

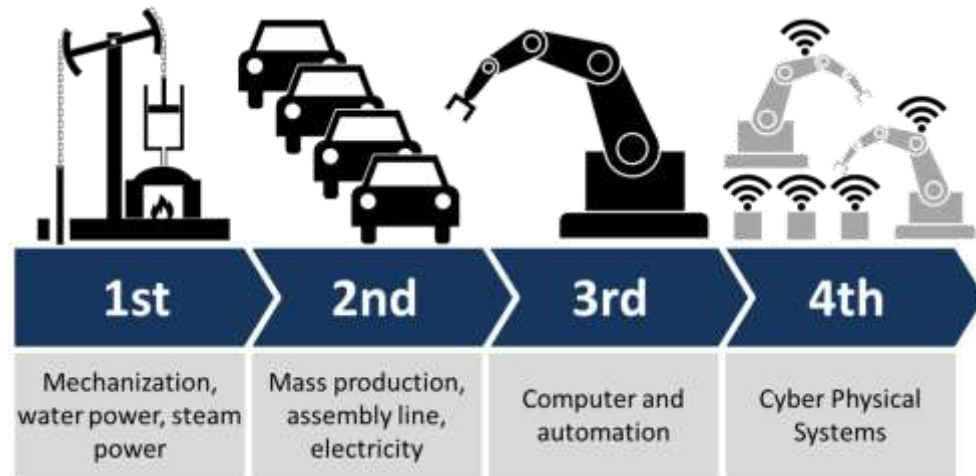
BLOCKCHAIN ASPECTS

BLOCK
CHAIN

Spiros Moros
Managing Consultant
PRIORITY Quality Consultants

Industry 4.0 – 4IR

“Smart” industrial revolution



- Internet of Things (IoT)
- Robotics
- Virtual Reality (VR)
- Augmented Reality
- Artificial Intelligence (AI)
- Digital transformation
- Distributed Ledger Technology (DLT)
- Blockchain
- Smart Contract
- Platform economy
- Share (ή sharing) economy
- Digital energy
- Digital health
- Biotechnology
- Neurotechnology
- Drones
- 3D Printing

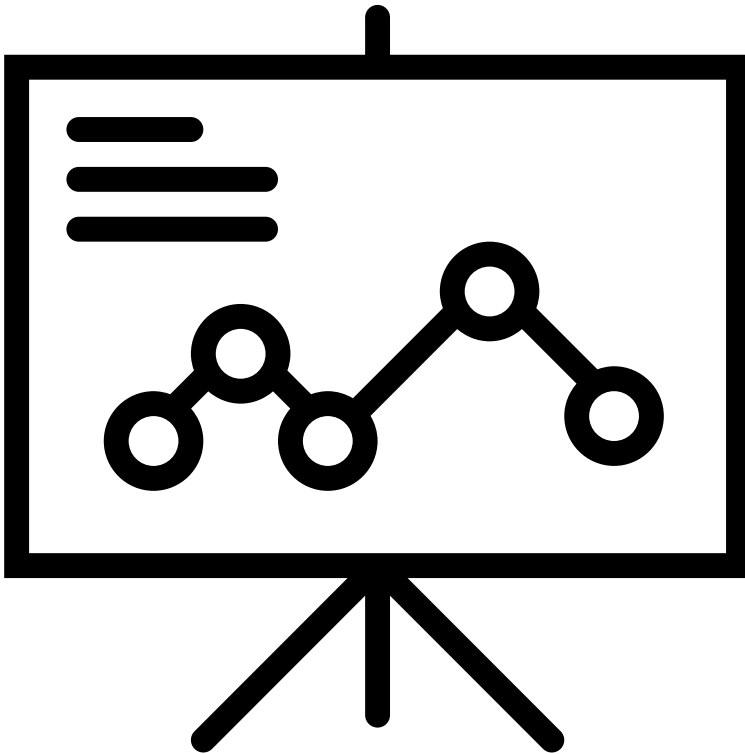
Οι βασικές αρχές του Blockchain



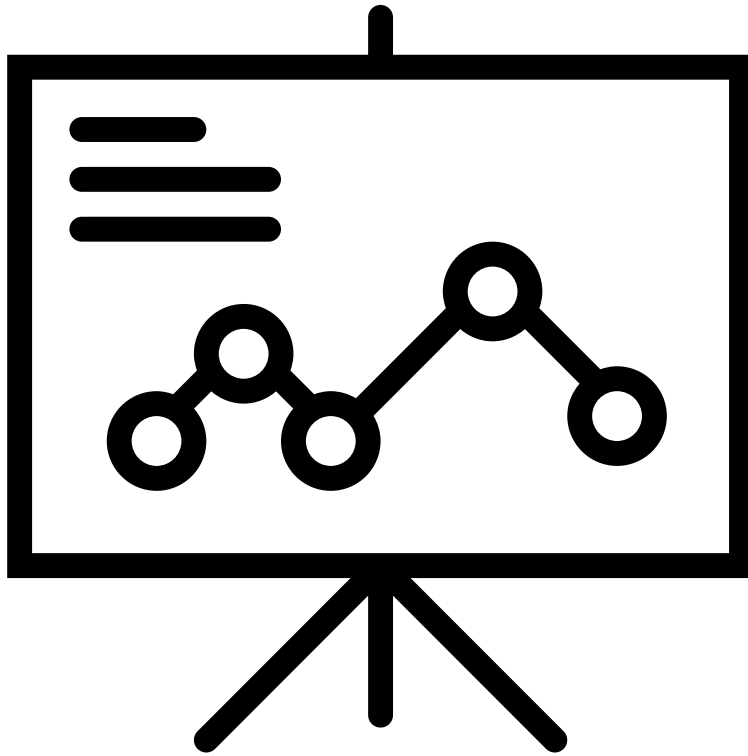
What is blockchain ?

■ Blockchain is :

- a shared, distributed ledger
- transactions are digitally recorded and linked together
- they provide the entire history or provenance of an *asset*
- It can contain anything that has “a value”
- An *asset* can be tangible (a house, a 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.

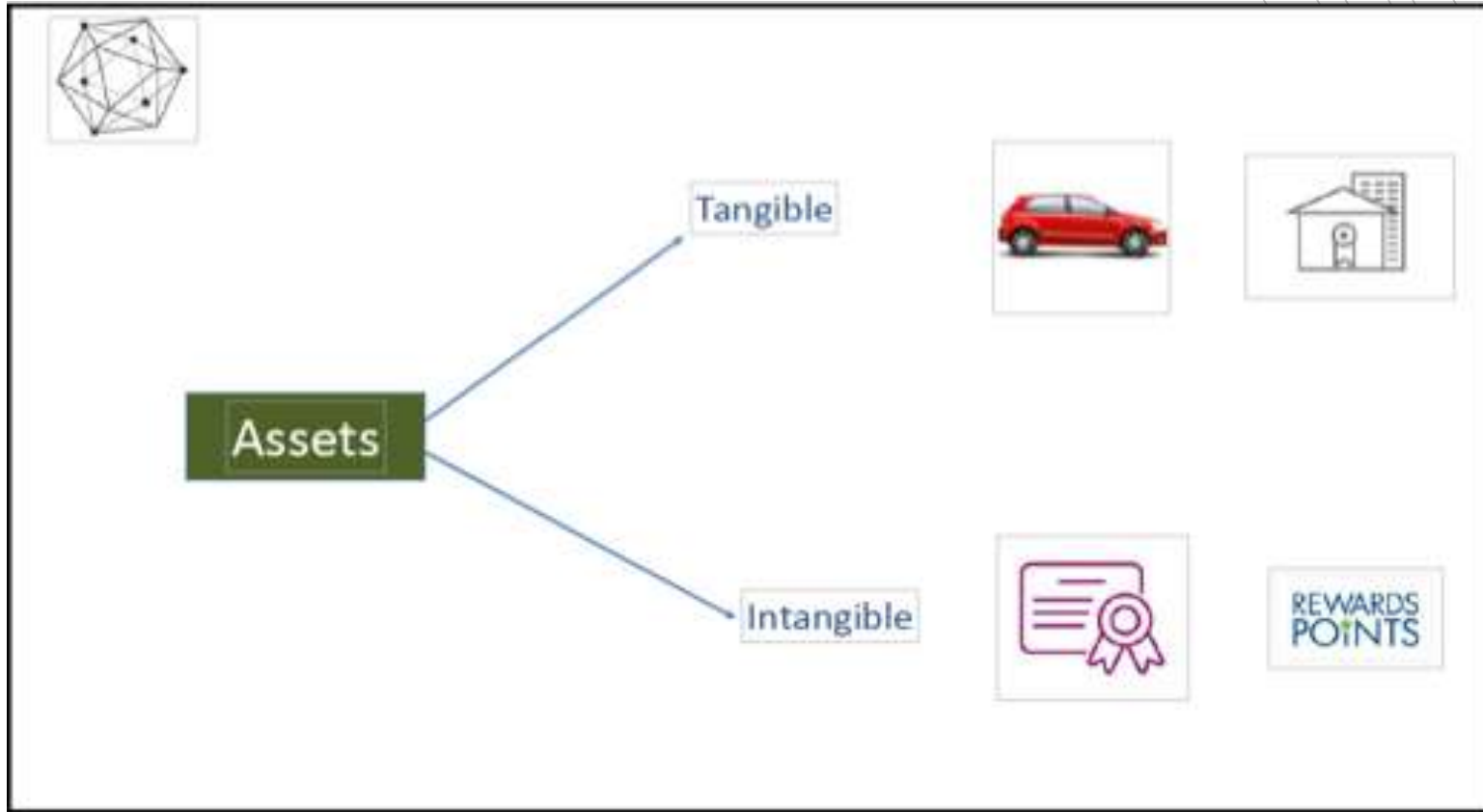


What is blockchain ?



