Evolution of Blockchain

SO, …WHAT IS BLOCKCHAIN?

"Blockchain technology" means a mathematically secured, chronological, and decentralised consensus ledger, or database, whether maintained by internet interaction, peer- to-peer network, or otherwise.

Vermont (US, Legislative Code) Rule of Evidence 902 §1913 (2016)

A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.

Vitalik Buterin (2015)

Blockchain is a distributed database that maintains a **chain** (i.e., chronologically ordered) of **blocks** (i.e., transaction records).

SATOSHI NAKAMOTO'S ORIGINAL POST – 11 FEB. 2009

P2P foundation

The Foundation for Peer to Peer Alternatives

Main | My Page | Members | Videos | Forum | Groups | Blogs | Chat

All Discussions | My Discussions | + Add

Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

Pre-History of Common Ledger

A unique form of currency that is several hundred years old:

- very big and heavy, “mined” on a different island,
- deposited in at one place, and were never moved,
- no ornamental value, no industrial use

- long history (chain) of custody & transactions recognised by community,
- communal agreement that was important

PRE-HISTORY OF COMMON LEDGER

RAI STONES FROM
YAP ISLAND

MARKET CAPITALISATION OF TOP 10 CC's (FEB, 2018)

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$138,393,150,858	$8,217.84	$10,702,500,000	16,840,575 BTC
2	Ethereum	$84,056,127,632	$863.33	$5,496,780,000	97,362,911 ETH
3	Ripple	$29,161,573,355	$0.747556	$1,918,970,000	39,009,215,838 XRP *
4	Bitcoin Cash	$18,822,278,178	$1,110.78	$769,661,000	16,945,100 BCH
5	Cardano	$8,021,705,989	$0.309395	$716,862,000	25,927,070,538 ADA *
6	NEO	$6,647,680,000	$102.27	$381,570,000	65,000,000 NEO *
7	Litecoin	$6,587,160,949	$119.70	$652,153,000	55,032,883 LTC
8	Stellar	$6,262,434,175	$0.339773	$212,880,000	18,431,229,602 XLM *
9	EOS	$5,439,778,186	$8.45	$1,017,680,000	643,450,810 EOS *
10	NEM	$4,457,457,000	$0.495273	$46,401,200	8,999,999,999 XEM *

BLOCKCHAIN UZBEKISTAN

- Uzbekistan Sets Plans to Dominate the Asian Blockchain Industry In Motion
- Uzbekistan Will Integrate Blockchain Technology Into a Huge Chunk of Its Economy
- President of Uzbekistan Signs Decree on Blockchain Integration, Tax Exclusions for Crypto
- Uzbekistan Creates State Blockchain Development Fund
- First pilot introduction of blockchain technology in Uzbekistan

- Estonia is one of the world's most digitally advanced societies
  - In 2005 Estonia became the first state to hold elections over the Internet
  - In 2014 the first state to provide e-residency by using Blockchain
  - Estonia is on the cutting edge of using blockchain to run a fully digital infrastructure, with plans for their own cryptocurrency in the works.

