

FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGIES (ITUA40181B)

Unit I

Introduction to Blockchain

Dr. Priya M Shelke


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

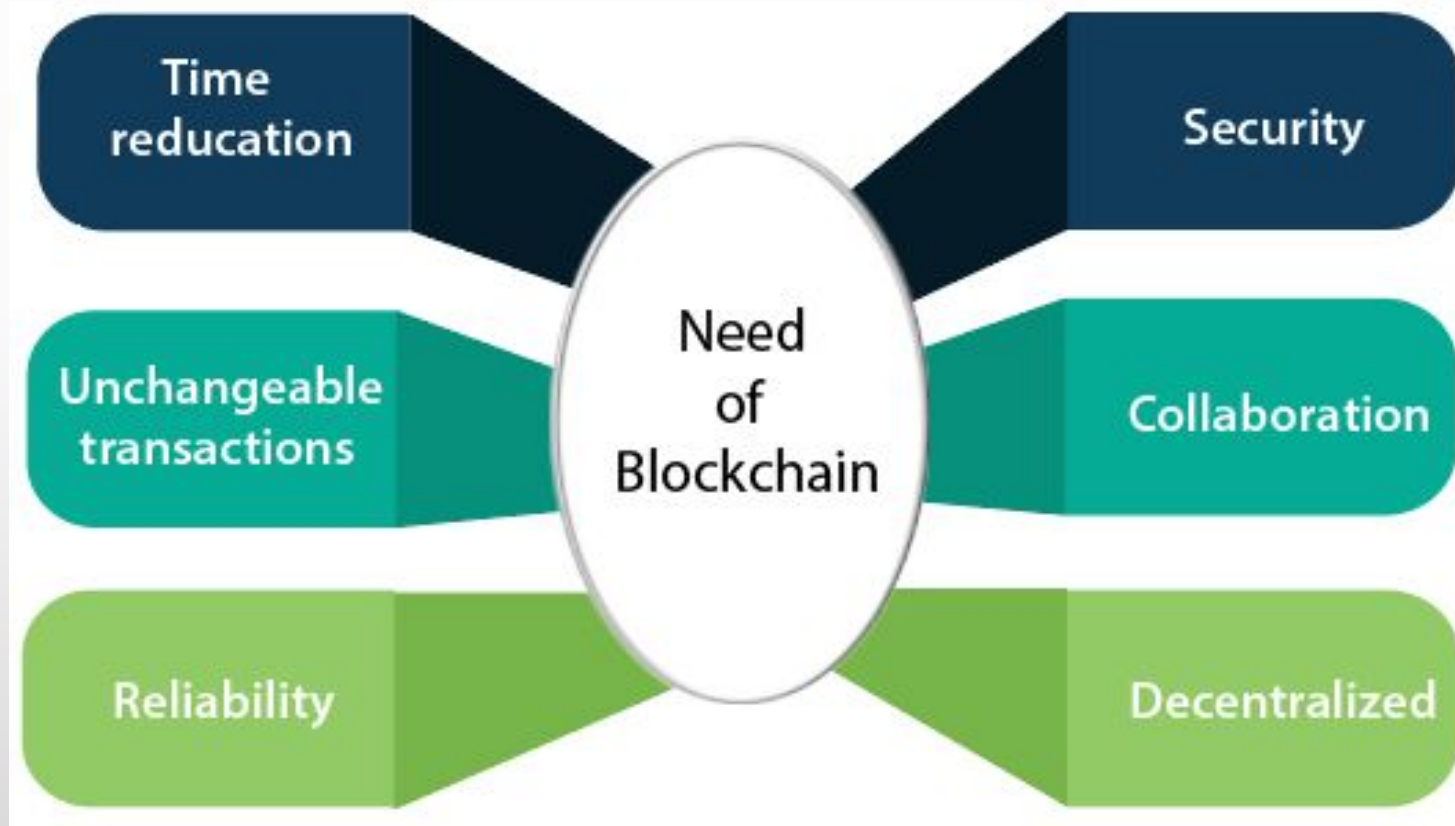
We need blockchain because..

