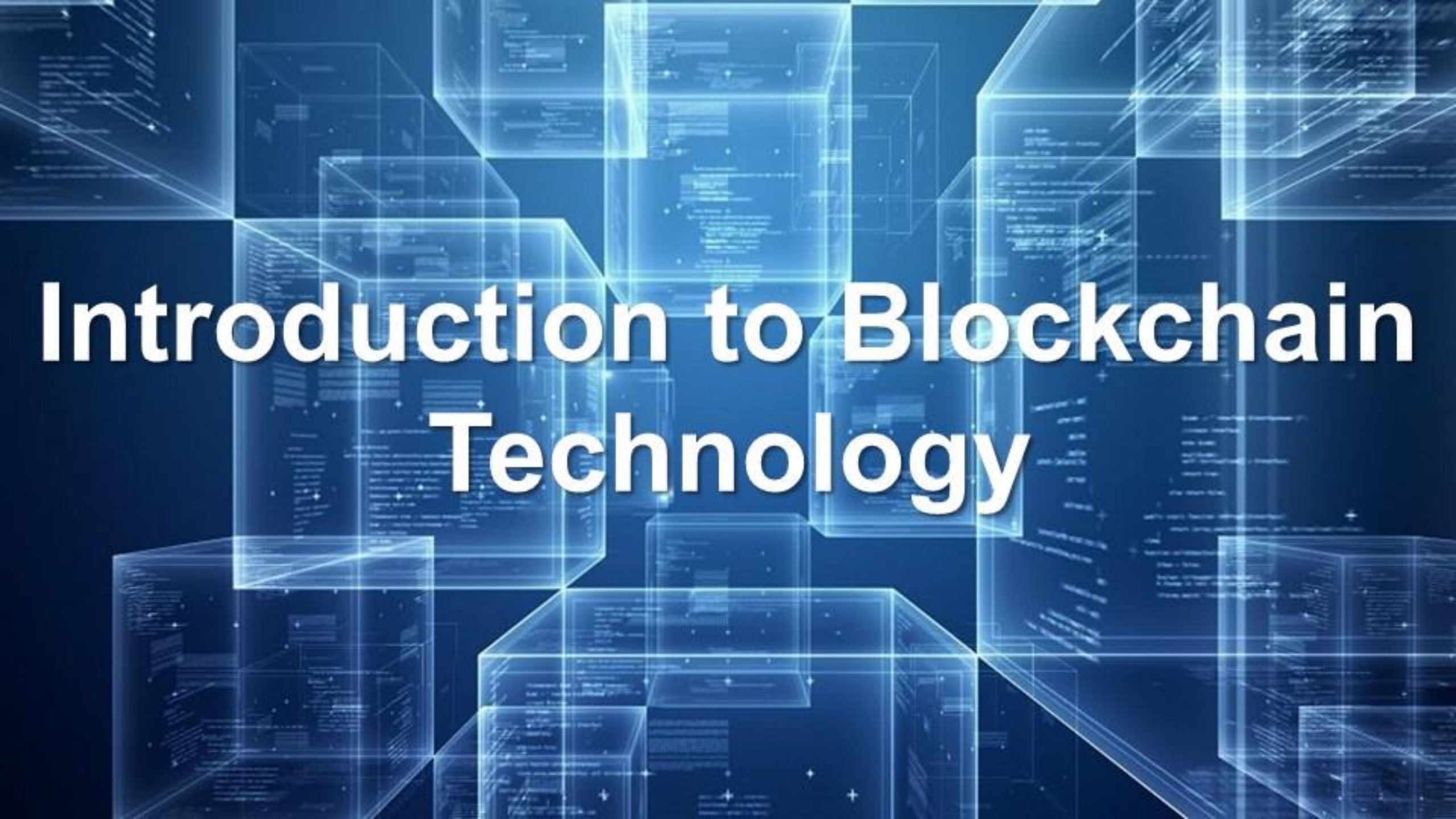

Introduction to Blockchain
Technology

AGENDA

I. Motivation

II. What is a Blockchain ?

III. Why use Blockchain ?

IV. Evolution of Blockchain Technology

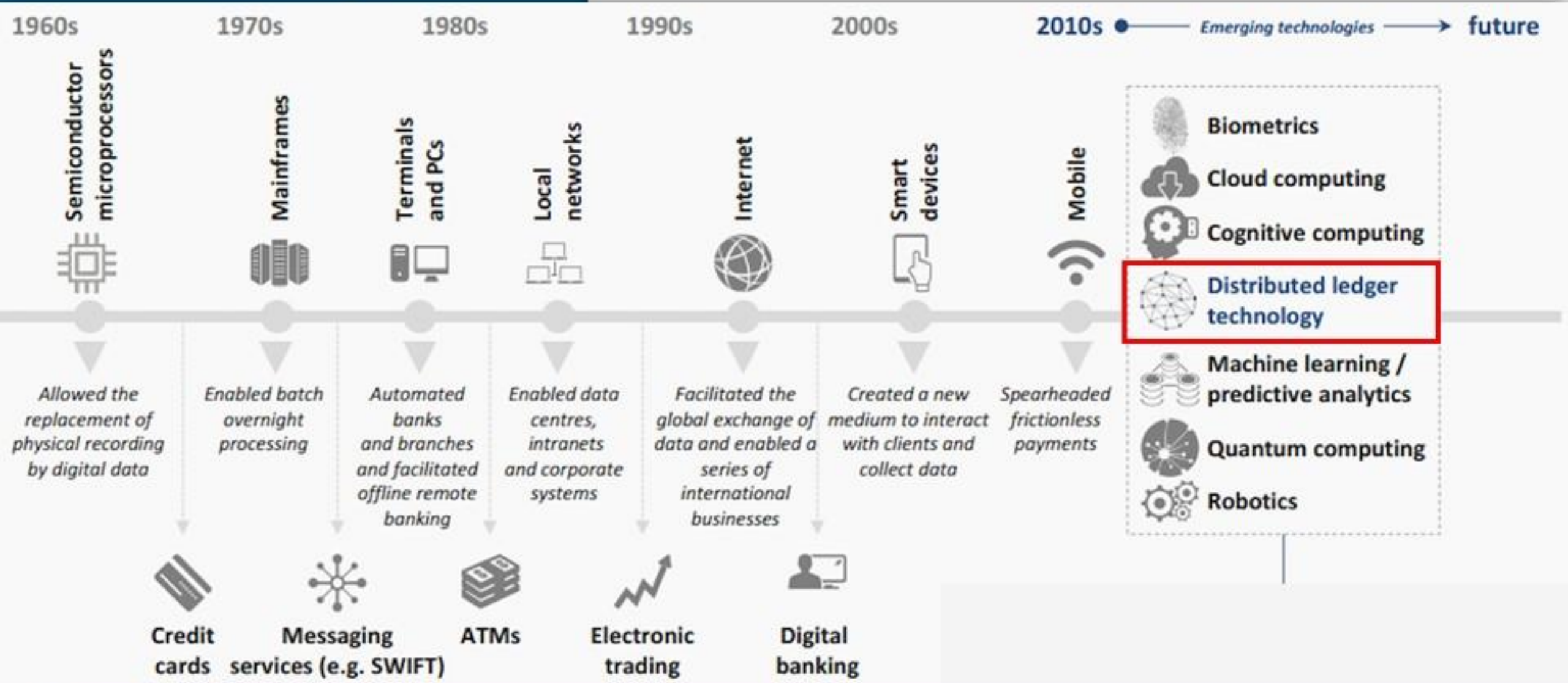
What is a "Blockchain" ?