guardtime

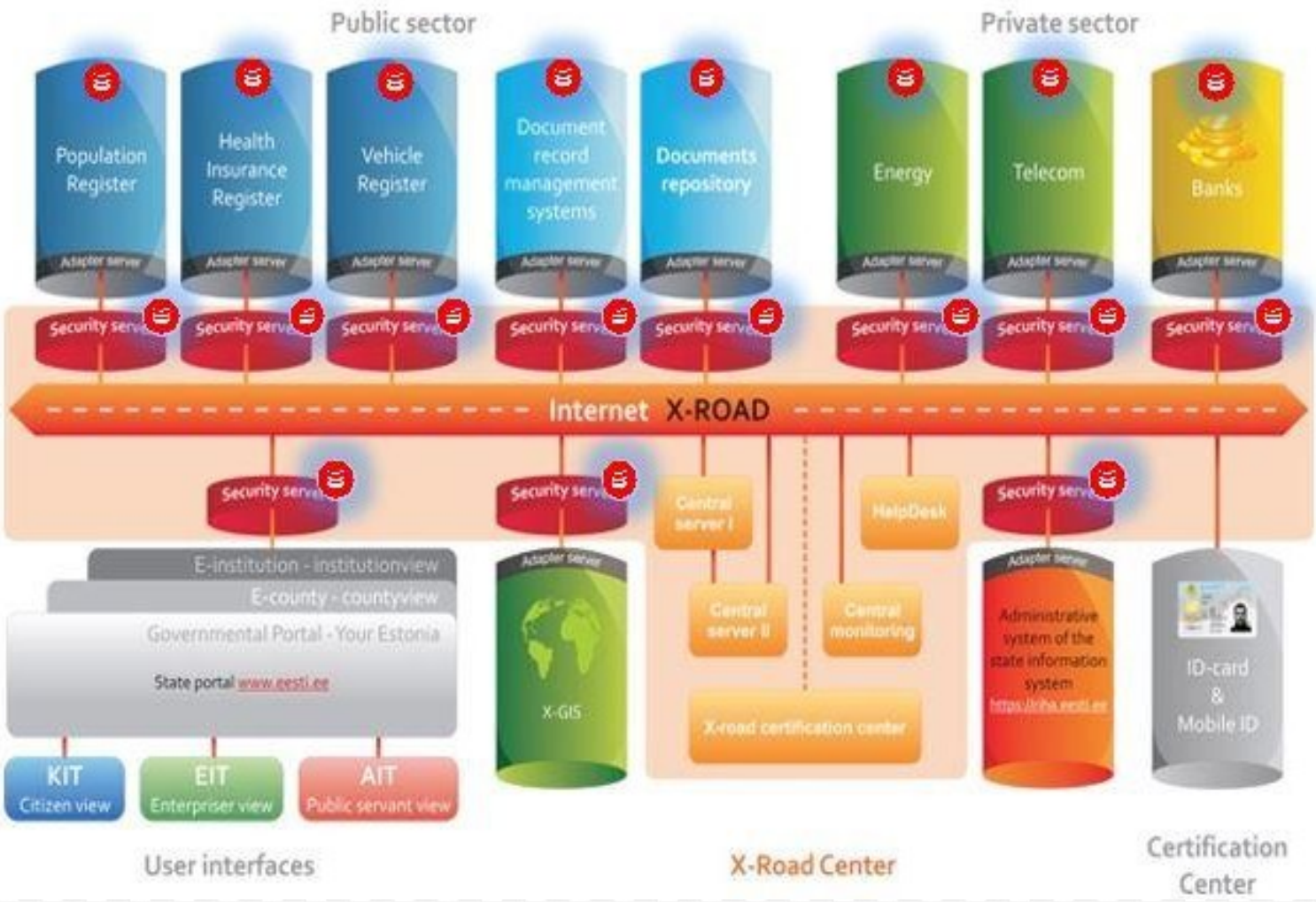
Blockchain Integration Points

Estonia: 100% Government Data on Blockchain

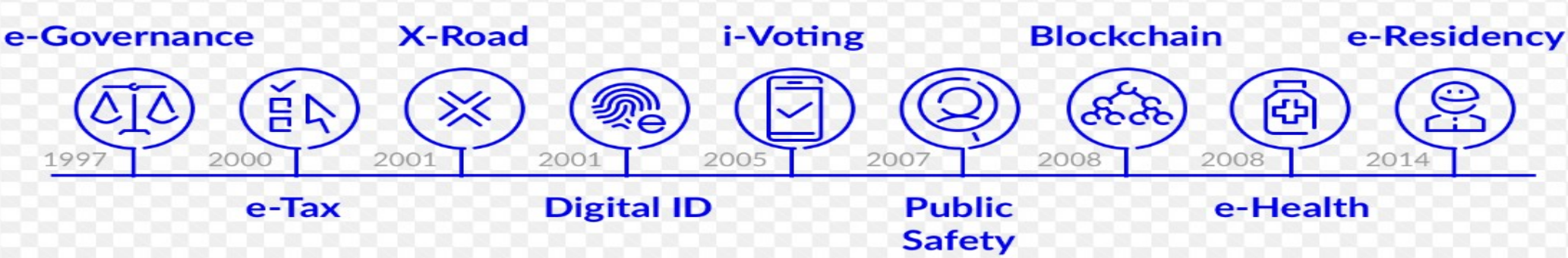
Blockchain is implemented as an integrity layer throughout Estonian Government Networks.