- 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

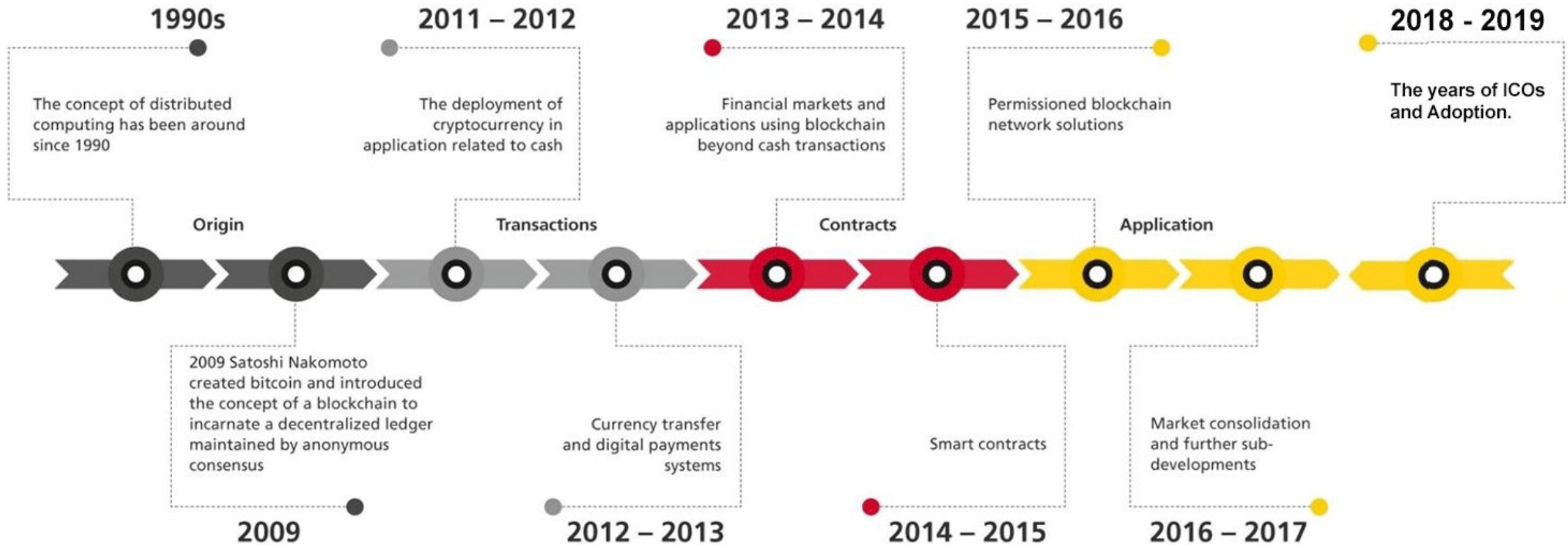
History of Blockchain

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 knew 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.