- A transaction is added to the blockchain only after it has been validated using a consensus protocol, which ensures it is the only version of the truth. Each record is also encrypted to provide an extra layer of security.
- Blockchain is said to be “immutable” because the records cannot be changed and transparent because all participants to a trade have access to the same version of the truth.
- **Blockchain is a technology NOT a software**
- The global Blockchain market is currently (Year 2021) worth an [estimated \\$6.6 billion](#) (IDC), will reach \$19 billion in 2024 (IDC) and experts predict that it will reach a [\\$69 billion valuation by 2030](#), growing at more than 68% per year.

Assets Categories



Source: Blockchain Train Alliance

Create value with Assets

- Anything that is capable of being owned or controlled to produce value, is an asset
- Two fundamental types of asset
 - Tangible, e.g. a house
 - Intangible e.g. a mortgage
- Intangible assets subdivide
 - Financial, e.g. bond
 - Intellectual e.g. patents
 - Digital e.g. music
- Cash is also an asset
 - Has property of anonymity



Technology and Blockchain

Blockchain is a combined use of existing older technology.

- **Accounting Ledger** – 1000's of years old, now triple-entry ledger with the internet and Blockchain S/W

- **Cryptography** – “coding messages” has been used for thousands of years, and still used in complex S/W algorithms for military and business applications like Blockchain

- **Business Computer Network Technologies** – Blockchain makes extensive use of P2P networking architectures

Blockchain Rules

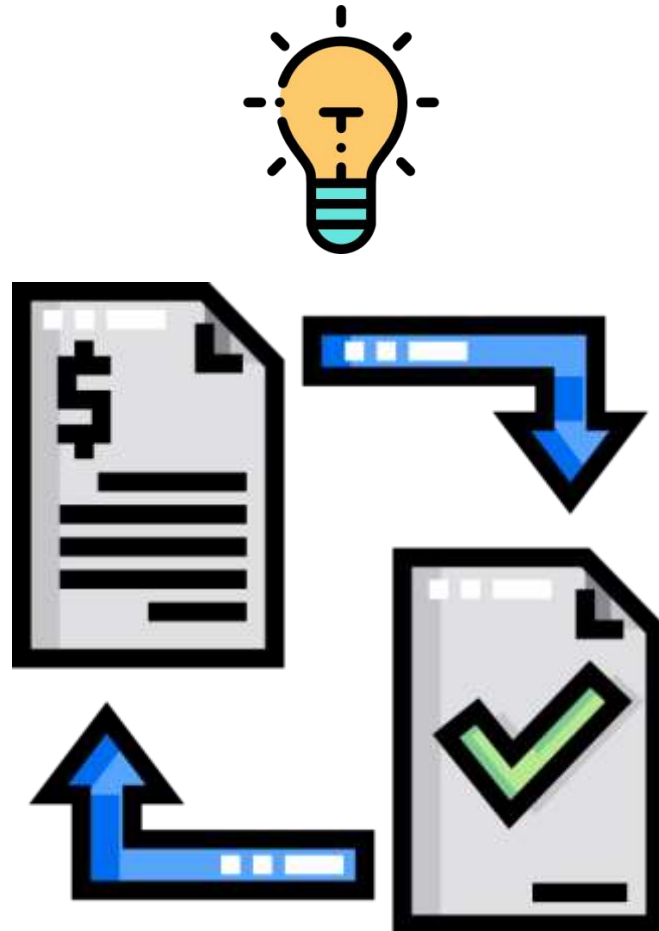
- Once something has happened, and we create a record of that, the fact that it happened never changes
- Data written into a blockchain is a historical record and is immutable
- Blockchains have to prove that they haven't been tampered with
- All the nodes (computers) running on a blockchain must agree (i.e. have consensus) on ALL the data stored on it (aka – The World State of the Blockchain)

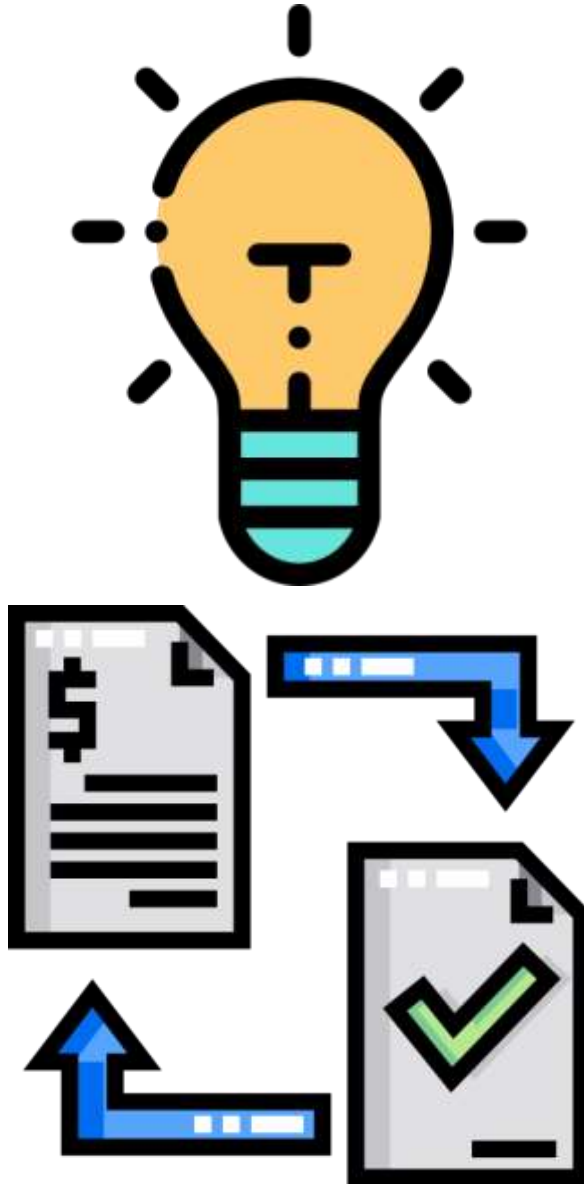
Consensus in Distributed Networks

- In order to update the ledger, the network needs to come to consensus using an algorithm
- Consensus: what does it mean to come to consensus on a distributed network?
 - It means that everyone agrees on the current state (e.g. how much money does each account have) and making sure that no one is double-spending money (easy in Bitcoin, more complex in Ethereum, business networks)

What is a ledger ?

- Is a record keeping device.
- Allows the keepers of a ledger to tell a story.
- This story usually revolves around the ownership and history of ownership of assets, although ledgers can be used to record just about any type of data imaginable.





What is a ledger

- A ledger is like a database, a Google or Excel spreadsheet
- Add new records by appending rows
- Each row contains information
 - Account balances, who owns certain assets

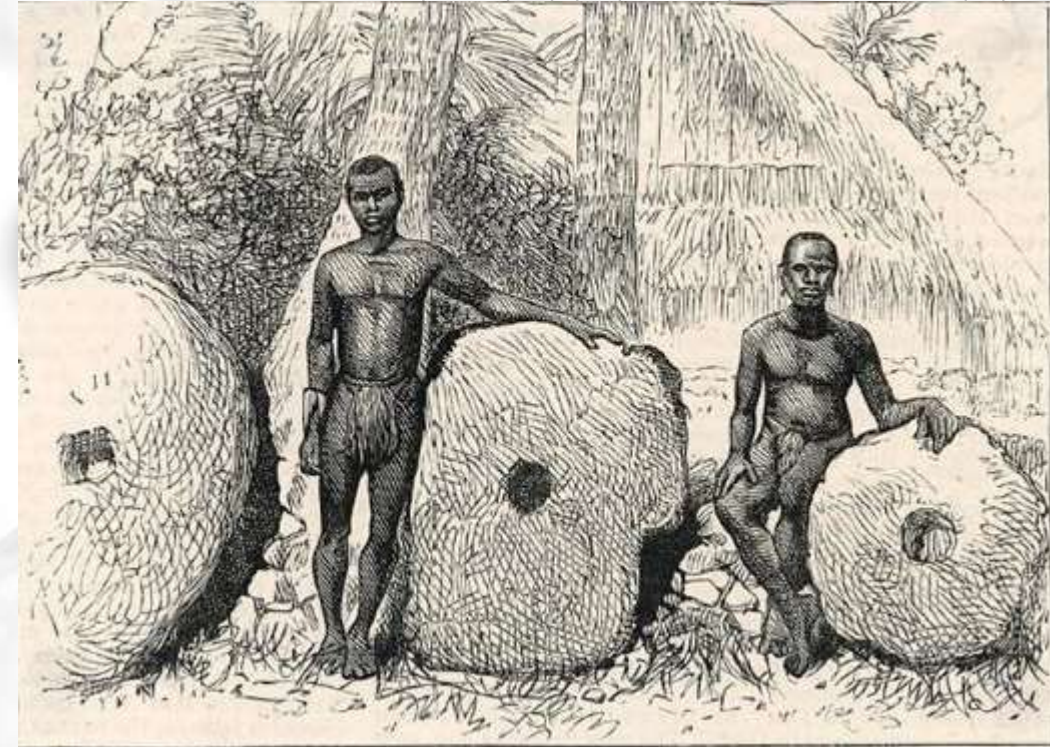
History of Ledger

- Ledgers appear around 5,000 BC
 - Single entry only
- 300 BC – Chanakya
 - First documented accounting standards
- Double-entry ledger appears in 1340 A.D.
 - Track debits and credits
 - Tell the story of a transaction from both / all sides
- Triple-entry ledger appears in 2009
 - aka Blockchain!
 - Debits, credits, and an immutable link to all past debits and credits
- Before this time ledgers were largely unnecessary
- Soon after humanity gave up a nomadic lifestyle to pursue an agrarian one the benefits became apparent.