https://tuoitre.vn/bat-song-blockchain-1436355.htm

"Blockchain có thể là tương lai của Internet – Internet của Niềm Tin

Ý tưởng của Blockchain rất 'đẹp', nó không chỉ mang tính đột phá mà còn được mệnh danh là phiên bản **Internet 2.0 - Internet của NIỀM TIN**. Nếu như người ta cho rằng khái niệm **Chủ Nghĩa Hoàn Hảo** hay CNXH không tưởng với bốn yếu tố: ***An Toàn, Công Bằng, Minh Bạch, Dân Chủ*** là không thực tế thì Blockchain có thể hiện thực tinh thần chủ nghĩa này trong *Thế Giới Số*. An toàn bởi hệ thống không sợ bị tấn công, đặc biệt là tấn công đơn điểm; minh bạch bởi các tập luật, dữ liệu, quy trình tương tác cho đến source code đều minh bạch; dân chủ bởi người tham gia làm chủ mọi quyết định, được cập nhật mọi thông tin trong hệ thống, mọi ý kiến đều được tôn trọng và mọi người, kể cả tác giả người sáng lập hệ thống cũng chỉ là một thành viên không có gì hơn người khác"

Landscape


1960s
1970s
1980s
1990s
2000s
2010s
Emerging technologies
future
Semiconductor microprocessors
Mainframes
Terminals and PCs
Local networks
Internet
Smart devices
Mobile
Allowed the replacement of physical recording by digital data
Enabled batch overnight processing
Automated banks and branches and facilitated offline remote banking
Enabled data centres, intranets and corporate systems
Facilitated the global exchange of data and enabled a series of international businesses
Created a new medium to interact with clients and collect data
Spearheaded frictionless payments
Credit cards
Messaging services (e.g. SWIFT)
ATMs
Electronic trading
Digital banking
Biometrics
Cloud computing
Cognitive computing
Distributed ledger technology
Machine learning / predictive analytics
Quantum computing
Robotics

Motivation

The First Use Case for Blockchain

"Bitcoin is the first decentralized crypto-currency that uses underlying characteristics of Blockchain technology"

Bitcoin

≠

Blockchain

Bitcoin is an implementation of technology

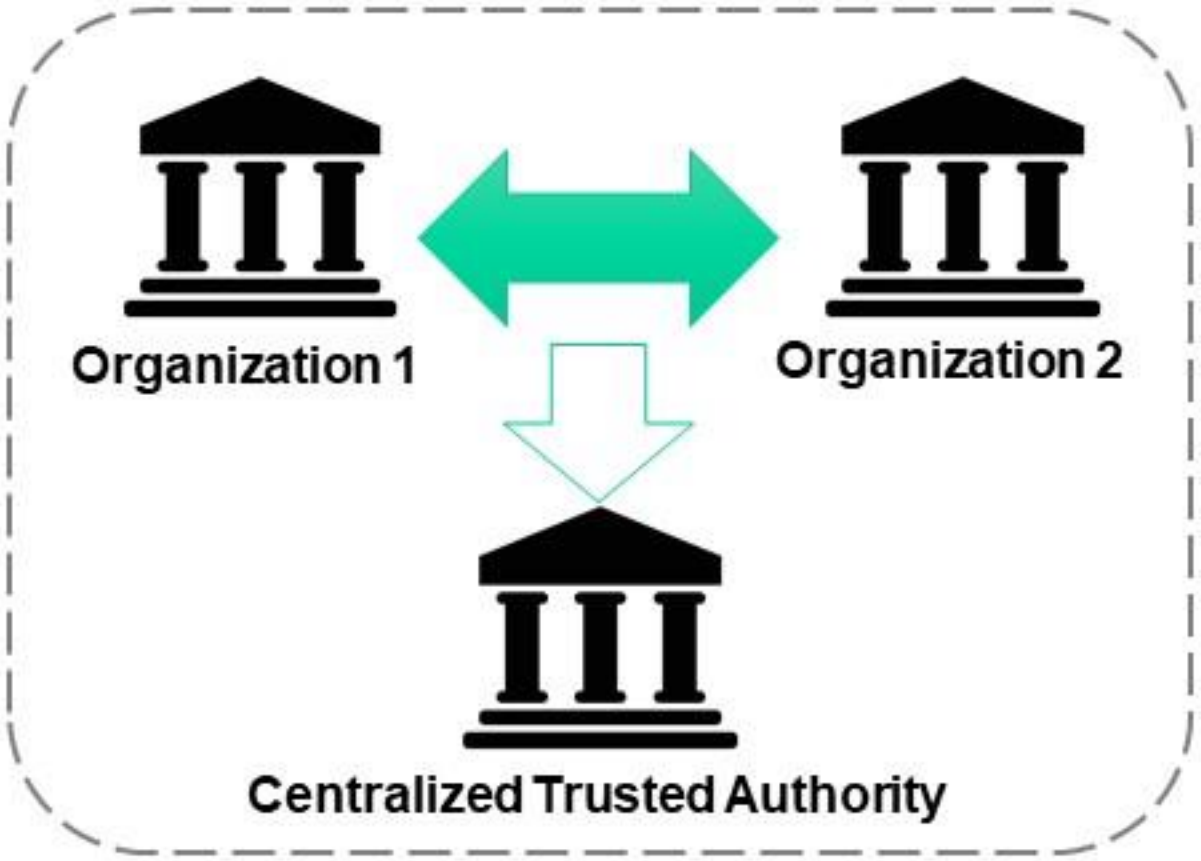
Blockchain is the core technology

Internet Challenges

- Digital content - Text, Graphic, Video, Audio, Data…
  - Easy creation of digital content
  - Easy duplication (make a copy)
  - Easy distribution
  - ➔ BUT difficulty to protect copyright or original of digital content

Internet Challenges

- Centralized approach (Client-Server)



Traditional trusted environment

Trusted Market

Trusted Payment

Trusted Authentication

Case-study: Centralized Approach

Traditional trusted environment

- Database is controlled by a central and trusted third-party.
- The more complex the flow, the more middlemen required.
- Fees are high (Fixed Fee + 1-3%), settlement is slow (multiple days).
- Single point failure.
- Hackable.