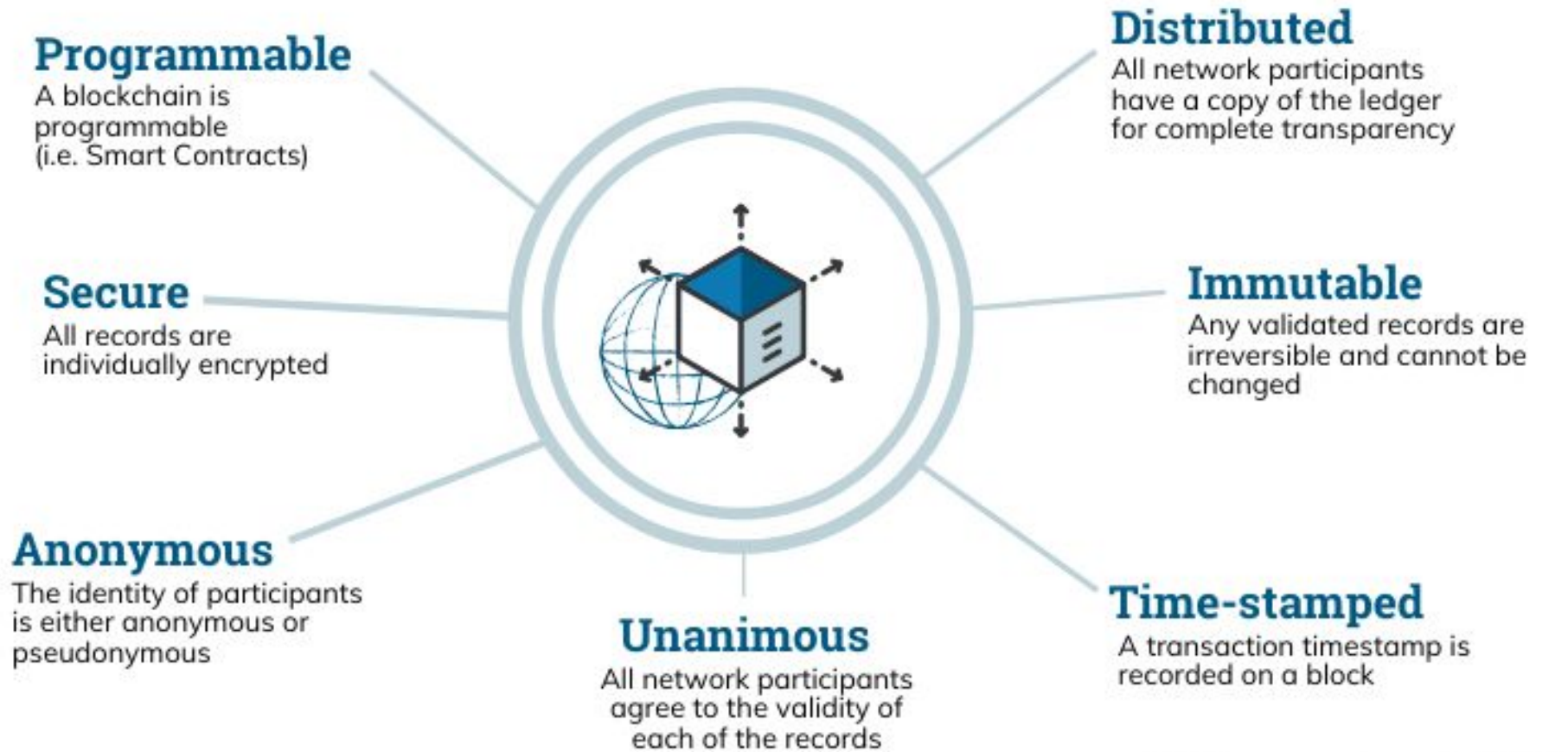
So how does a blockchain differ from a database?

- **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)