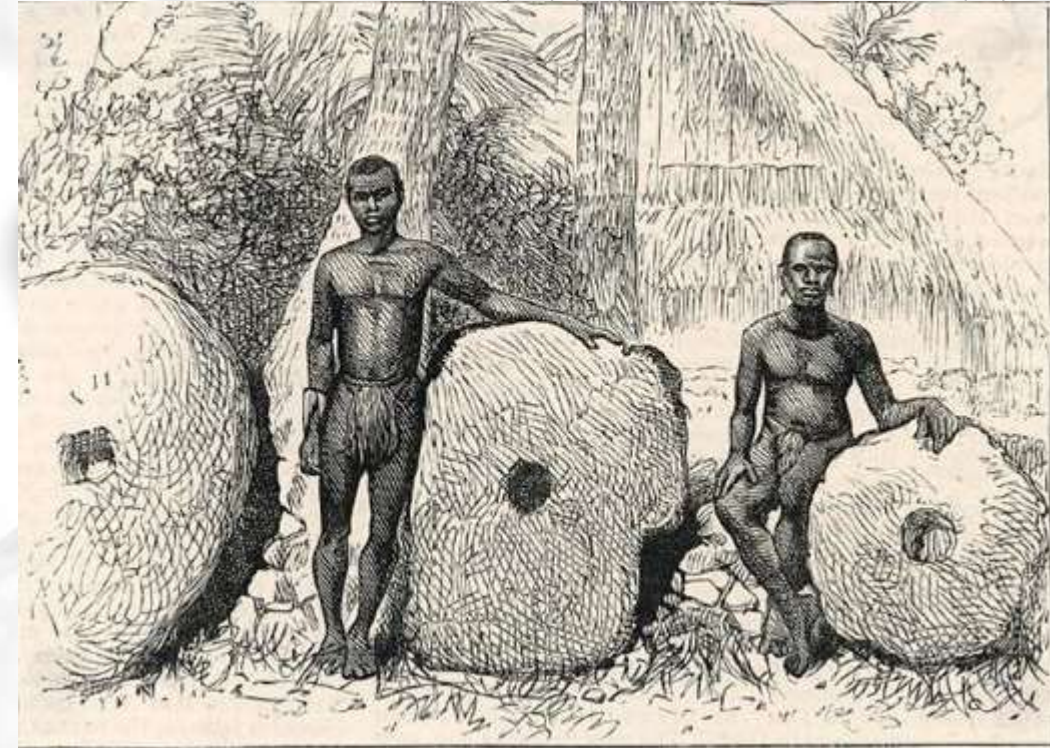
History of Ledger

- What happens when money can't be *physically* traded?
- A ledger is kept
- A ledger is a recording of all transactions
- The ledger records:
 - What was exchanged?
 - Who exchanged it?
- Stones or coins do not have to be physically traded
- Their ownership can be tracked on a ledger



Source: Blockchain Train Alliance

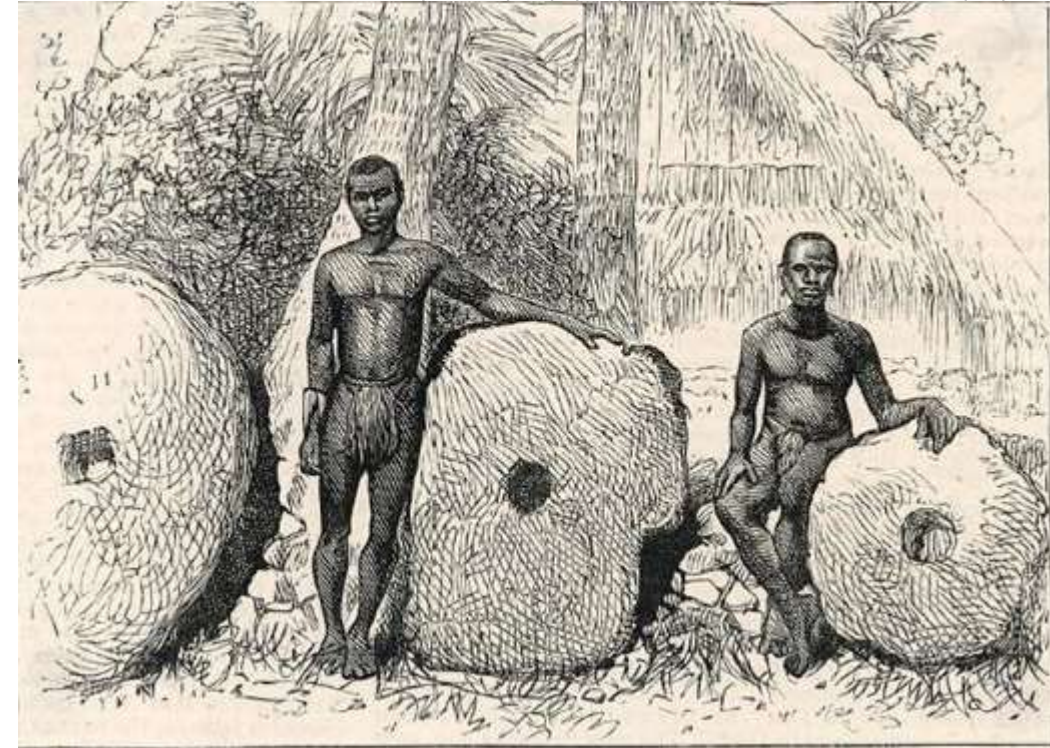
- How did the Yapese manage the ledger?
- **Decentralized Ledger**
- All tribe members keep a copy of the ledger in their head
- Everyone knew who owned which Rai stone at any time
- When two parties wished to transact, they would **announce** their transaction to the tribe
- When a transaction was announced, all tribe members updated their mental ledger



Source: Blockchain Train Alliance

History of Ledger

- Alice agrees to trade Bob her stone by the pond in exchange for all of his cattle.
- Alice and Bob announce their transaction to the tribe.
- Everyone updates their mental ledger. From this point on, they agree that the coin by the pond is owned by Bob until he trades it.



Source: Blockchain Train Alliance

BLOCKCHAIN HISTORY

- Whitepaper published by an anonymous author a decade ago.
- Blockchain began as an idea documented by Satoshi Nakamoto.
- The ideas outlined in this whitepaper lead to the world's first and largest Blockchain – Bitcoin(2009).
- Bitcoin is a cryptocurrency that keeps its users highly anonymous through public key cryptography and cryptographic hashing.
- In public key cryptography users store their bitcoin in a digital wallet.
- This wallet contains the account's private key which is used to sign all transactions from that account.
- Any transactions presented by that account will be verified by the network using the corresponding public key for the account.
- It is important to note that while common, anonymity is not a requirement of a blockchain platform.

BLOCKCHAIN HISTORY

The financial services industry is spending **about \$2.53 billion in 2022 on blockchain**, that will reach **22.46 in 2026** ([Statista report 2022](#)).



Tip Lesson: Bitcoin and blockchain are *not* the same. Blockchain provides the means to record and store Bitcoin transactions, but blockchain has many uses beyond Bitcoin. Bitcoin is only the first use case for blockchain.

SIGNIFICANT BLOCKCHAIN DATES



- 2009 - First Bitcoin Block Created.



- 2010 - Satoshi Disappears in December – Date of last public post.



- 2015 - Ethereum and Hyperledger both go live.



- 2018 – Demand for blockchain increases, 14 Open Jobs for every blockchain developer.

