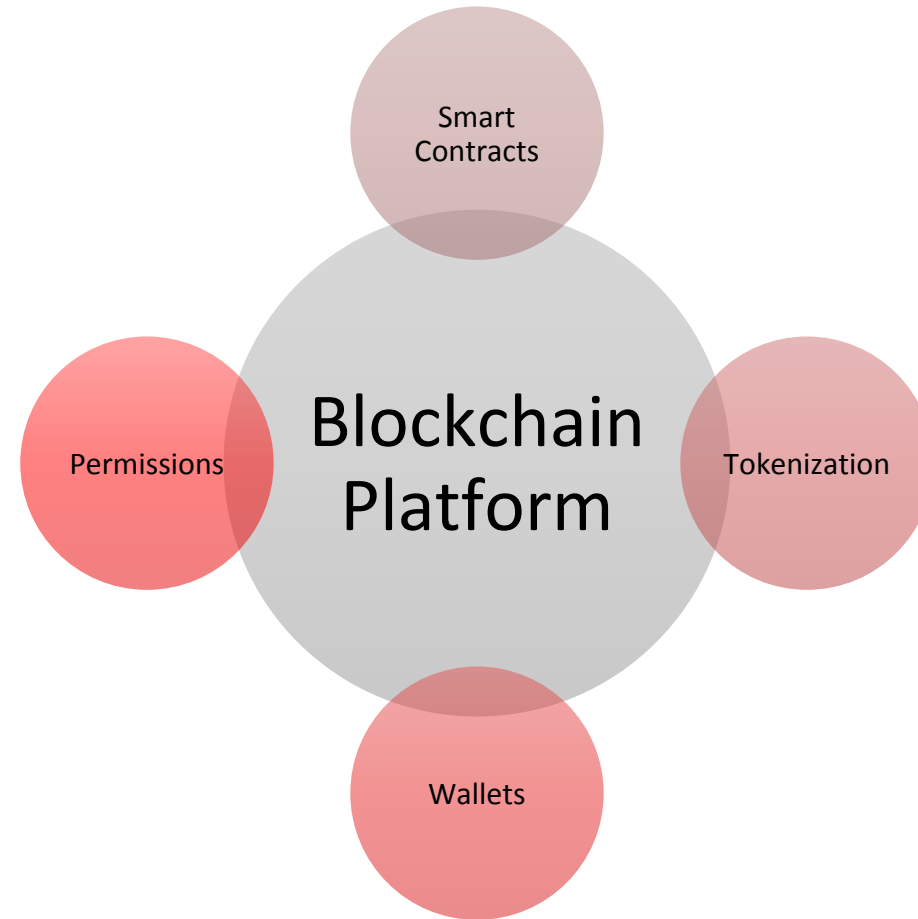


# Lecture 18

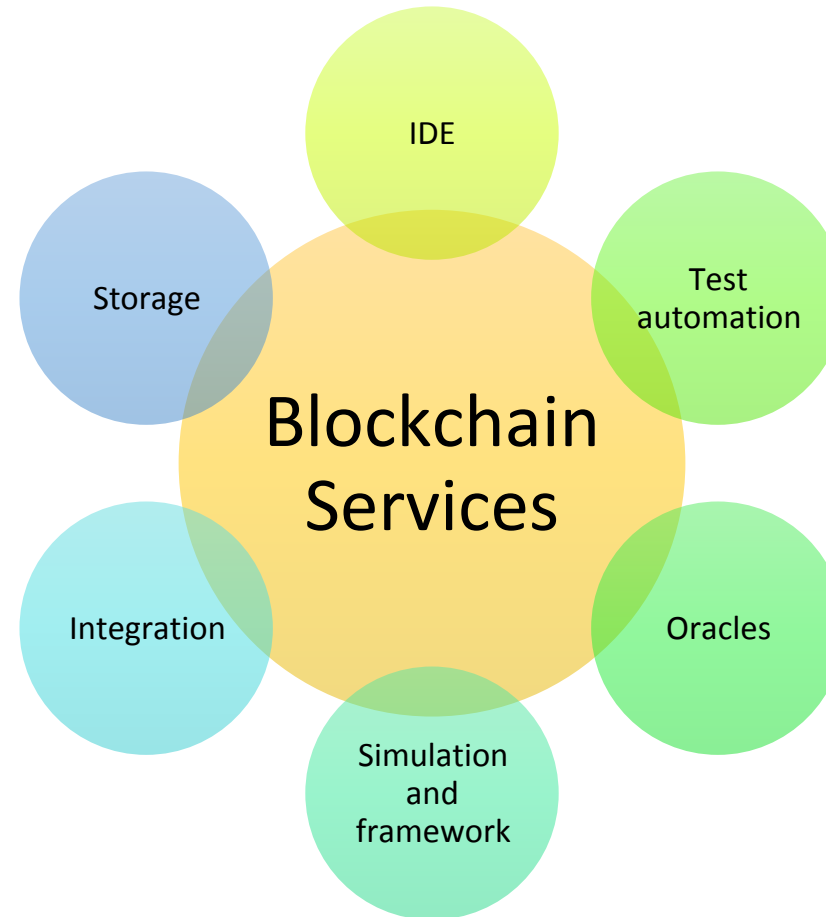
# Blockchain Core



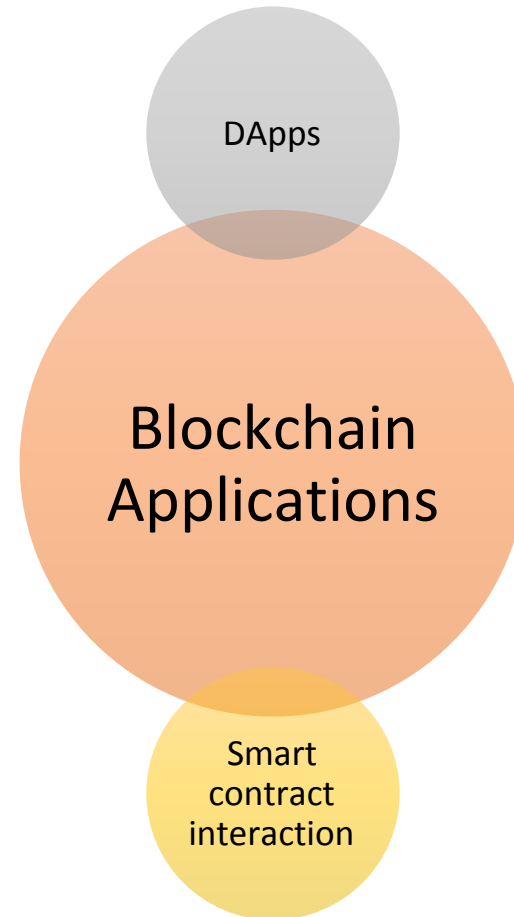
# Blockchain Platform



# Blockchain Services



# Blockchain Applications





# Types of Blockchain applications

Fully decentralized	Simple blockchain solutions	Enterprise solutions	Enterprise blockchain ecosystem
<ul style="list-style-type: none"><li>• Mostly public blockchains</li><li>• Cryptocurrency and tokens</li></ul>	<ul style="list-style-type: none"><li>• Generally private network</li><li>• Start as POC ,then evolve to enterprise solutions</li></ul>	<ul style="list-style-type: none"><li>• Established with Proof of value</li></ul>	<ul style="list-style-type: none"><li>• More stakeholders start joining</li><li>• Deliver value to end user</li><li>• Might support IOT etc</li></ul>