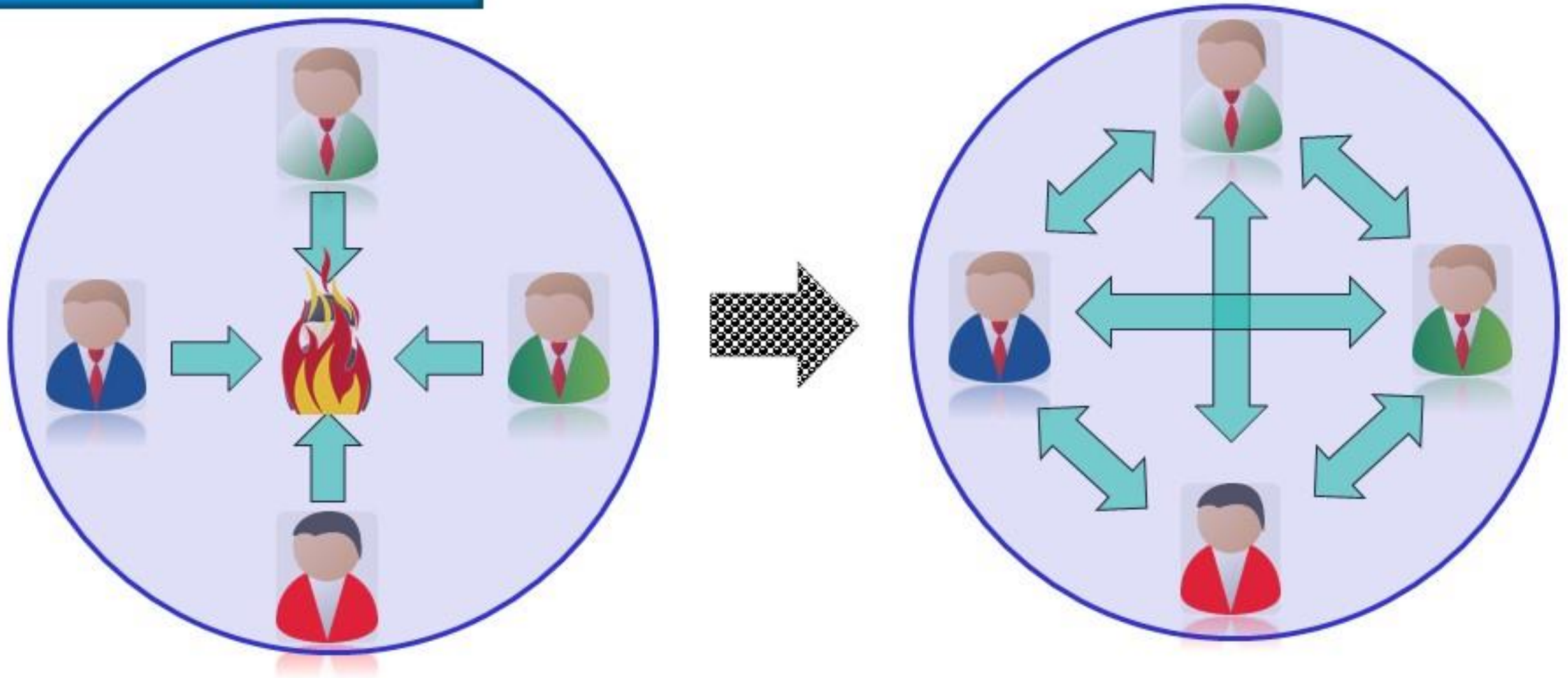
Until now, this is the best way we've been able to achieve the goal of person-to-person transactions at a distance.

❖ Disadvantages of Centralized approach (Client-Server)

- ❑ Rely on a completely trusted centralized control
- ❑ Lack of transparency, mechanism for verification of a trusted third-party
- ❑ High risks: Network congestion, Denial of Service attack (DoS), …

What is a Blockchain?

Decentralized Approach



Centralized Approach

Decentralized Approach

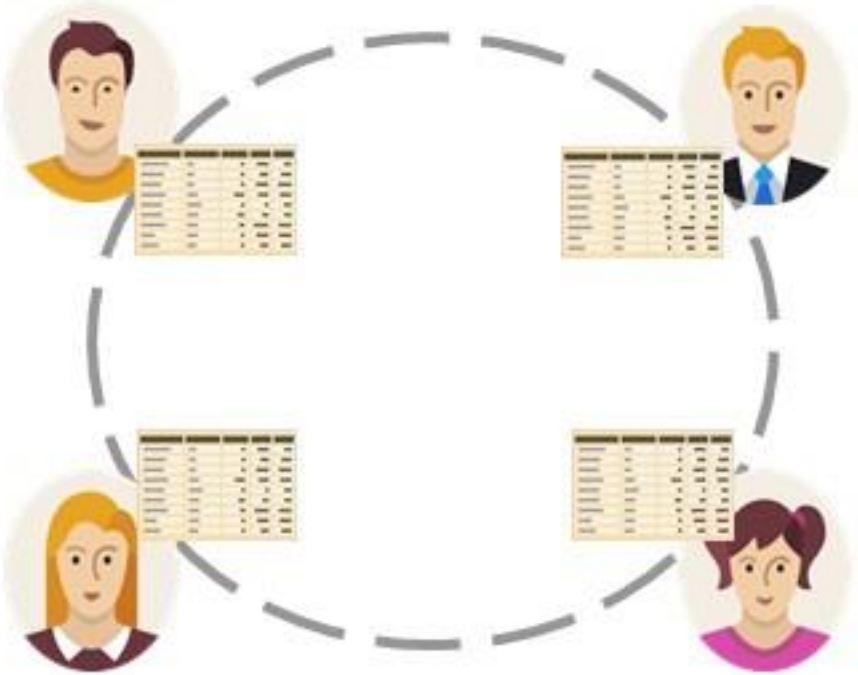
Decentralized Approach

What is Decentralization?

- To enable disintermediation (cut out the middleman).
- No node is instructing any other node as to what to do.
- If one node is corrupted the network can "repair" itself and still able to operate.
- To take down the whole network, must take down each and every nodes inside that network.

Decentralized Approach

- Removing a central authority is risky:
  - **Who maintains** the record of transactions?
  - How do you **prove** that a transaction is **valid**?
  - How do you **come to an agreement** (consensus) in a decentralized system where some of the participants could be **lying**?