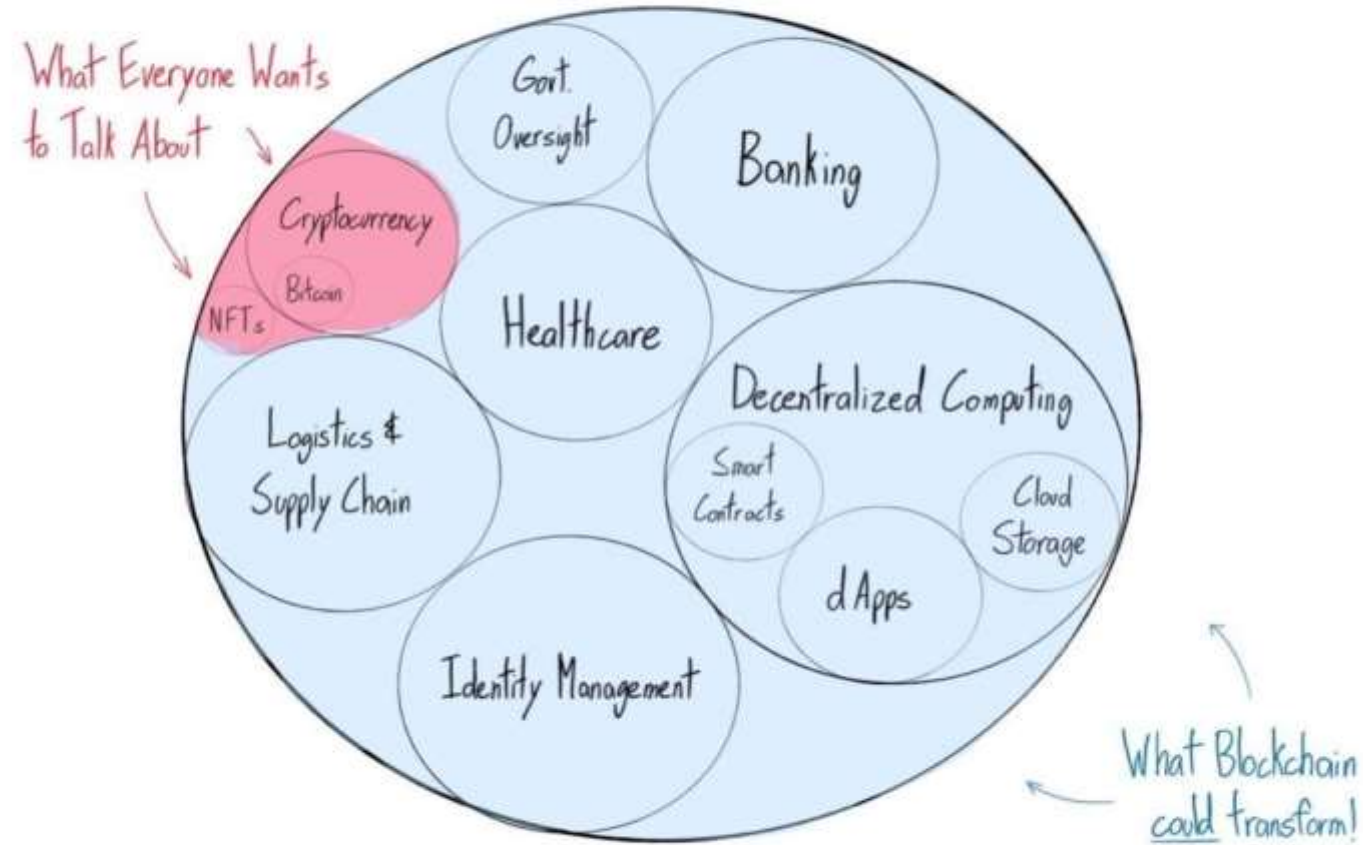


- 2019 - Walmart requires produce suppliers to be using a blockchain solution.



- 2021 - Dubai hosts all government operations and record-keeping operations on blockchain as part of the Smart Dubai 2021 initiative.

Blockchain's Use Cases



Blockchain is so much more than Bitcoin, NFTs, & Crypto!

Blockchain and Cryptocurrencies

BLOCK
CHAIN

Blockchain / Bitcoin

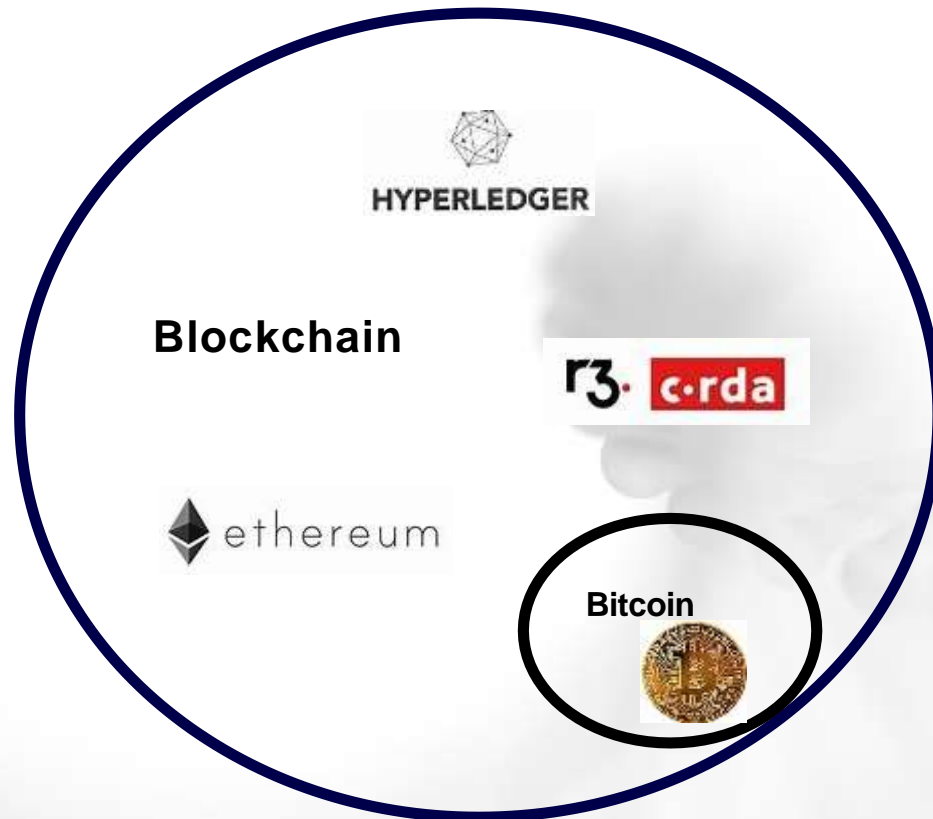
Bitcoin is a **digital, decentralized, disintermediated, trustless** currency



Source: Blockchain Train Alliance

Blockchain is the underlying security software that manages and controls the WW Bitcoin Network, allowing for safe, trustless, and secure P2P transfer of Bitcoin, or any other cryptocurrency.

Bitcoin was the First Blockchain



Similar to Facebook, where Facebook is simply an application that runs on the Internet.

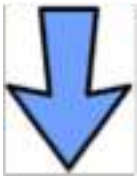
Transaction “BLOCKS” of Blockchains

- A standard Blockchain Block has roughly 25 transactions (1 MB limit)
 - Each record is complete with time, data, all transaction details.
 - When a Block has 25 complete transactions, the Nodes “validate” the transactions on the current page and post it on the Blockchain.
- By comparison, the Bitcoin Blockchain can have up to ~ 2000 Bitcoin transactions per Block. (~ 500 data bytes per transaction)

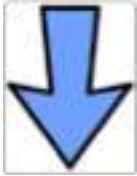
Alice pays Bob \$150.00
Joe played a song on your album
You cast 100 votes for Candidate A
Bob pays Mary \$1,500.00
Apples are treated w/ pesticide
Concert tickets go on sale
Landlord is paid rent on time
Student A earns blockchain cert
Mary pays Sally \$342.97
Ralph sells his home to Louisa
Sue votes 75 for Candidate C
Alicia earns Master's Degree in CS
Tony has complete Hot Wheels
Vehicle is serviced under recall
Farmer collects insurance payout
Harrison sells horse for \$28,000.00
Judy buys 64 ETH