# Lecture 19

# Cryptographic tokens

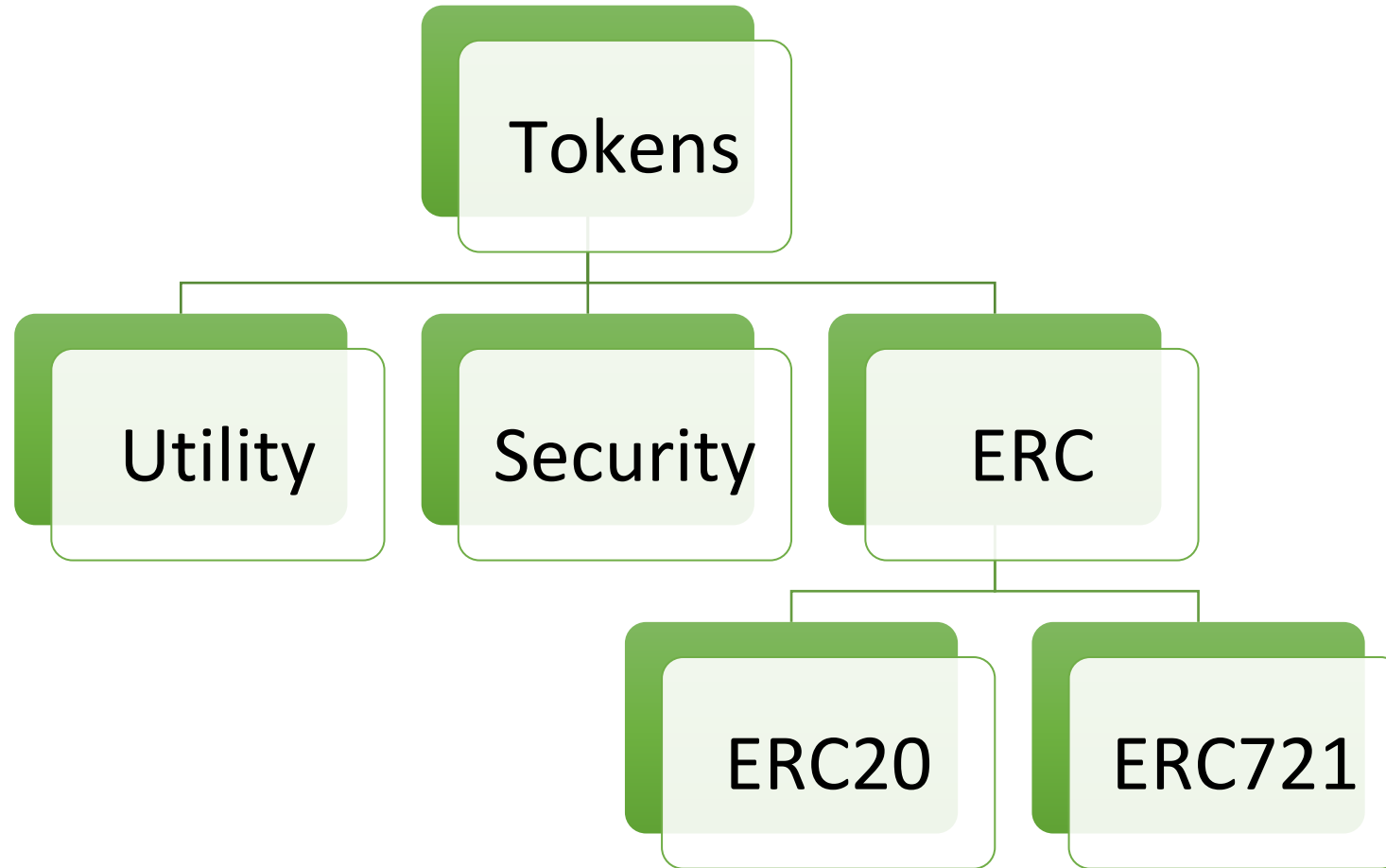
- A cryptographic token represents a programmable asset that is created and managed by a smart contract.
- The smart contract decides the number of units of tokens to be created and handles the transactions involving the token and each token holder's balance.
- While a cryptocurrency such as ETH will be available for all the applications implemented on Ethereum, the cryptographic token is implemented by a particular application and can be accessed and controlled only by the smart contract belonging to that particular application.
- There is difference between token and coin.