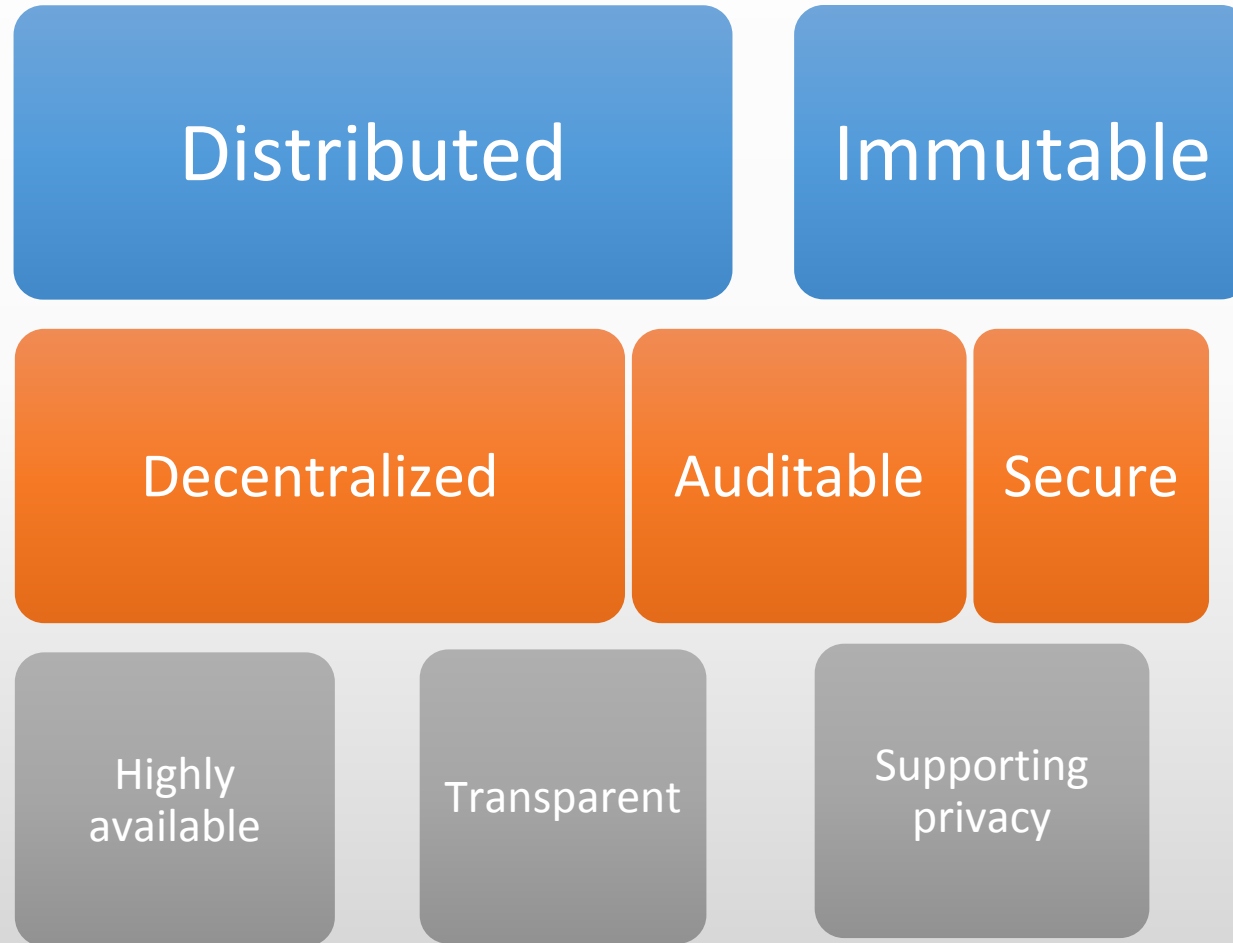
© Euromoney Learning 2020

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

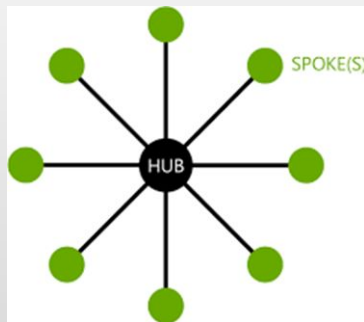
- As with existing databases, Blockchain retains data via transactions
- The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.
- The transaction is, immutable, or indelible
- 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....