Addresses

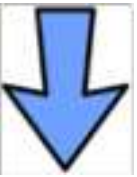
Private key



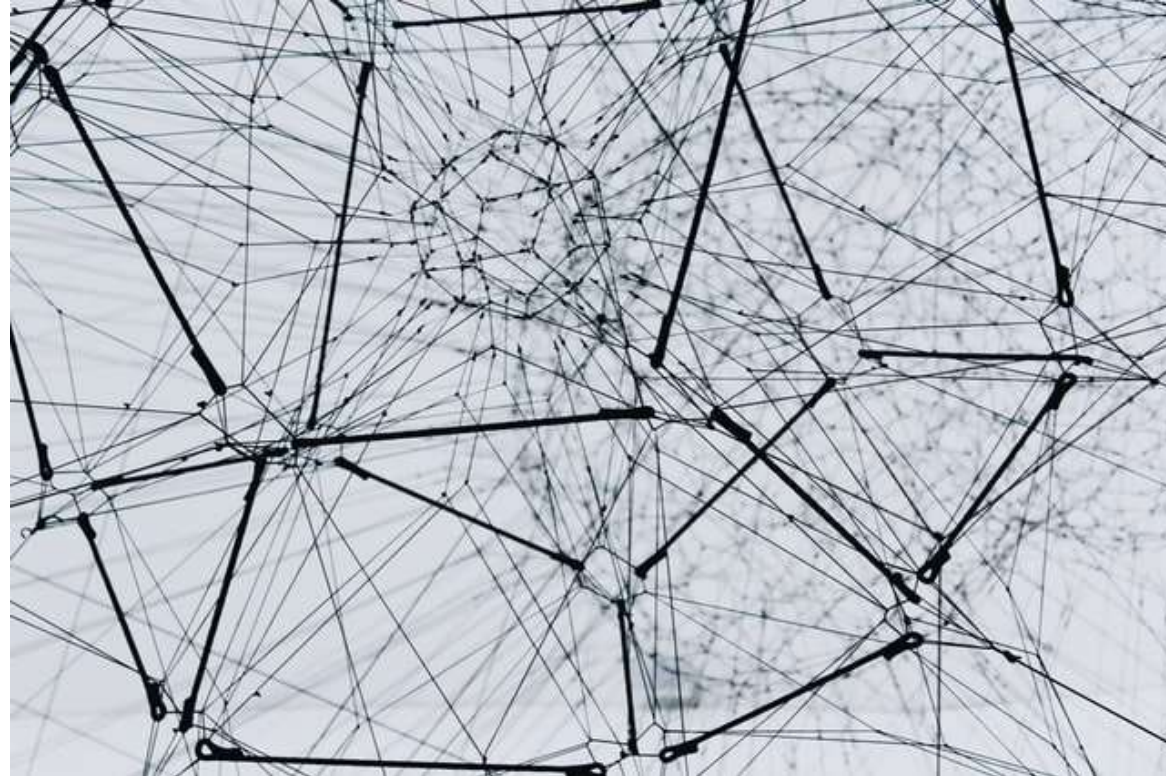
Public key



Hash Encode



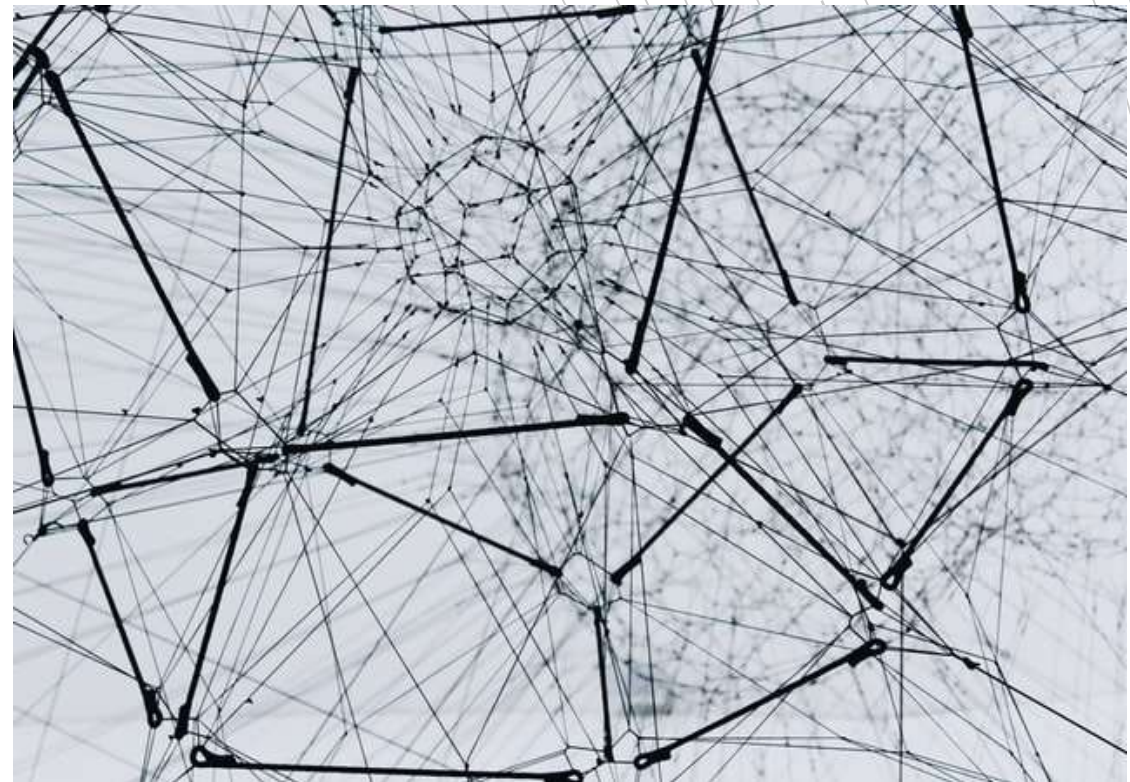
Address



Source: Blockchain Train Alliance

Addresses

- Hides your public key (because of the hashing), but you still have both the public and private key
- This is your bitcoin 'Address' – must be shared with those who need to send coins to your address
- You will (can) have many Addresses
- Your digital wallet software keeps track of all payments made 'to' your Address



Source: Blockchain Train Alliance

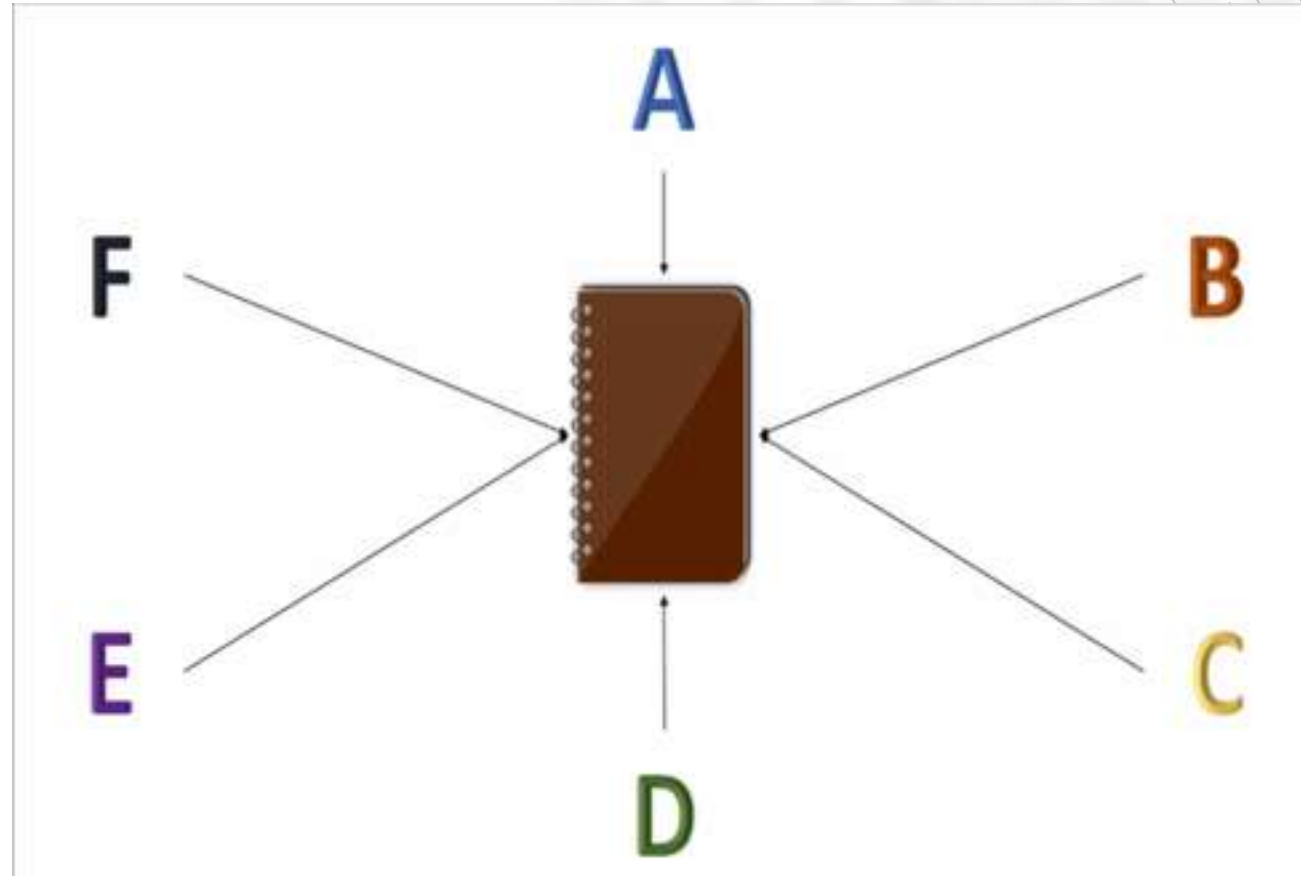
Why Blockchain

A person is holding a yellow sticky note in their hand. The sticky note has the words "BLOCK CHAIN" written on it in blue ink, with a blue underline under the word "CHAIN". The background is blurred, showing a person's head and shoulders and a computer monitor with some text on it.

BLOCK
CHAIN

What problem does Blockchain solve?

Common Ledger (i.e. everyone has the same record)



Source: Blockchain Train Alliance

Benefits of Blockchain

- What are the benefits of Blockchain?
 - Publicly verifiable
 - Accountability to customers and end-users
 - (permission-less)
 - Secure
 - Control who sees what data when (permissioned)
 - Quality assurance
 - Track origin of all supply chain components
 - Example – Food origin and/or safety recalls
 - Smart Contracts as a replacement for middlemen operators
 - Lower transactions costs
 - Removing middlemen reduces cost



Blockchain and Risks



Drawbacks of Blockchain

- What are the drawbacks of Blockchain?
 - Slow adoption to newer technology
 - Quickly evolving making it difficult for companies to commit
 - BaaS (Blockchain as a Service) is expensive to use
 - High cost for trained developers to develop your own Blockchain
 - Development Risks
 - Best Blockchain solutions for industries is still evolving
 - Scalability, transaction speed / cost are still adoption concerns

- Application Use Case adoption is slow. Fear of not working?
- Lack of Standardization
- Stigma and history of Blockchain
 - ❖ Cryptocurrency Hacks and principal losses
 - ❖ ICO/ITO scams
- Anonymity of origin – Satoshi Nakamoto
- No Regulatory Agencies Governing International Blockchains
- AML/KYC - GDPR

Why Not a Database

- Blockchains solve specific problems:
 - Fully distributed - highly fault tolerant
 - No centralized authority
 - 3rd party trust without trust (Relationship)
 - Low barrier to entry - computer + internet = win
 - Instant, Global transactional capability
 - Very low transaction costs
- Traditional Databases have centralized control and do not perform these functions.