- Coins are native to the platform and are accessible to all applications developed using the platform whereas tokens are accessible to the application that creates tokens on the platform.
- In short, coins are out of the box currency provided by the platform whereas tokens are not out of the box, they are explicit implementations by blockchain applications and smart contracts.
- E.g. On Ethereum an Ether unit can be considered as coin, while cryptokitty is a token.
- For practical purposes, tokens can exist on any blockchain platform that decides to support it.
- Not all blockchain platform support out of the box currencies and such platforms cannot have coins.
- Also, it is not practical to implement tokens on blockchain platform that do not support smart contracts.

- Tokens can not be listed on an exchange without some customization on the exchange code.
- These tokens can not be transferred between different wallets or used in applications other than the one that created it.
- Here, Ethereum Request for Comment (ERC) standard is handy.
- Ethereum Improvement Proposal (EIP) is a design document that provides information to the community or describes a new feature or a new process etc.
- The EIP document should contain justification for introducing a new feature and detailed technical specification for implementing that feature in Ethereum platform.
- The author of the new feature is responsible for getting acceptance from the community.

- EIP is categorized into three important tracks.
- 1. Standard track-It describes changes that impact most of the Ethereum implementations. Standard track can be divided into following categories.
  - A. Core-It describes improvements in consensus forks.
  - B. Networking-It describes improvements to network protocol specifications.
  - C. Interface-It describes improvements to client specifications and standards.
  - D. ERC- It describes application level standards and conventions.
- 2. Meta track-It describes process change requests.
- 3. Informational track-It provides guidelines or information to Ethereum community.

# Cryptographic tokens



- Utility tokens-They are user tokens that provide access to the products or services offered by the company. They can help in driving the internal economy within a blockchain project. They can be used to provide the advantages to the holders of the utility tokens. The holders can be privileged to do voting on important decisions on the blockchain project. E.g Golem network token(GNT) provides the holders access to the Golem ecosystem. GNT uses personal computer to offer services that are currently done by servers. People using these services can pay the providers using GNT.



- Security tokens-They represents legal ownership of a physical or digital asset.
- They are generally tied to the company's profit or loss valuation.
- These tokens are heavily regulated and failing to comply with regulations shall have serious consequences which can even lead to complete shut down of blockchain project.
- E.g Siacoin,Blockstak STX token

- ERC tokens-ERC tokens define rules that will enable the tokens to be handled and exchanged between various Dapps and wallets.
- ERC20-It defines the rules that need to be followed while implementing fungible tokens.
- A fungible token is a token that is not unique, something that can be easily replaced with something identical and it is easily interchangeable.
- All the fiat currencies are fungible. A dollar can be easily interchanged with some other dollar bill, a rupee note is the same as that of another, what matters is the value and not the physical paper.
- Similarly bitcoin or other cryptocurrencies are fungible coins in the sense that overall ownership matters and not which coin is held by whom.
- Fungible tokens can be easily interchanged during transactions. Fungible tokens can be created on the chain.
- EOS is an ERC20 token that is popular in the market on Ethereum blockchain network and millions of ERC tokens are in circulation.
- ERC tokens are used to represent the currency, shares of the company, loyalty points, gold certificates etc.