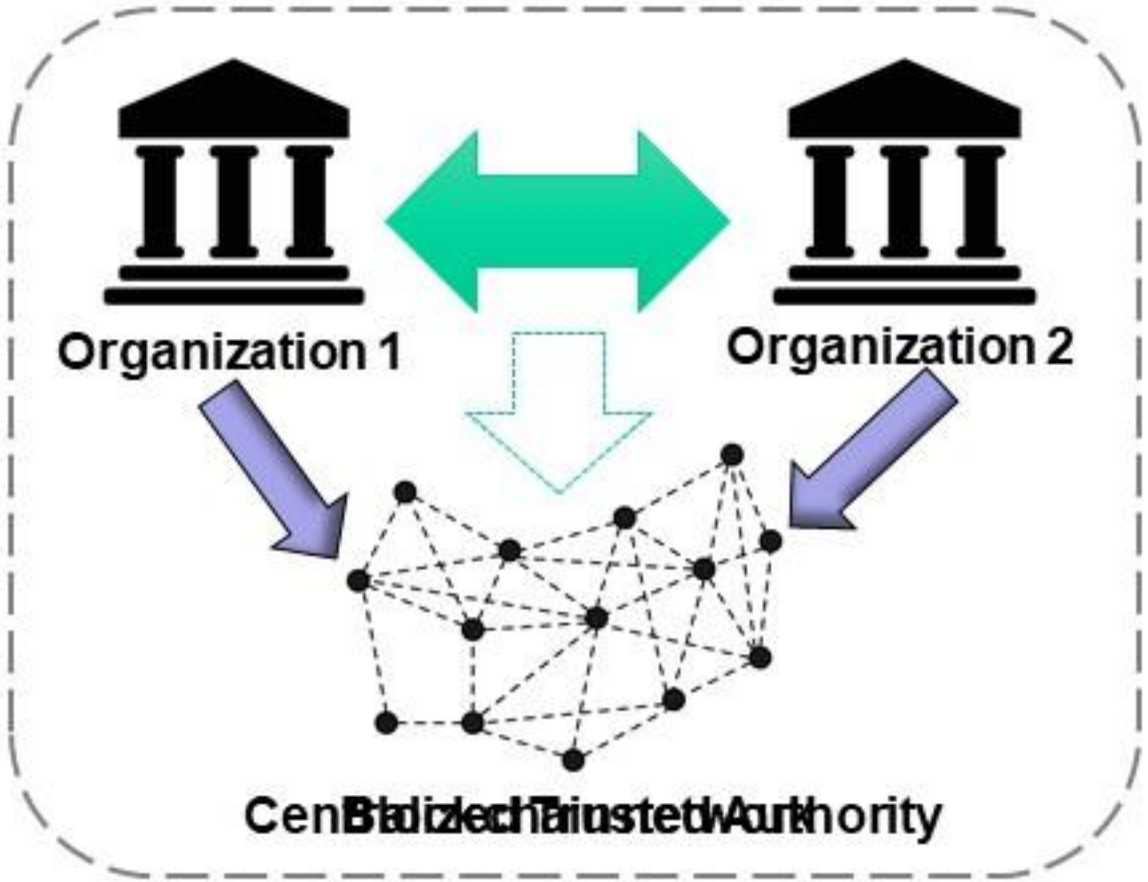
Who can really be trusted?

Blockchain replaces AUTHORITY with CRYPTOGRAPHY (security)

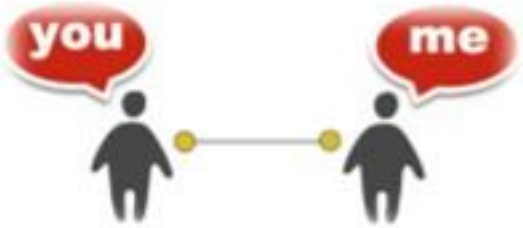
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System | Oct 31, 2008

Case-study: Decentralized Approach

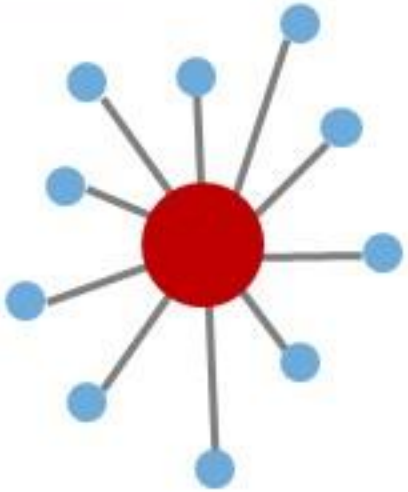


- Each participant has a copy of the ledger, ensuring **immutability**.
- Lower cost, no monthly fees.
- Near real-time settlement.
- No single point of failure.
- Hack-resistant.
- Transparency.



Blockchain replaces centralized trusted third-parties.

Comparison

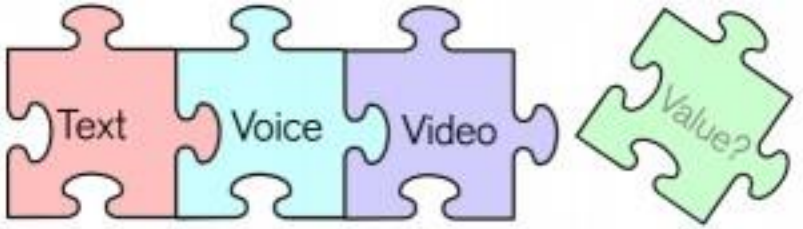


Centralized

Decentralized

Problems	Solutions
Central point of failure	Decentralized network
Expensive to secure	Shared security cost
Trust who is in charge	Trust a fixed set of rules

Value Exchange Revolution



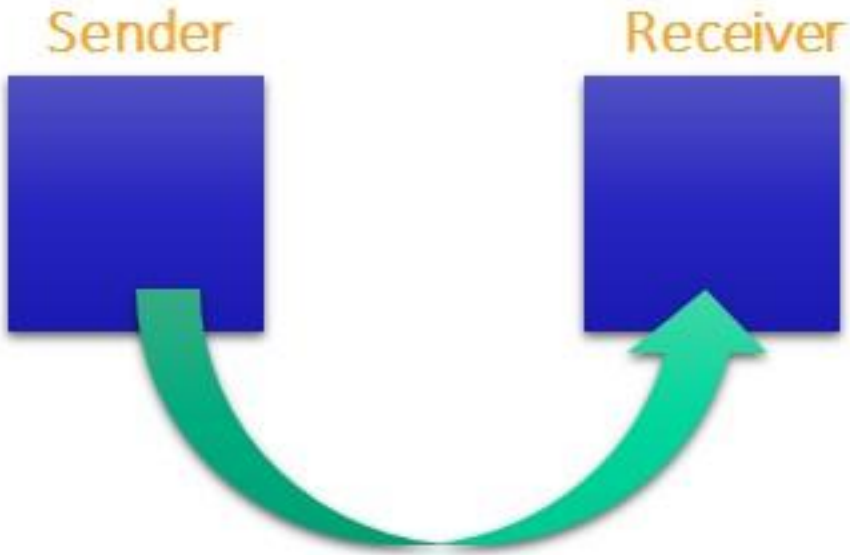
- Today, to exchange value digitally (can be duplicated or manipulated), we rely on trusted intermediaries to establish trust (prevent fraud) between untrusted parties.
- Blockchain uses a decentralized mechanism to establish trust, without the need for a trusted intermediary.