Append Only Ledger

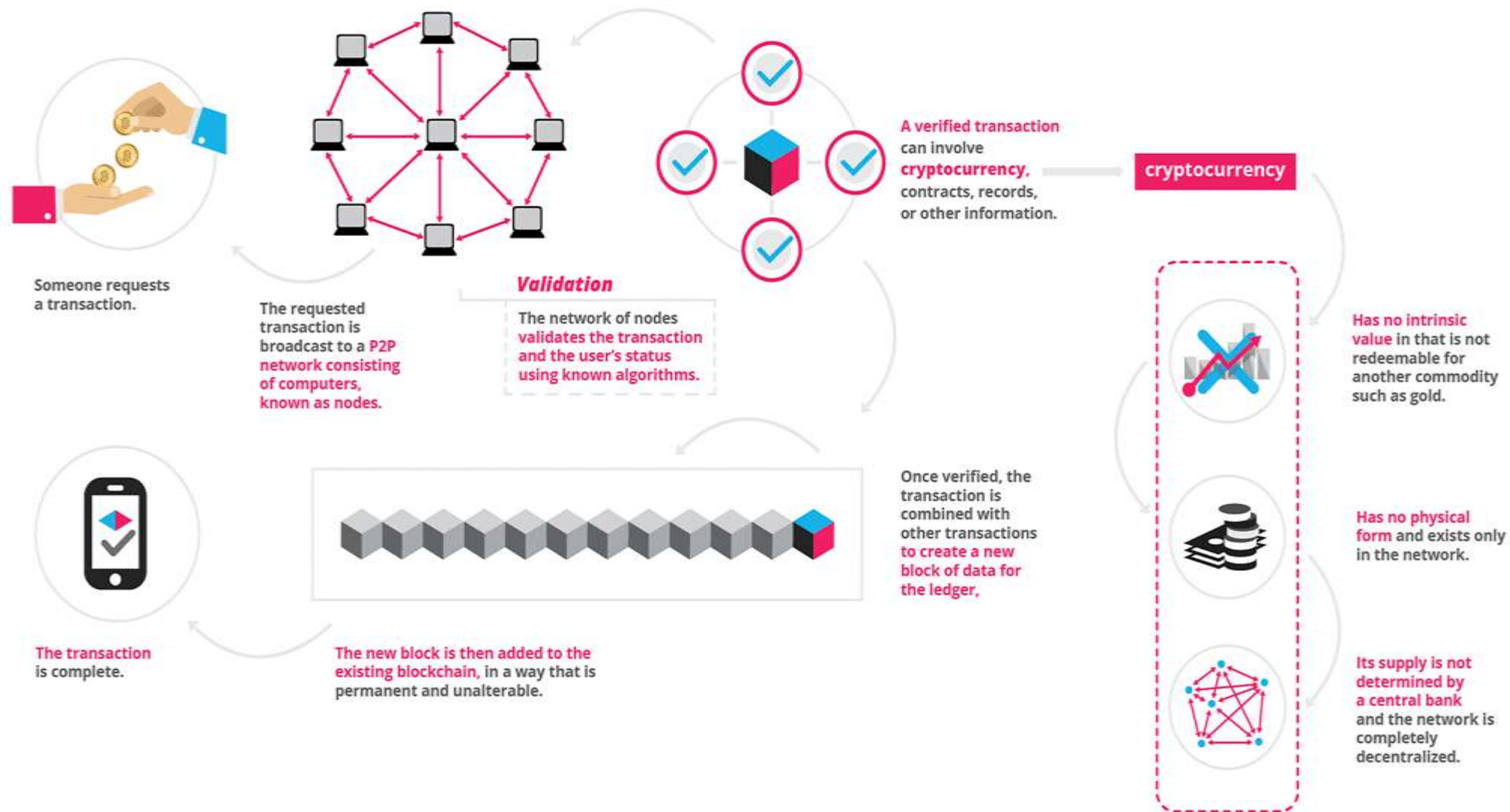
Databases have four primary operations or functions:

- **CREATE**
 - New records can be created and added to the database.
- **READ**
 - Existing records can be read from the database.
- **UPDATE**
 - Existing records can be updated in-place.
- **DELETE**
 - Existing records can be removed or purged from the database.

In blockchain, the last two of these functions have been intentionally removed.

- **CREATE**
 - New records can be created and added to the ledger.
- **READ**
 - Existing records can be read from the ledger.





How it works ?

Blockchain application

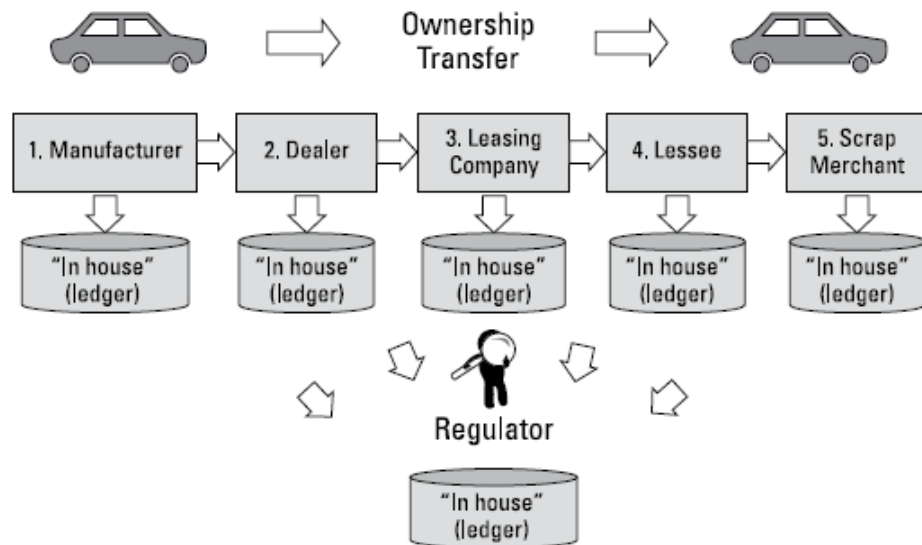


FIGURE 1-1: Tracking vehicle ownership without blockchain.

Source: Blockchain Train Alliance

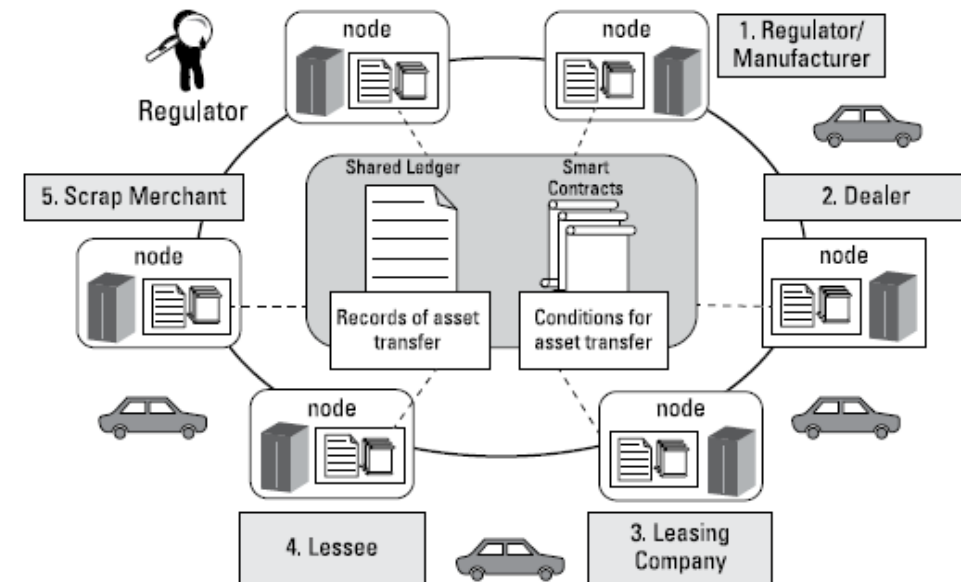
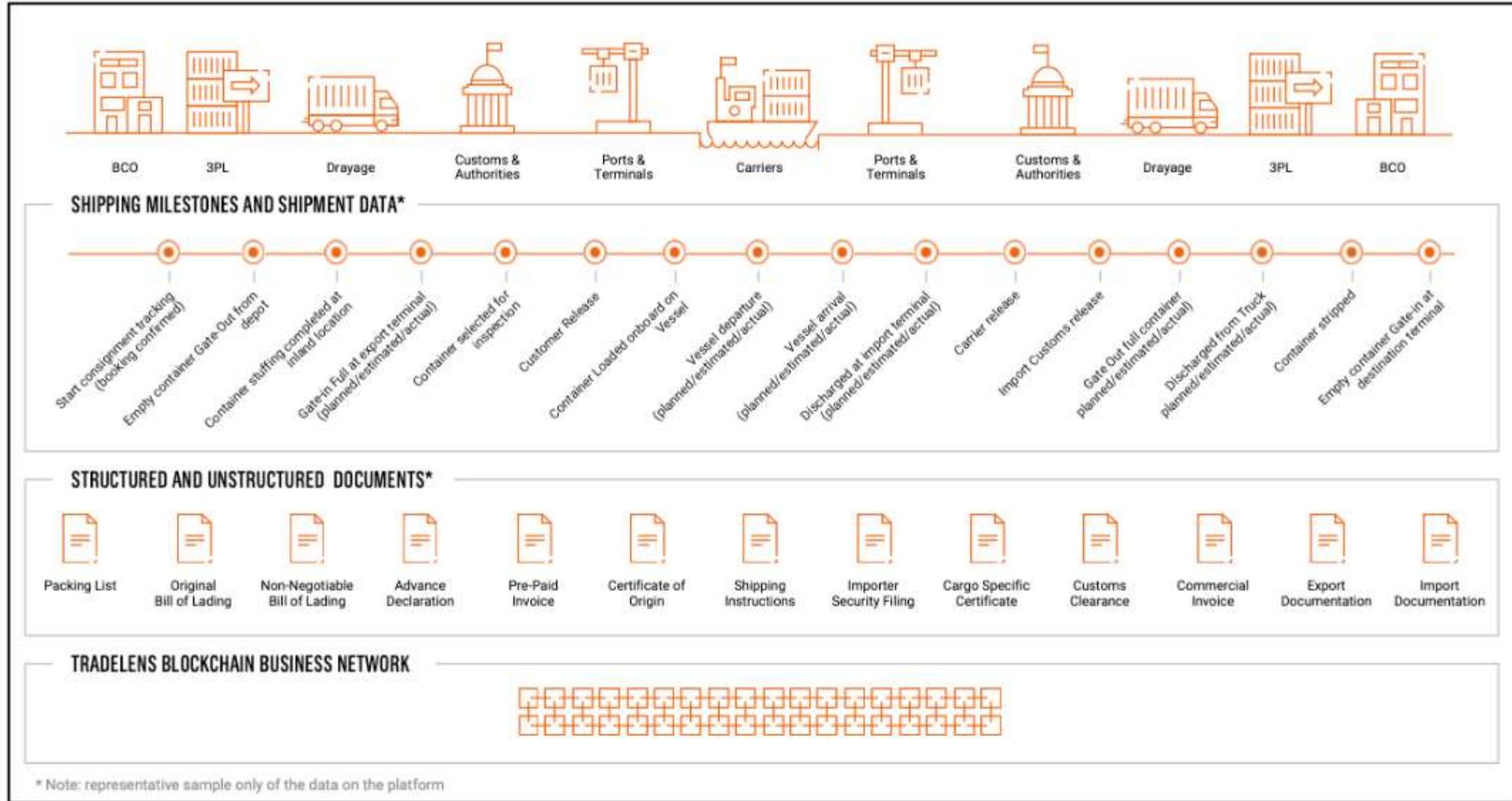


FIGURE 1-2: Tracking vehicle ownership with blockchain.