- ERC20 standard defines six mandatory functions that need to be implemented by the smart contract that creates and manages tokens.
- It also involves three key optional attributes “name”, “Symbol” and “decimals”.
- Mandatory functions are as follows:-
  - totalSupply
  - balanceOf
  - Transfer
  - transferFrom
  - Approve
  - allownace

# ERC721 tokens

- ERC721 tokens- They defines the rules that need to be followed while implementing non-fungible tokens(NFTs).
- A NFT is a unique token and holding of these tokens needs to be managed. Such tokens needs can not be interchanged without changing the ownership. In this case holding a physical asset is important. e.g real estate property. Here it is more important which property someone is holding than the total no of units one holds.

<https://youtu.be/NNQLJcJEzv0>

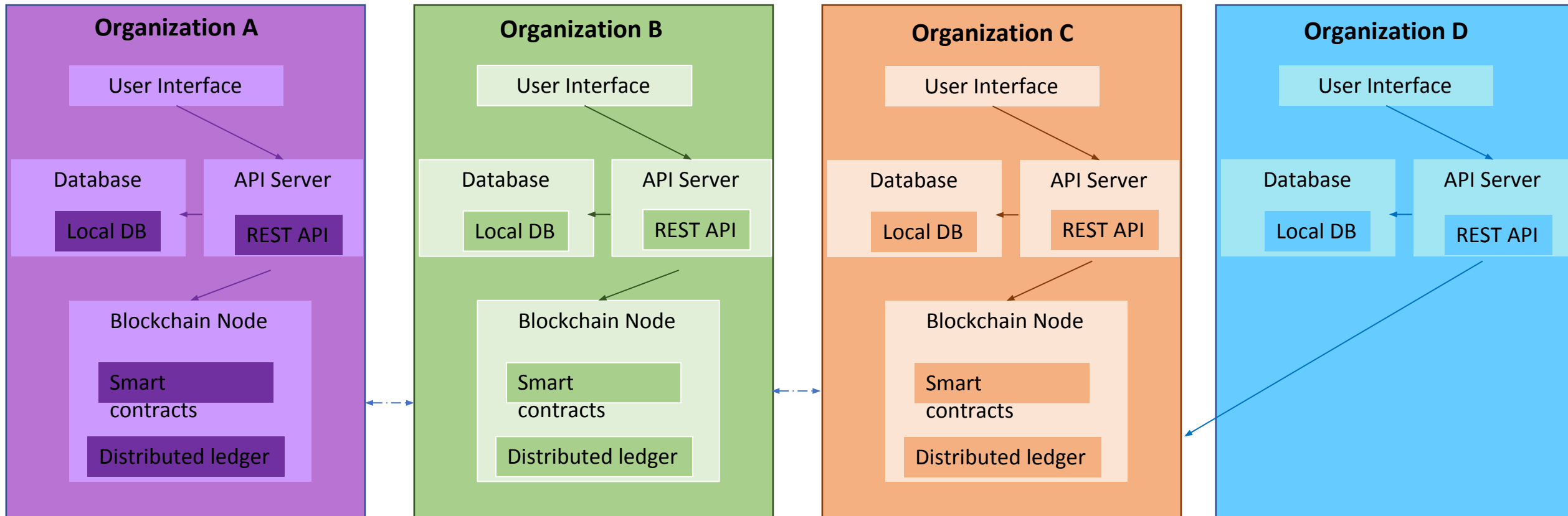
<https://youtu.be/FkUn86bH34M>

<https://youtu.be/d00bydAilx0>

- ERC721Mandatory functions are as follows:-
  - totalSupply
  - balanceOf
  - ownerOf
  - transferFrom
  - safeTransferFrom
  - approve
  - setApprovalForAll
  - GetApproved

# Lecture 22

# Typical Solution architecture for enterprise use case



# Types of blockchain solutions

## Value transfer

- P2P payments
- Cross border payments
- Trade finance
- Remittance
- Cryptocurrency
- Insurance payments
- Loyalty points

## Provenance

- Supply chain traceability
- Counterfeit detection of drugs
- Clinical drug sample movements
- Precious wood tracking
- Ethical sourcing of diamonds