"The Internet of Value", "The Internet of Trust"

- The Internet revolutionized the way we exchange **INFORMATION**

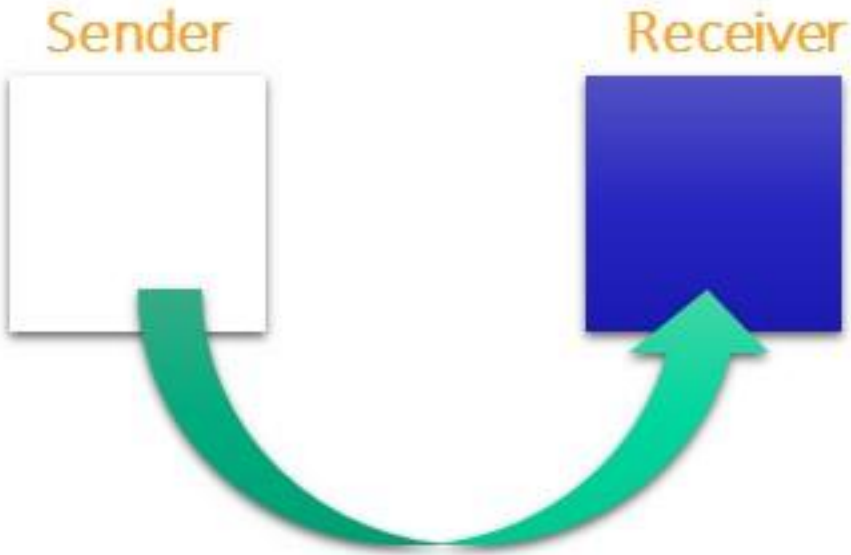
- Blockchain is revolutionizing the way we exchange **VALUE** on the Internet

Value Exchange Revolution



COPY

Email: Sent message are still remain in Sent Box, it's a copy.



MOVE

Blockchain: Transfer the value of digital currency to another.

What is a "Blockchain" ?

"Blockchain is *a tamper-proof, secure, shared* digital data structure (ledger) that is used to maintain a continuously growing list of records (asset transactions), called blocks, between members in a public or private peer-to-peer network"

"Blockchain is a cryptographically secure protocol for building an *immutable* (extremely hard to change) historical record of asset transactions (ledger)"

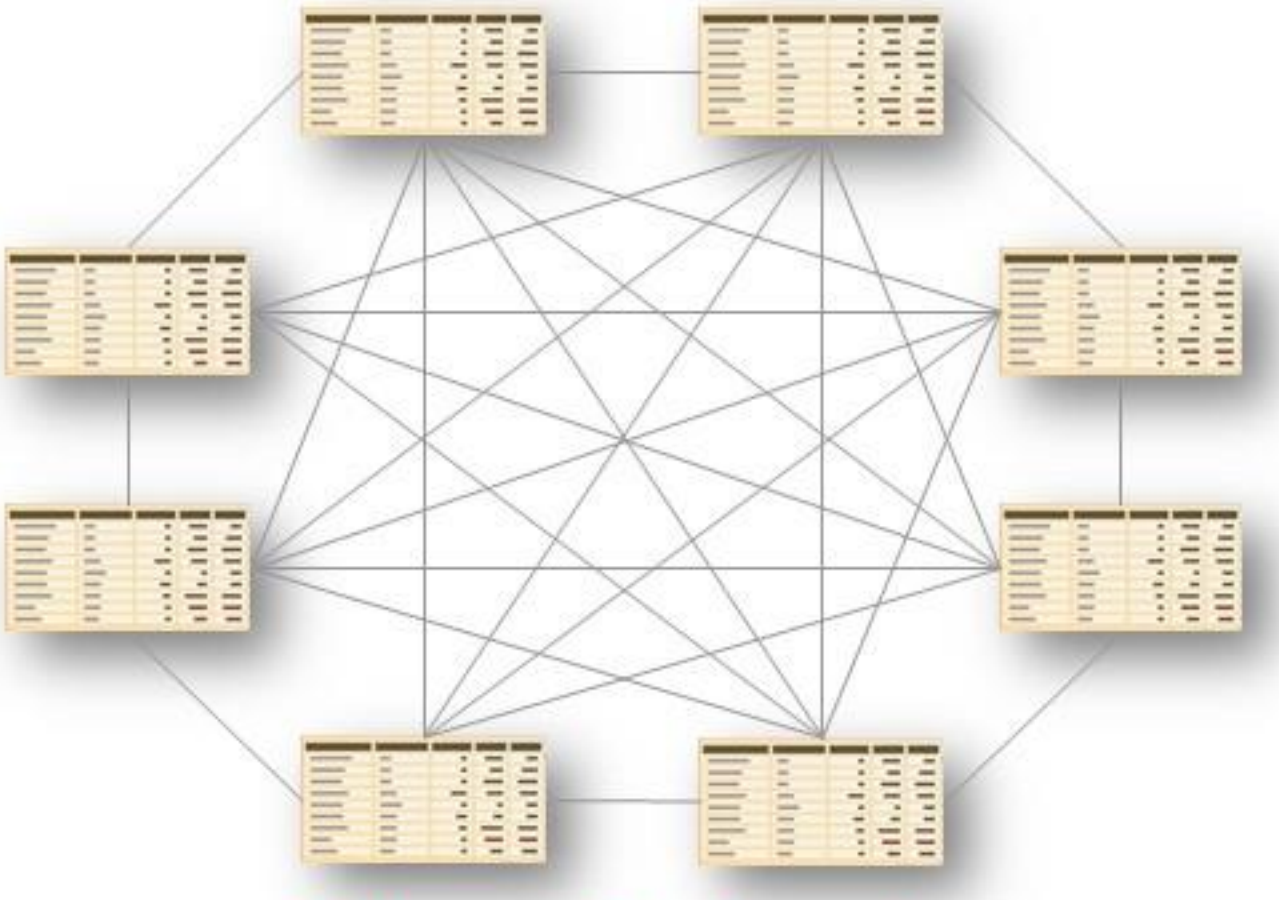
"Blockchain is used to *establish "smart" trust* (consensus) among parties in *a decentralized network* where trustless, no relationship currently exist"

What is a “Blockchain” ?