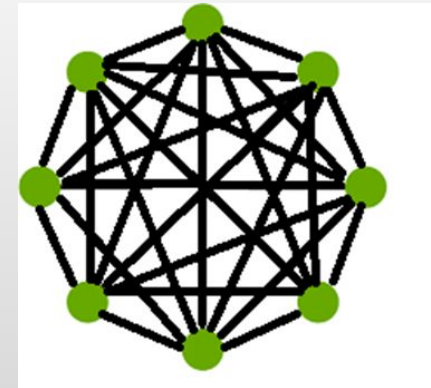
Decentralized

- 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

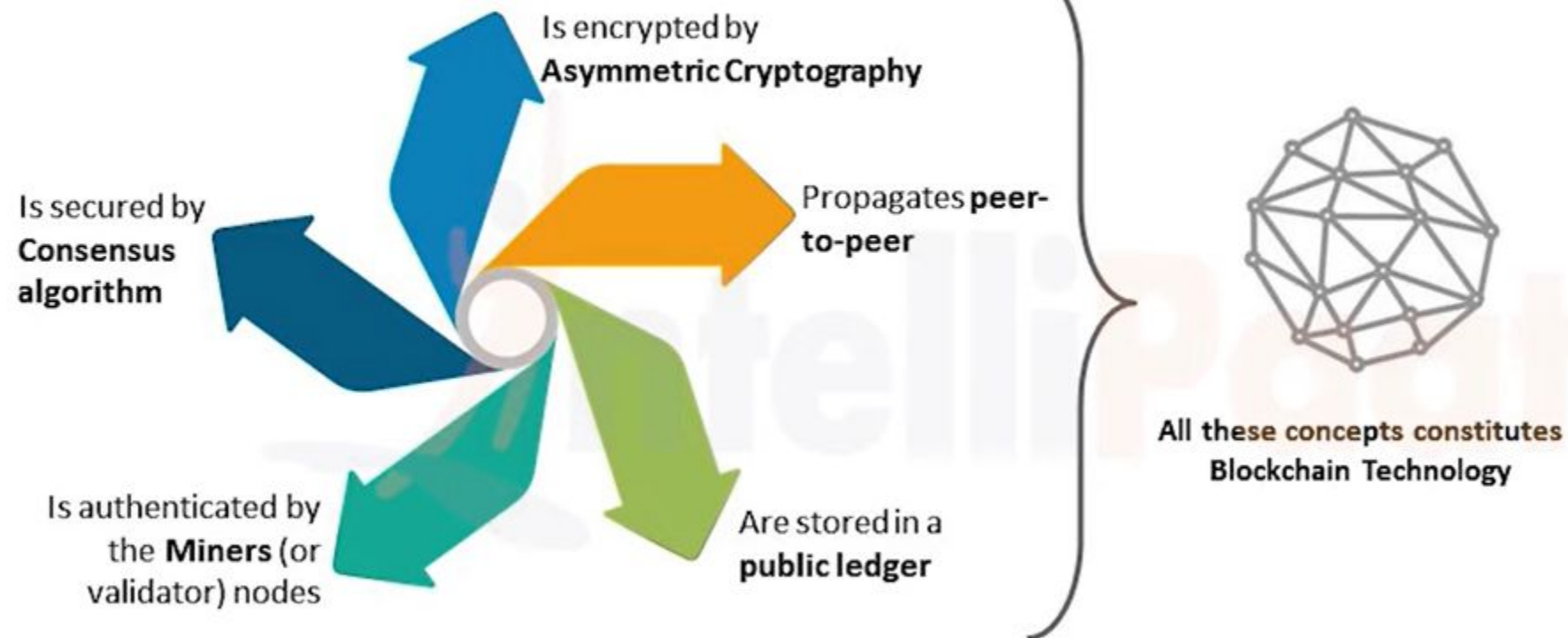
- In a blockchain, all the participants have a copy of ledger entries.
- Entries to the ledger are created by preset rules that are defined at network configuration.
- This sharing of data and logic encourages transparency in blockchain.