## Identity Management

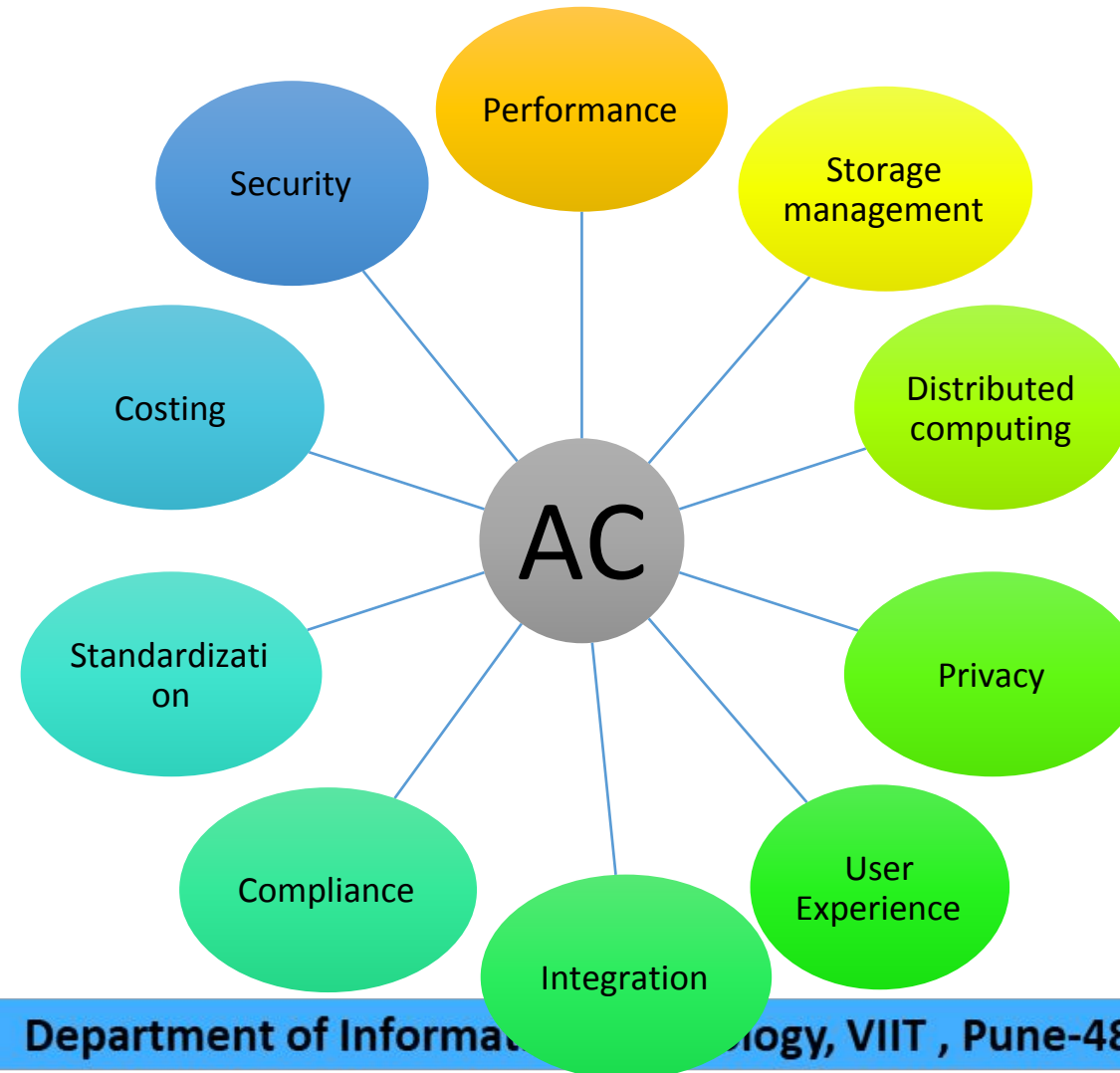
- Identity verification solutions
- Non custodian login solutions
- Self sovereign identity
- Real estate use cases