What is a “Blockchain” ?

FROM	TO	PROPERTY	VALUE
Alex	Katie	**Payment**	$500
Jim	Sally	**Payment**	$300
Alex	Garth	**Asset**	Car
Katie	Tony	**Payment**	$100
Molly	Paula	**Message**	Phone bill paid

Example Ledger



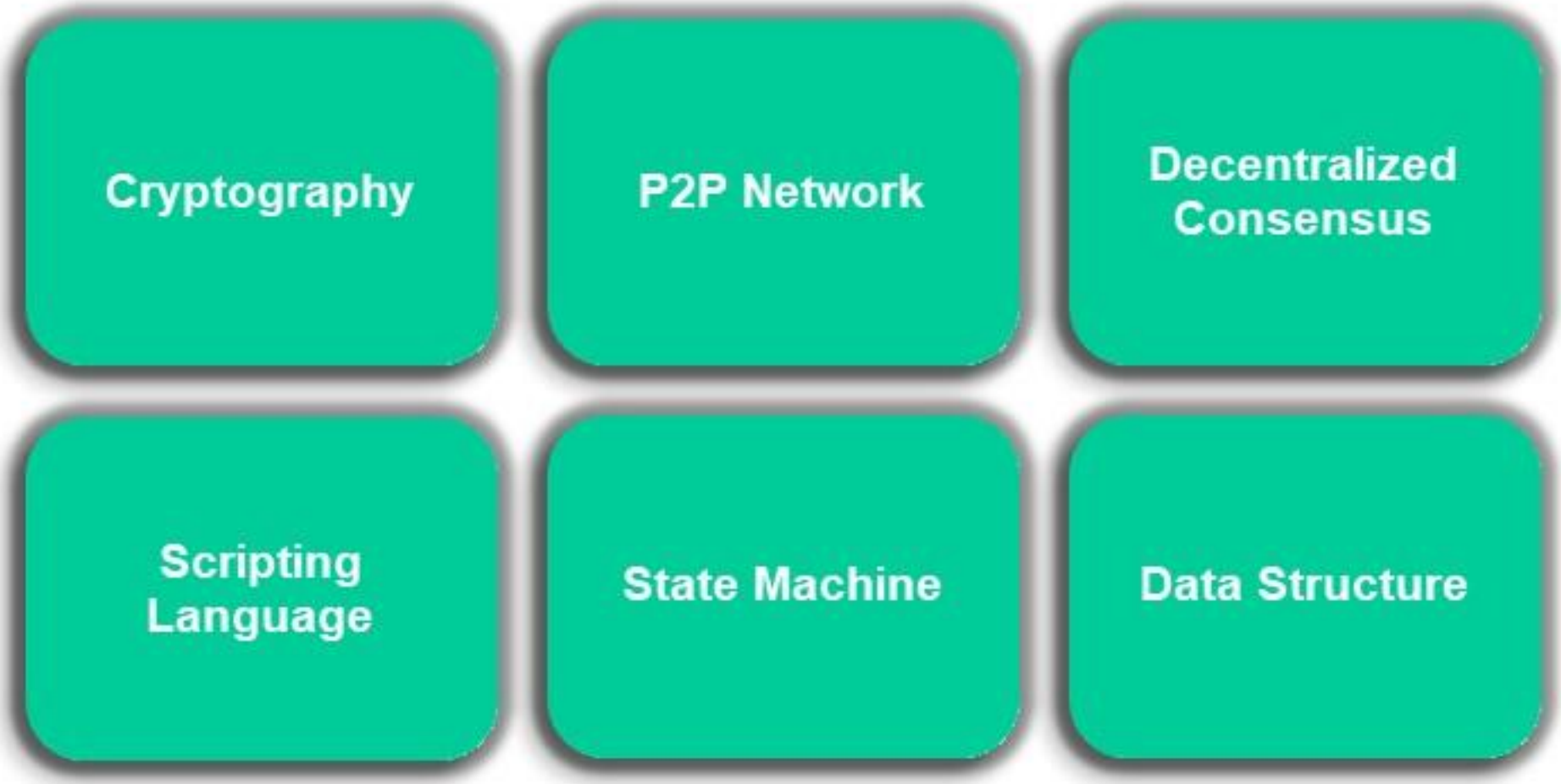
Entire participating nodes have the same Ledger

Why are Blockchains Tamper Proof?

Each network participant keeps a copy of the entire blockchain, the file where all past transactions are recorded. New transactions can be verified by all members of the network. Only if the majority agrees that a transaction is valid, the transaction is validated.

If a malicious party makes unauthorised changes to his copy of the blockchain on his computer, other members of the network will refuse the transaction, since that malicious version of the blockchain data will differ from the rest of the network. To tamper data and transactions, you need to tamper copies of the same data on the majority of the network