Types of Blockchains

- Public vs Private
 - Who can **write** data to the Blockchain?
 - Public – everyone can add a record
 - Private – only certain participants can write data
 - Consortium – more than one manages the blockchain (banks, gov organizations)
 - Hybrid – combines features from both

- Open vs Closed
 - Who can **read** data from the Blockchain?
 - Open – everyone can read Blockchain data
 - Closed – only certain participants can read data



Public or Private Blockchain

- Should the solution be a permissioned or permission-less Blockchain
 - Are all participants considered equal, or should some have abilities that others do not?
 - Election chairperson can add candidates to an election = permissioned
 - A digital currency which can exchanged and traded by all = permissionless



How Blocks are created



Blockchain Basics

Blocks



Mining



Consensus



Source: Blockchain Train Alliance

The “Blocks” of a Blockchain

Transactions are grouped
together into a Block

25 Transactions per Block





- Blocks are numbered in ascending order, 0 is first/oldest
- The number is the 'height' of the block
- Arrows only go from newer to older blocks - a block only directly links to the one immediately before it
- Once a block is stored, it's read-only (which is why it doesn't link to the ones after it - that would require you to update it)



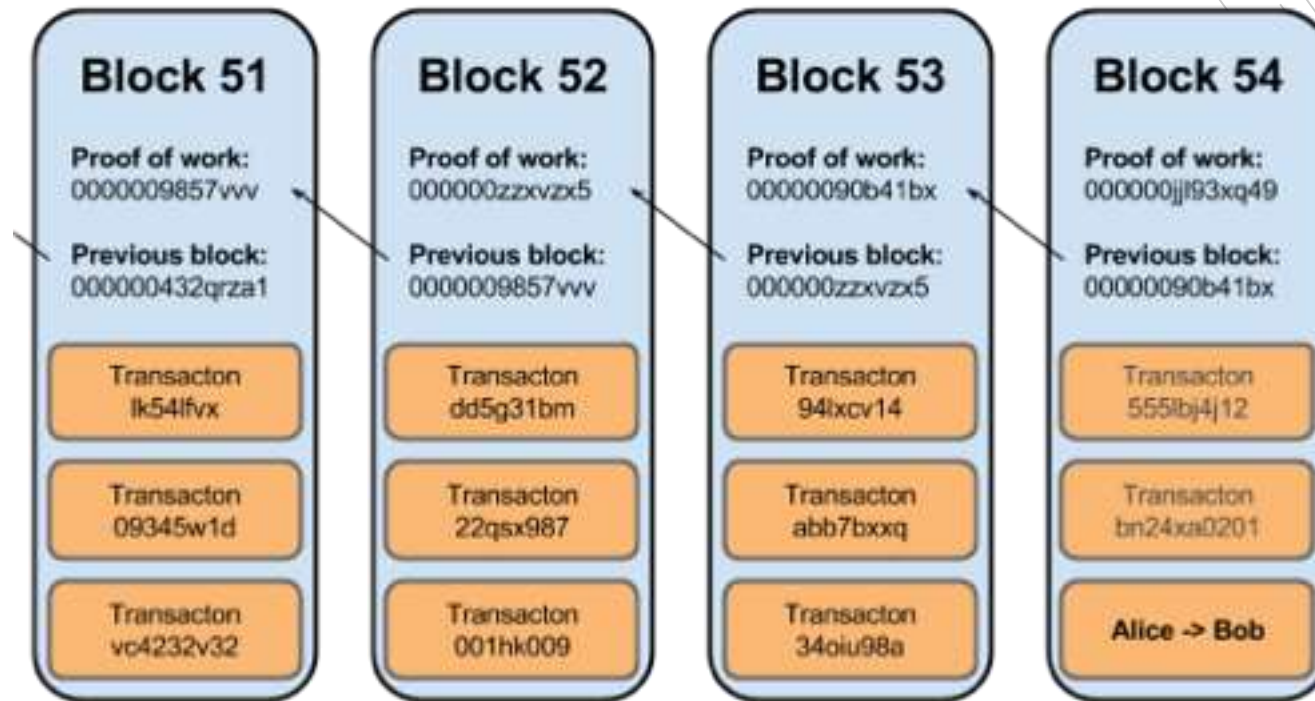
- Blocks store data, in Bitcoin, it's the transactions, but it could be any digital data
- Blocks are created periodically (on average, 10mins for Bitcoin) by a process called 'mining'
- A block represents a set of events that have occurred over a particular time frame (usually, since the previous block)

Blockchain Blocks



- Blocks aren't identified by their height, but by their id
- Block id is the hash of the **data** in the block
 - ✧ 0=000000000019D6689C085AE165831E934FF763AE46A2A6C172B3F1B60A8CE26F
 - ✧ 1=00000000839A8E6886AB5951D76F411475428AFC90947EE320161BBF18EB6048
 - ✧ 2=000000006A625F06636B8BB6AC7B960A8D03705D1ACE08B1A19DA3FDCC99DDBD
- Block id is a digital fingerprint of that block

What is in a Block?



The connection between blocks means that the Blockchain is much more *tamper-proof* than standard database structures. Since Blockchain is a ledger of records, this tamper-proof record of assets is known as an “Immutable Ledger”.

Mining a Block

- Mining is the process of adding transactions to the large distributed (among all users of a blockchain) public ledger of existing transactions distributed.
- Mining involves creating a hash of a block of transactions that cannot be easily forged, protecting the integrity of the entire blockchain without the need for a central system.
- Mining is done on a dedicated computer.



Mining a Block



- It requires a fast CPU. In 2009, could mine 200 Bitcoins with a personal PC. In 2015, it would take about 98 years to mine just 1 Bitcoin.
- Higher electricity usage.
- More heat generated than typical computer operations.
- Users who choose to use a computer for mining are rewarded for doing so. Bitcoin mining, rewards people who run mining operations with more bitcoins (12.5 bitcoins per hash, a maximum of 21 million Bitcoins can be generated).

Smart Contracts



Smart Contracts

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

Blockchain	Smart Contracts?
Bitcoin	No
Ethereum	Yes
Hyperledger	Yes
Others	Depends

Smart Contracts – what they do?

Example:

- The procedure for buying a car at a dealership, has several steps - a like frustrating process.
- If can't pay for the car outright, we'll have to obtain financing.
- Credit check requirement.
- Fill out several forms with our personal information to verify our identity.
- Interact with several different people, including the salesperson, finance bank personnel, credit risk personnel, insurance personnel etc.
- To compensate their work, various commissions and fees are added to the base price of the car (loan interest rate etc).

Smart Contracts – what they do?

With smart contracts all this complex process, is streamline

- With our identity stored on a blockchain, credit risk personnel can quickly make a decision about credit.
- Then, a smart contract would be created between our bank and our identity, so that once the funds have been released to the dealer, the bank will hold the car's title and repayment will be initiated based on the agreed terms.
- The insurance personnel will be informed to issue the insurance contract.
- The transfer of ownership would be automatic as the transaction gets recorded to a blockchain, is shared among the participants and can be checked at any time.

Blockchain platforms



- Corda
 - R3 is a consortium of world's leading financial institutions that built one of the open source blockchain platforms called Corda in 2015.
 - Cutting-edge blockchain platform, which enables institutions to transact directly with smart contracts by removing costly frictions in business transactions.
 - Does not have a cryptocurrency or built-in token and is a permissioned blockchain platform which only allows the authorized participants to access the data, not the entire network.
 - It enhances privacy and offers fine-grained access control to digital records.
 - More than 60 firms, including Intel and Microsoft, are using Corda as a blockchain platform.
 - HSBC, Intel, Bank of America Merrill Lynch, and dozens of other institutions have invested around \$107 million into R3 Corda. Uses Asynchronous Byzantine Fault Tolerance to reach the consensus between nodes.