## Data sharing

- Electronic health records
- Provider data management



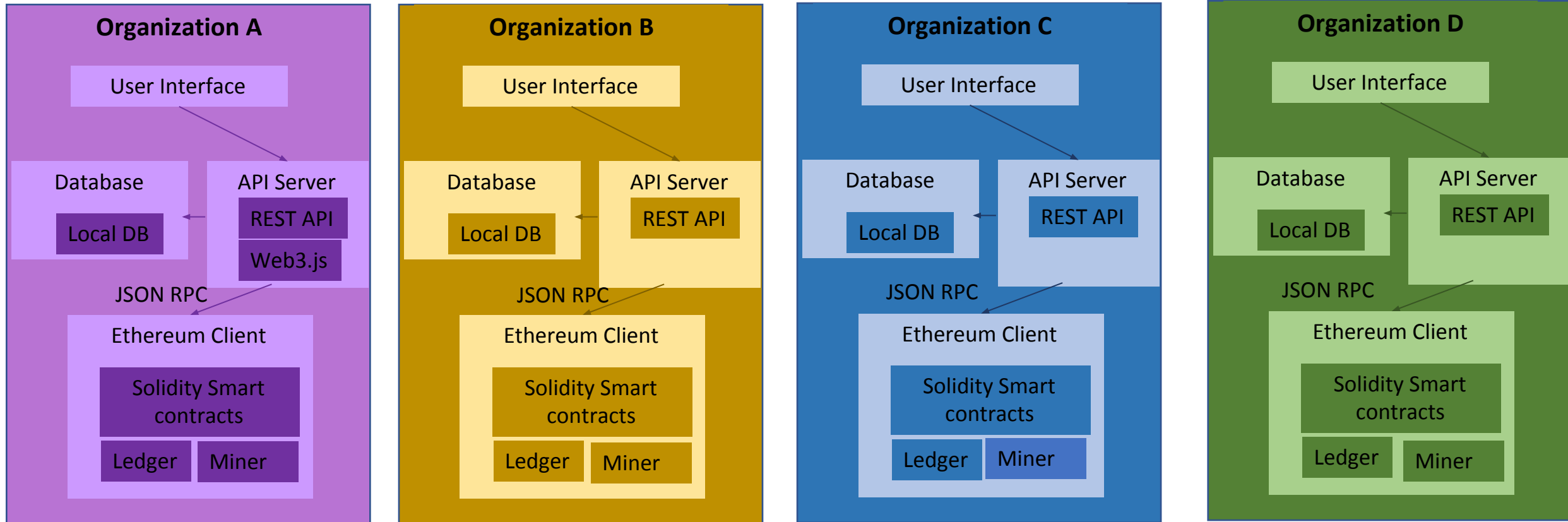
# Architecture considerations



# Architecture with blockchain platforms

- Ethereum Architecture
- Hyperledger Fabric Architecture

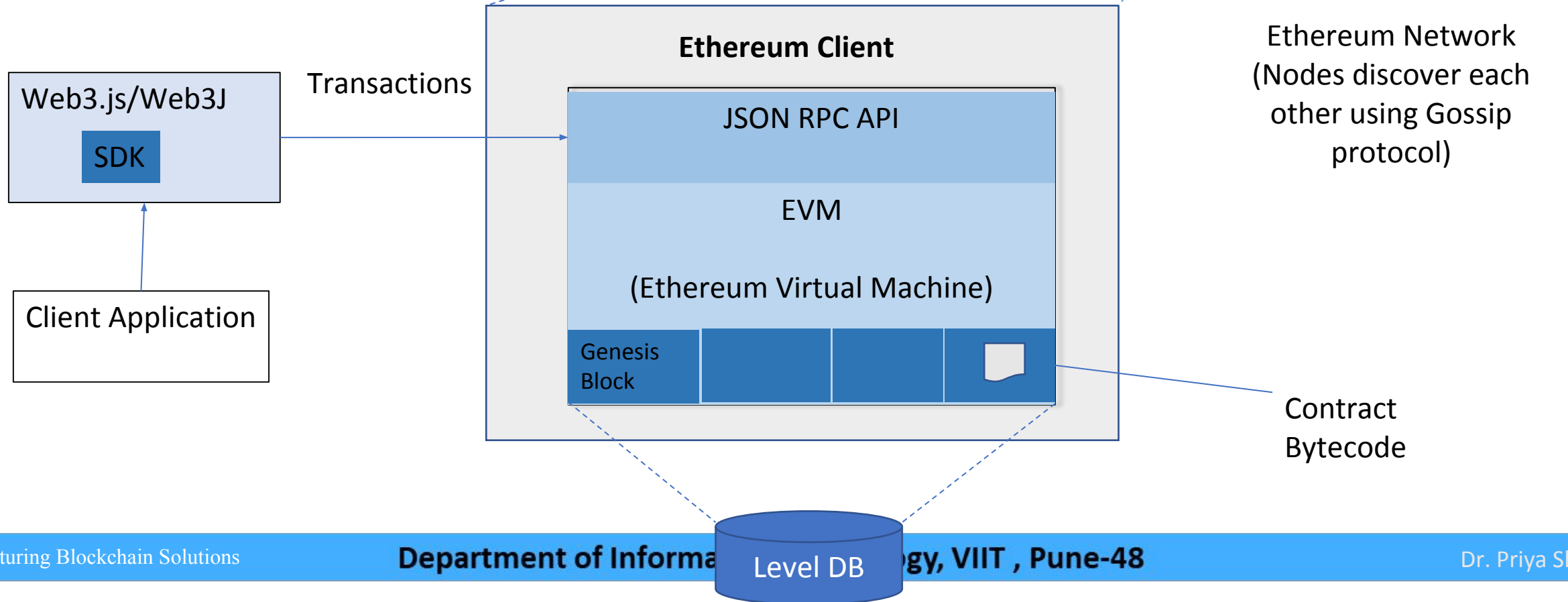
# Ethereum typical solution architecture