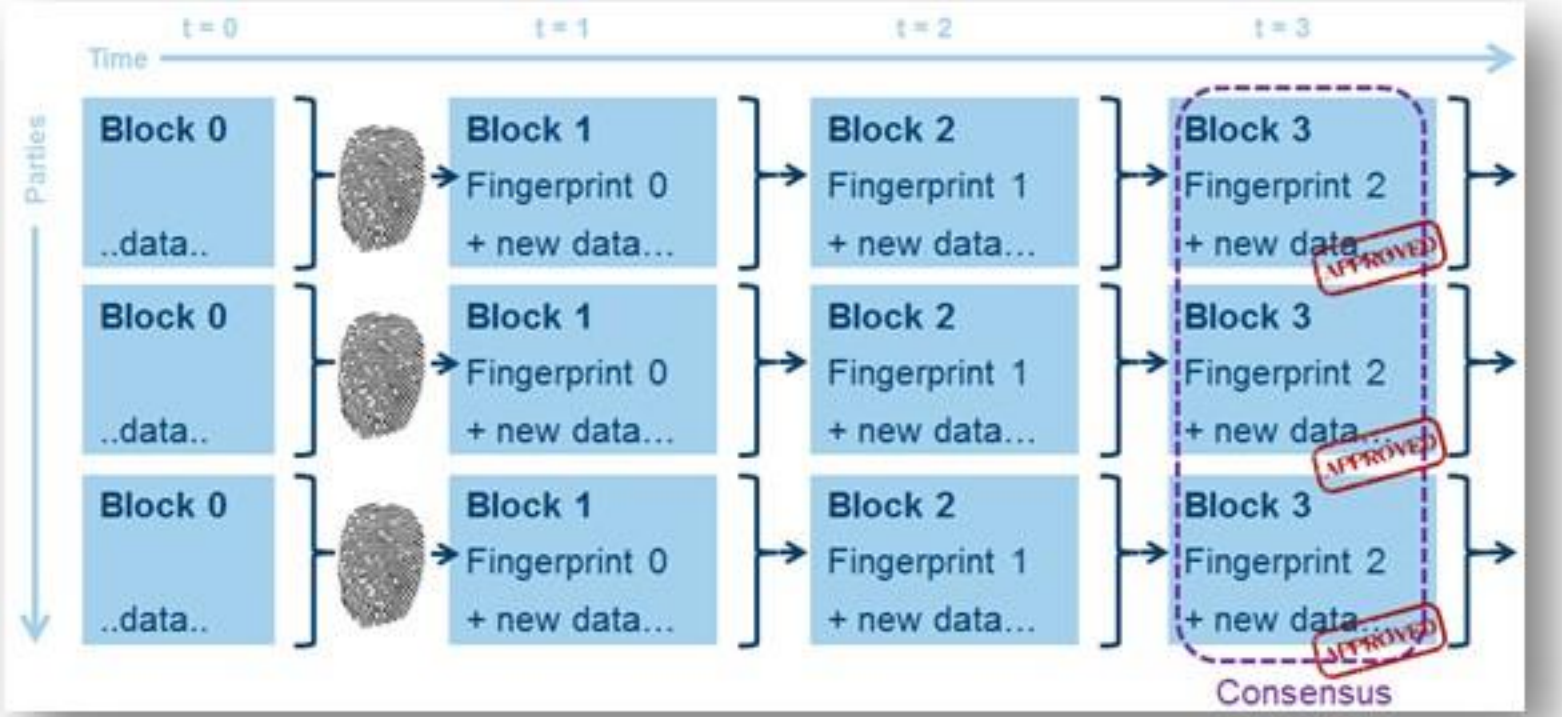
Components in Blockchain



What is a "Consensus" ?

- Instead of relying on a trusted third-party, member nodes in a Blockchain Network uses a Decentralized Consensus Mechanism *(Governance Decision)*
  - to ***come to an agreement*** before a new transaction is ***added*** to the Ledger
  - to ***ensure*** that these shared Ledgers are **exactly the same** (maintain data consistency)
  - to ***establish trust*** between unrelated parties over **an untrusted, anonymous network** (like the Internet)

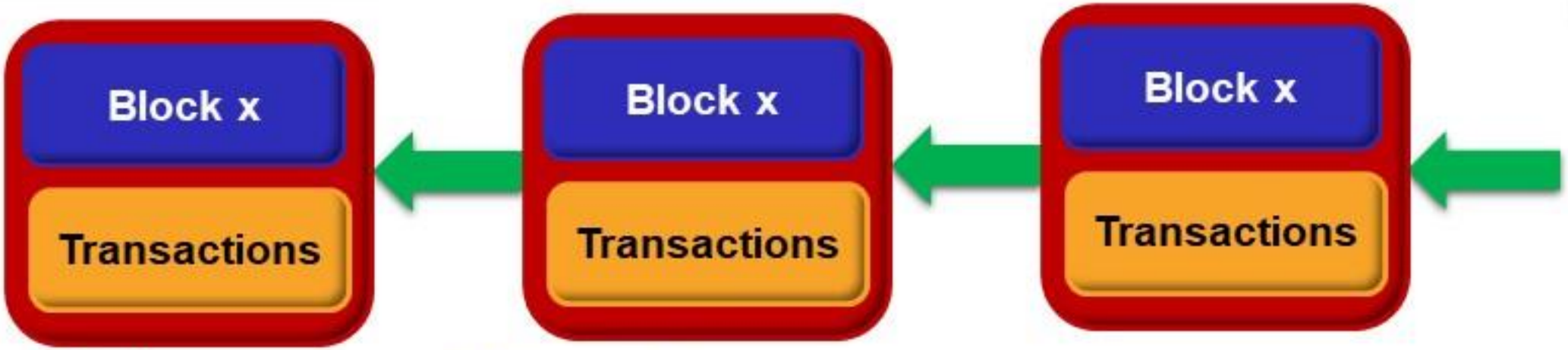
Decentralized Consensus



❖ Decentralized Consensus Mechanism

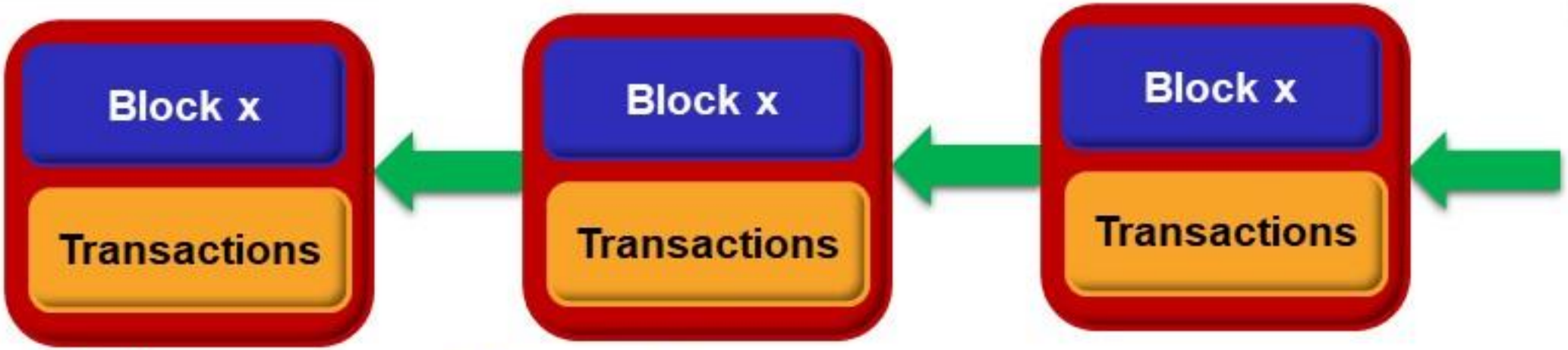
- ❑ The hard part of the distributed (P2P) network
- ❑ Consensus is the backbone of a Blockchain and provides decentralization of control
  - Based on **game theory incentive mechanisms** combined with **cryptography**
  - Using **"Proof-of-work"** (e.g. Bitcoin), **"Proof-of-stake"** (e.g. Peercoin, Nxt)

Structure of Blockchain Ledger



- A logical "Block" is a set of valid transactions that have been **verified** by participants on the network
  - Transactions are the actions created by the participants in the system
  - Blocks record these transactions and make sure they are in the correct sequence and have not been tampered with
  - The Chain is bundled by multiple inter-linked chronologically ordered valid Blocks

Structure of Blockchain Ledger



- A logical "Block" is a set of valid transactions that have been **verified** by participants on the network
  - Blocks are numbered in ascending order (the "height" of the Block), 0 is "genesis/first/oldest" Block
  - Blocks are created periodically (on average, 10mins for Bitcoin) through a process called "mining"