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

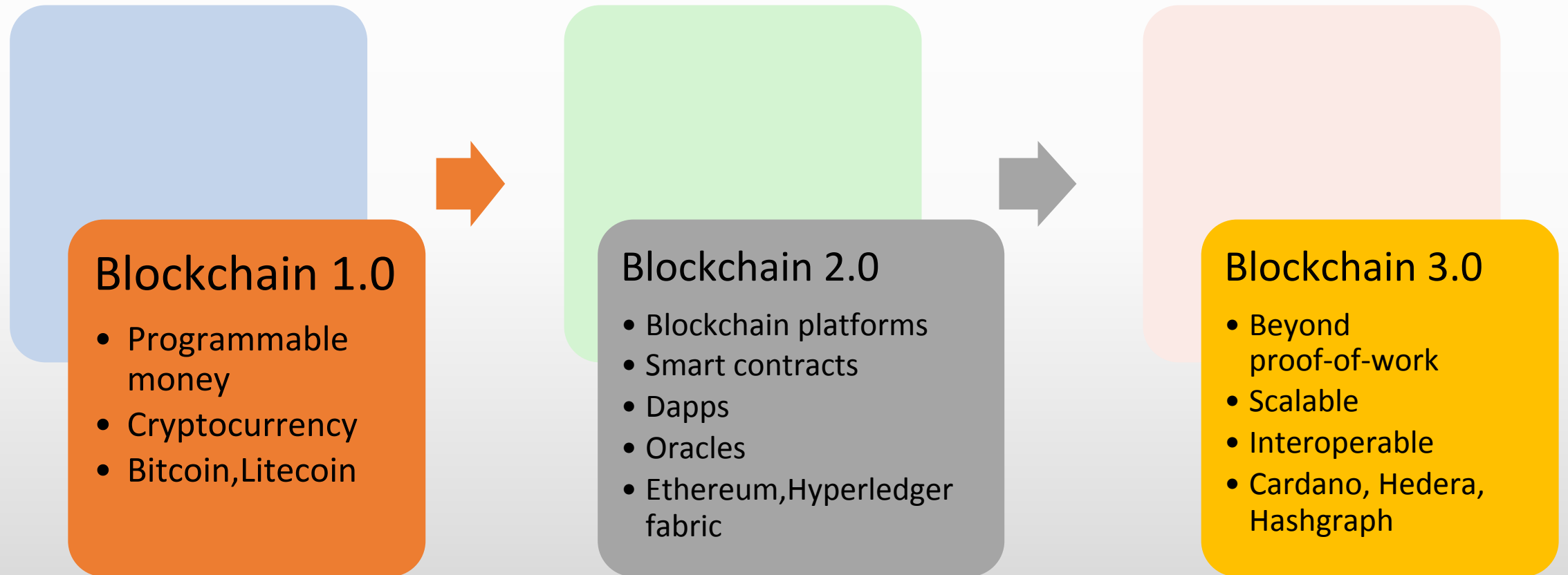
Data is not owned or controlled by the server or any single entity

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.