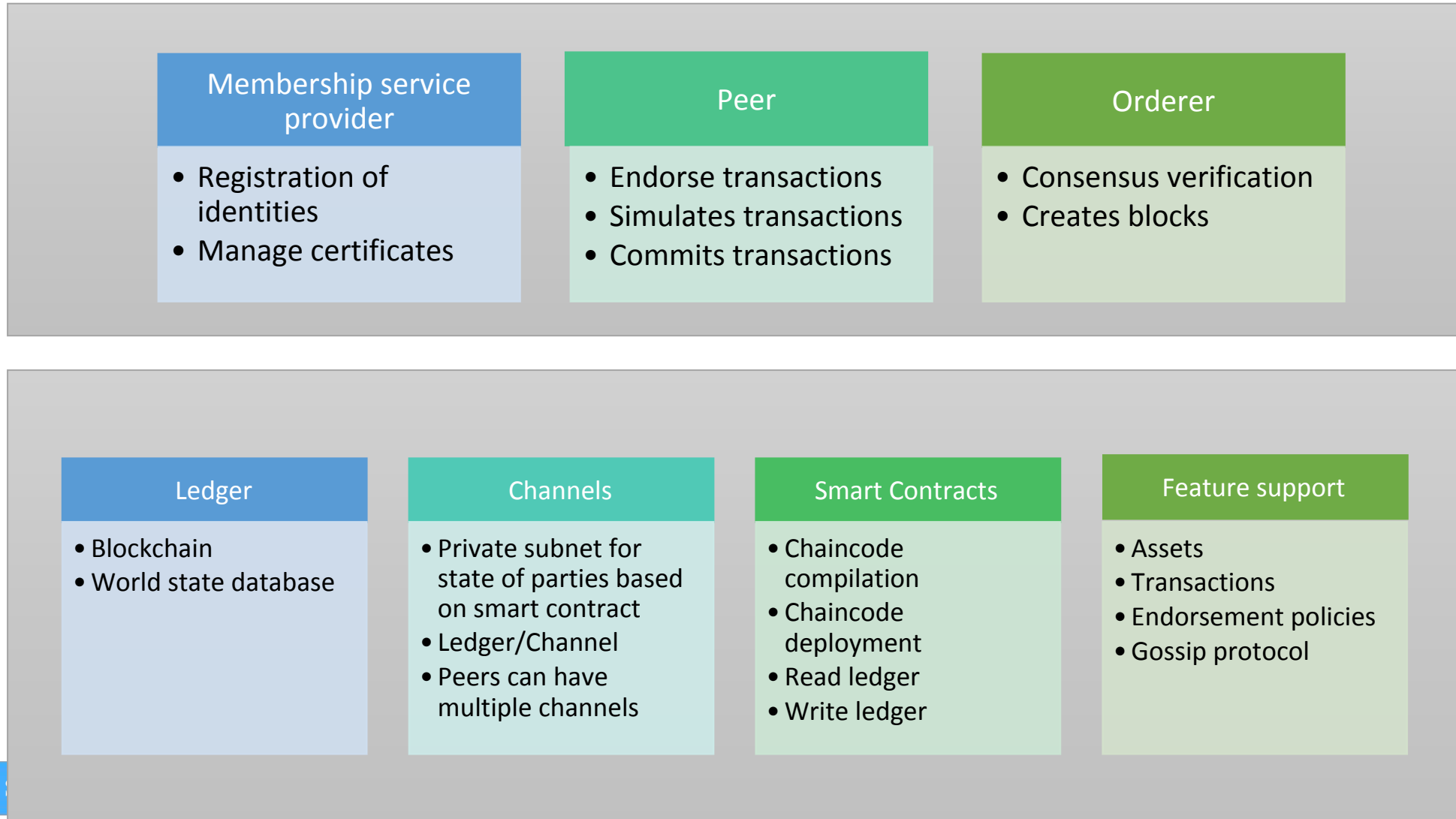


# Ethereum Solution components

Ethereum client connects to the network using a set of preconfigured Boot strap nodes