Structure of Bitcoin Ledger

BLOCK

Blocks are units of the Blockchain

HEADER

- Version
- Previous Block Hash
- Merkle Root
- Timestamp
- Difficulty
- Nonce

BLOCK CONTENT

- Coinbase TX
- Bitcoin TX

Transaction

Each transaction is a Bitcoin payment

TECHNICAL DATA

- Version
- Lock Time (delay)
- Number of Inputs
- Number of Outputs

INPUTS

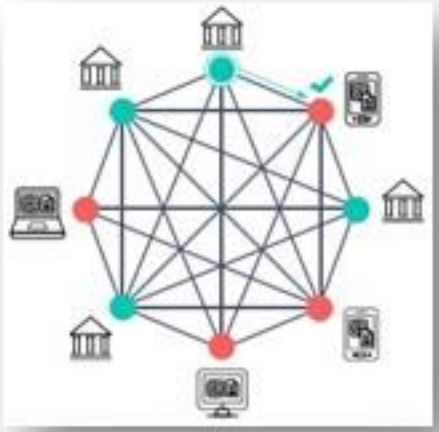
- Previous TX Hash / Output Index
- Private Unlock Script
- Script Length

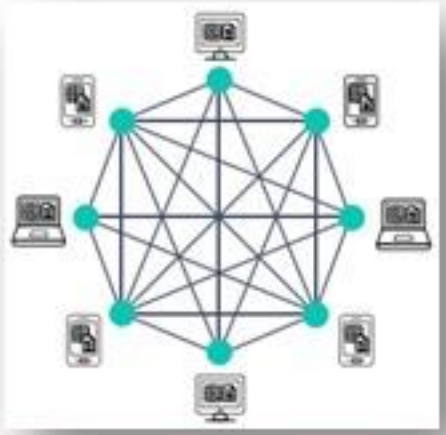
OUTPUTS

- Amount
- Public Locking Script
- Script Length

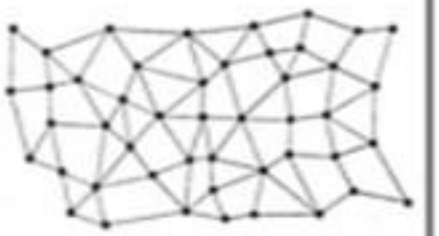
Type of Blockchains

- **Validator node**
  (Can both *initiate/receive* and *validate* transactions)
- **Member node**
  (Can only *initiate/receive* transactions)





	Permissioned Blockchain (Private)	Permissionless Blockchain (Public)
How do you get access to the network?	Authorized access *(used only within a specific organization, like an Intranet)*	Open access *(participation in a network is open to anyone, like the Internet)*
How are their approach to laws and regulations?	Comply to certain regulations such as KYC (Know-Your-Customer)	Censorship resistant
Who are the validators?	Pre-selected, trusted validators *(building a consensus is quite easy as participants are all identified)*	Anonymous, fully decentralized validators *(building a consensus is important in order to eliminate malicious participants)*
What can it be used for?	Enterprise-level systems	Open-access applications

Ledger	Mechanics			
	Level	*Copies*	*Readers*	*Writers*
Traditional		One	One	One
Permissioned Private		Multiple	Multiple	Multiple
Permissioned Public		Multiple	Unlimited	Multiple
Unpermissioned Public		Unlimited	Unlimited	Unlimited

Why use Blockchain?

Features of Blockchain

- Fully Decentralised/Distributed
  - Decentralized Ledger

    → Ledger is replicated on all nodes in a P2P network, and each node's copy of the ledger is identical to every other node's copy
  - Decentralized Network (No central authority)

    → No single point of failure, highly fault tolerant
- Openness/Transparency
  - Ledger is open to anyone (in principle)

    → Every participant has read access to the entire (permissionless) Blockchain
  - Open source software technology

Features of Blockchain

❖ Consensus mechanism

- ❑ All parties in the network can come to collectively agree on the validity of the data recorded
  - → All honest nodes have reached consensus on the same value

❖ Cryptographic security

- ❑ To makes history of data safe, complete, correct, and consistent in order to maintain the integrity of the whole system without the need of any central authority

❖ Privacy/Anonymity

- ❑ Identity of parties is not disclosed. Instead, security key pairs (public and private key) are required
  - → Anonymity = Pseudonymity (unreal identity) + Unlinkability

Features of Blockchain

❖ Immutability & Integrity

- ❑ Transactions cannot be altered without leaving some trace once verified by consensus mechanism and written to the ledger
- ❑ Data immutability

  → Data is contained in a committed transaction

❖ Traceability/Provenance

- ❑ To provide an indisputable mechanism to verify that a transaction has existed at a specific time in the block

❖ No Double-Spending

Features of Blockchain

- Perfect witness - A single source of truth
- Backbone of its crypto-currency

The challenges of Public Blockchain

- **Scalability**, limits on:
  - The size of the data on Blockchain
  - Transaction processing rate (e.g., transaction per second)
  - The number of Transactions included in each Block
  - Latency between submission and confirmation that a Transaction has been included on a Blockchain is affected by the Consensus mechanism

The challenges of Public Blockchain

- Privacy, limits on:
  - There are no privileged users
  - Every participant can access all the information on Blockchain and validate new Transactions
- Blockchain is absolutely not suited for storing large amount of data

Evolution of Blockchain Technology

The first generation of Blockchains (Blockchain 1.0)

- To use a (public) Ledger to store cryptographically-signed transactions and value transfer
- Very limited capability to support Programmable Transactions
- **E.g.,** Bitcoin, Litecoin, Dogecoin, …

The second generation of Blockchains (Blockchain 2.0)

- To use a general-purpose programmable infrastructure with a public Ledger that records the computational results
- Programs can be deployed and run on a Blockchain, and are known as Smart Contracts

  → To enable more complex programmable Transaction: conditions, business logic
- Ethereum is the most widely-used Blockchain that supports general-purpose smart contracts
- E.g., Nxt, NEO, …

Many Blockchains

Multiple implementations of Blockchain

- Bitcoin, Ethereum, Ripple, Litecoin, Dogecoin, Monero, Zcash, …

- Each coin is separated and runs its own Blockchain
- The value transferred within each Blockchain is primarily its own currency

Many Blockchains

- Key differentiation between Blockchain systems
  - Type of Blockchain
    - → Public vs. Private
  - Consensus approach
    - → Proof-of-work, Proof-of-stake, Proof-of-...
  - Programmability
    - → Smart contract
  - Resource consumption

Conclusion

- Internet Challenges
- Blockchain Technology
  - Decentralized Approach
  - Definitions, Components, Structure of Ledger, Features, Types
  - Challenges
  - Evolution


Thank you!