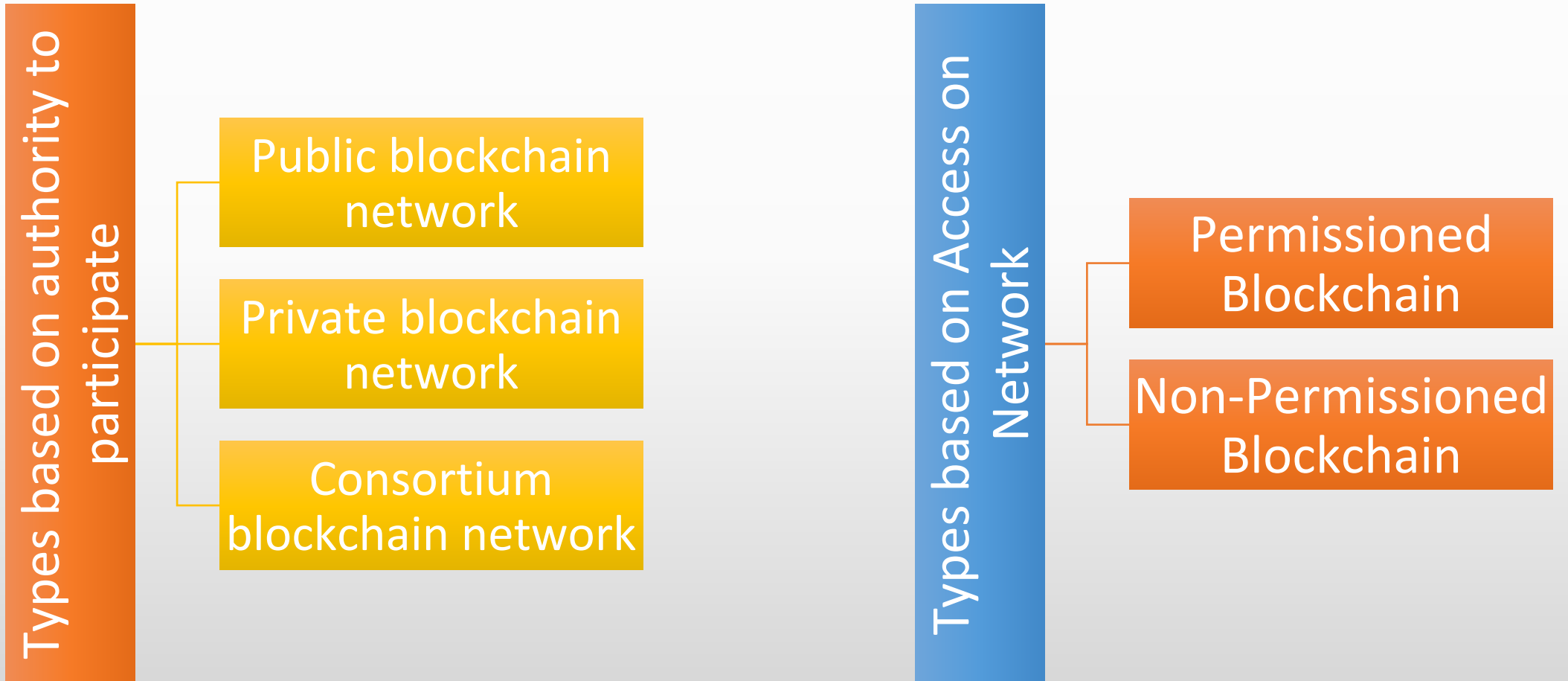
Hybrid consortium-example

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

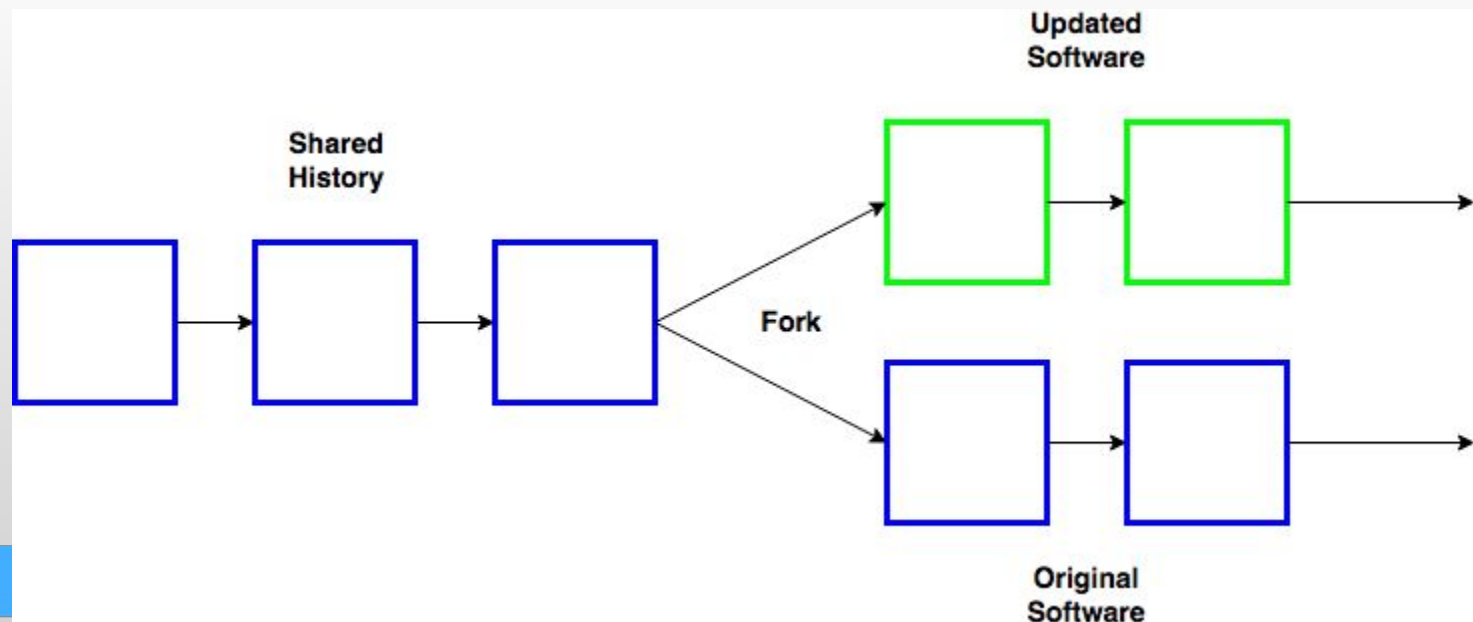
- Reads and writes are governed based on access permissions granted to the users.
- It falls in between public and private b. networks
- Super users hold the privilege to add or remove and grant access to members
- Limited set of users participate in consensus
- e.g Ripple