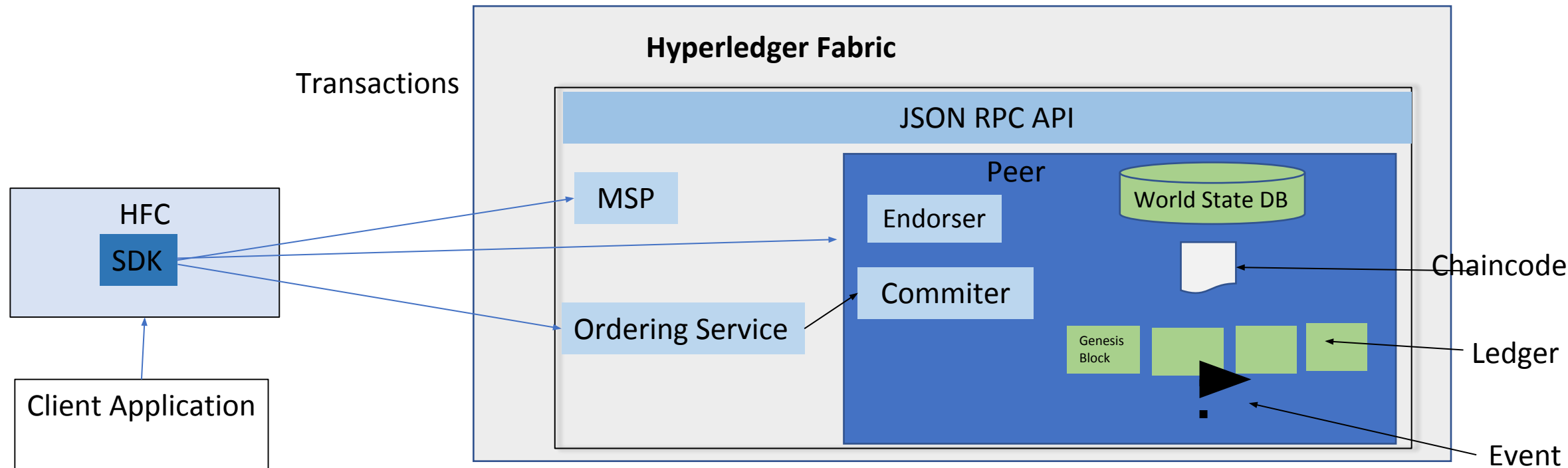


# Hyperledger fabric components



# Hyperledger Solution Components

Ethereum client connects to the network using a set of preconfigured Boot strap nodes



# Selection of Blockchain platform

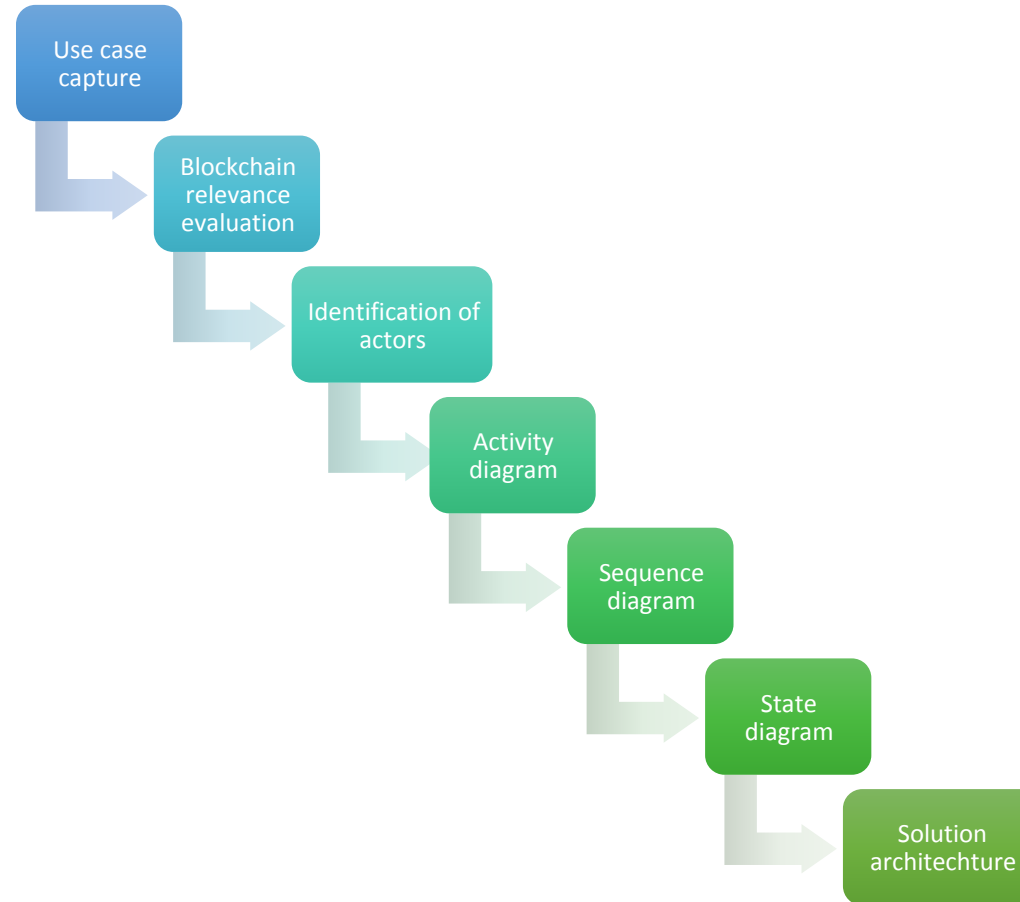
- Complete understanding of business process
- Scope of business functionality that will be implemented on blockchain.
- Type of blockchain network needed to implement the functionality.
- The functionalities provided by various blockchain platforms that would fulfill business requirements.
- Types of actors involved in the network.

# Selection of Blockchain platform

- Once a blockchain platform is selected many other decisions are to be made
  - Types of tools -e.g Truffle framework for Ethereum, Compositor for Hyperledger etc.
  - Programming language-e.g Solidity for Ethereum, Go for Hyperledger
  - Supporting technologies-e.g IPFS for decentralized storage



# Approach for designing blockchain applications



# Thank You