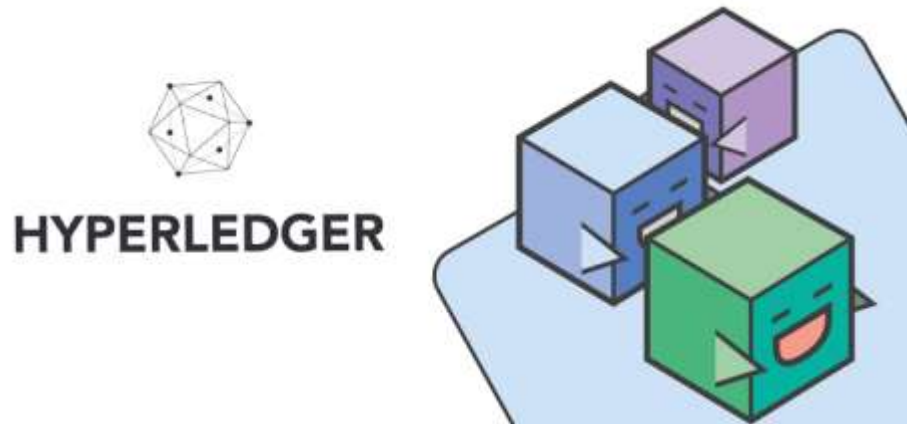
Blockchain platforms



- Ethereum

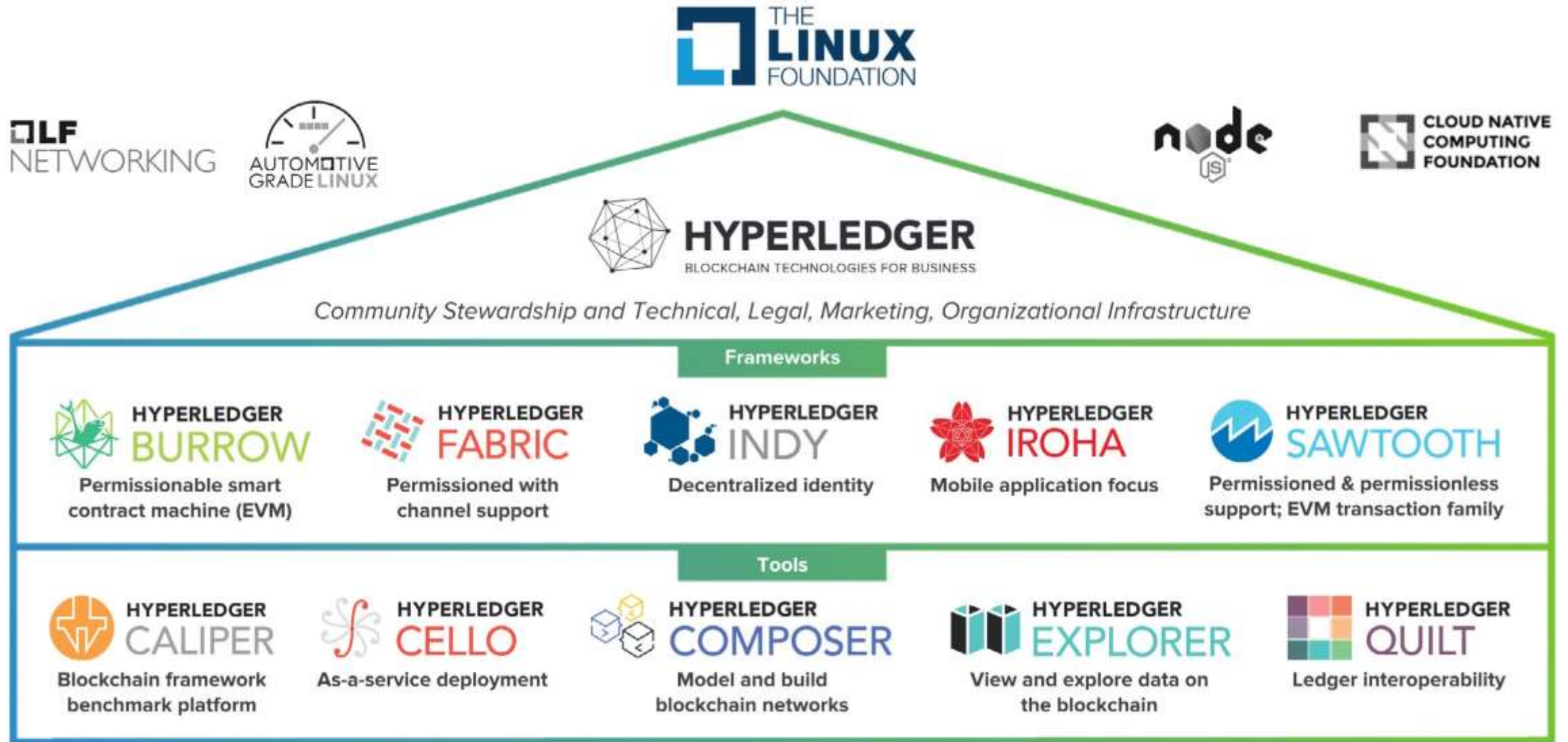
- Developed by Vitalik Buterin in the year 2014
- Open-source, used to develop decentralized blockchain applications
- Enables a run-time environment to run Smart Contracts built on Ethereum
- Ethereum Wallet, a gateway for decentralized applications, wallet for keeping ether and other crypto-assets built on Ethereum
- Industry Type: Cross-Industry
- Consensus Algorithm: Proof of Work
- Governance: Ethereum Developers
- Smart Contract Functionality: Yes
- Ledger Type: Permissionless

Blockchain platforms



- Hyperledger

- Hosted by the Linux Foundation
- Includes leaders in finance, banking, IoT, supply chain, manufacturing, and technology
- Business Blockchain Frameworks are hosted with Hyperledger
- Hyperledger Fabric: Blockchain platform for developing plug and play applications with modular approach
- Hyperledger Iroha: Founded by Linux Foundation, adherence to develop trusted, fast and secure decentralized blockchain applications. Compatible with Linux and Mac Os environment to build the supply chain and IoT solutions
- Hyperledger Sawtooth: Backed by Intel and founded by Linux, the most widely used **blockchain platform** that is used to create, execute and deploy distributed ledgers



Source: The Linux Foundation

Blockchain platforms



- Openchain
 - Developed by CoinPrism organization, is an open-source blockchain platform ideal for industries who want to handle their digital assets
 - A secure and scalable application powered by a partitioned consensus where you can have a single authority in validating transactions
 - One of the most efficient **blockchain platforms** as the transaction process is free of cost than any other **blockchain platform**
 - Industry Type: Digital Asset Management
 - Consensus Algorithm: Partitioned Consensus
 - Governance: Linux Foundation
 - Smart Contract Functionality: Yes
 - Ledger Type: Permissioned

Blockchain platforms



- Ripple
 - Aims to connect payment providers, digital asset exchanges, banks, and corporate via a blockchain network, RippleNet without any chargebacks.
 - Its digital asset called “XRP or Ripple,” is one of the popular cryptocurrencies like Ether and Bitcoin.
 - XRP is more scalable and faster than other blockchains.
 - Uses probabilistic voting to reach the consensus between nodes.
 - The Industry Focus is Financial Services, the Governance is done by Ripple Labs, it does not support Smart Contracts and Ledger Type is Permissioned.

Web 3.0/DeFi

BLOCK
CHAIN

- Web 1.0
 - first integration of the internet
- Web 2.0
 - Age of social media
 - Decentralized people
- Web 3.0 (Work in Progress)
 - Machine Learning/AI
 - Decentralize finance
 - Blockchain Based - Improve transaction speed
 - Trustlessness
 - Permissionlessness

■ Extensive use of Blockchain Applications



■ Barriers/Threats

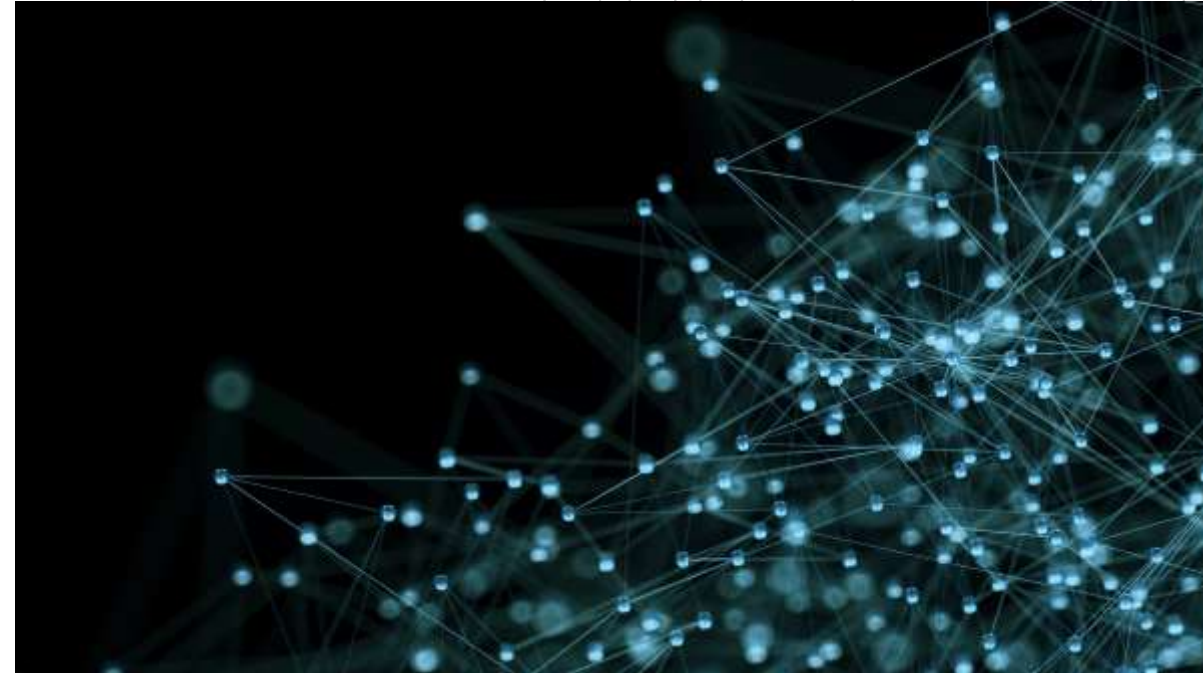
- legal risks
- regulatory risks
- lack of central control must take into consideration :
 - cybercrime
 - hate speech
 - misinformation

WEB 3.0 is the future and is coming !!!!



Decentralized Finance - DeFi

- Emerging financial technology
- Based on DLT
- P2P digital exchanges
- Use smart contracts on blockchain
- Primarily on Ethereum
- Absence of intermediaries
- DApps – Decentralized Applications
- Uniswap – Decentralized exchange – trade tokens to Ethereum





THANK YOU