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.

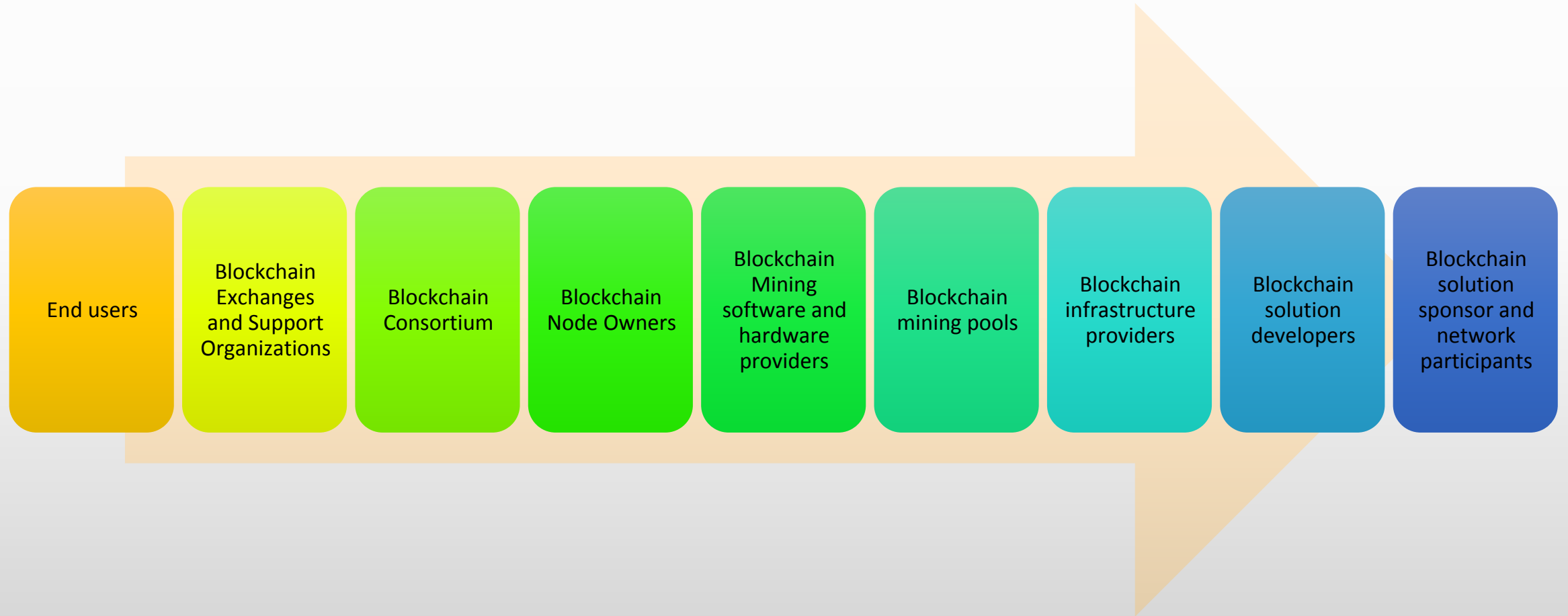
Testnet

- 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 Ξ) 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