Network Segregation of Government Departments

There is complete transparency and accountability between citizens and government.



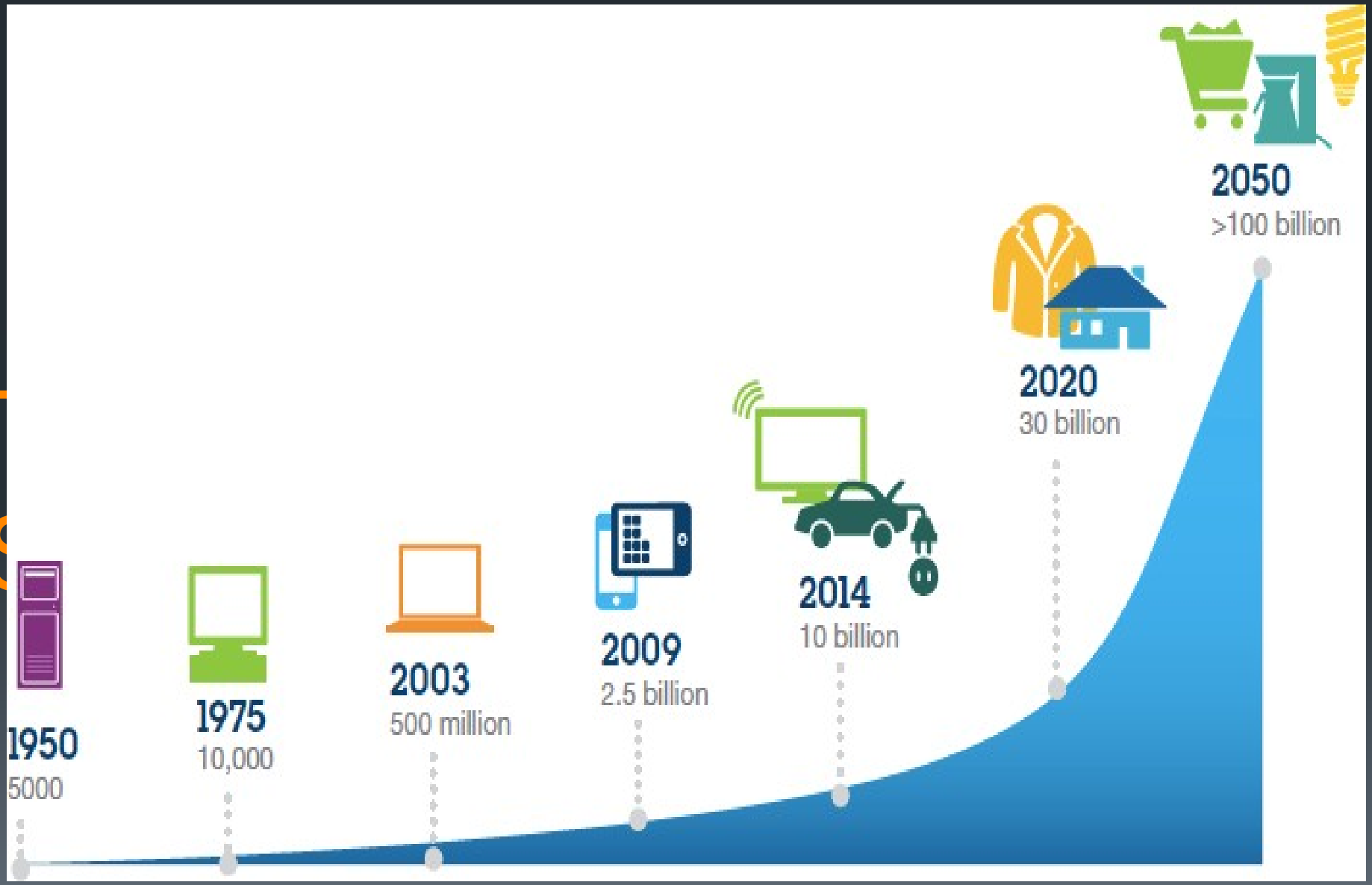
REPUBLIC OF ESTONIA GOVERNMENT



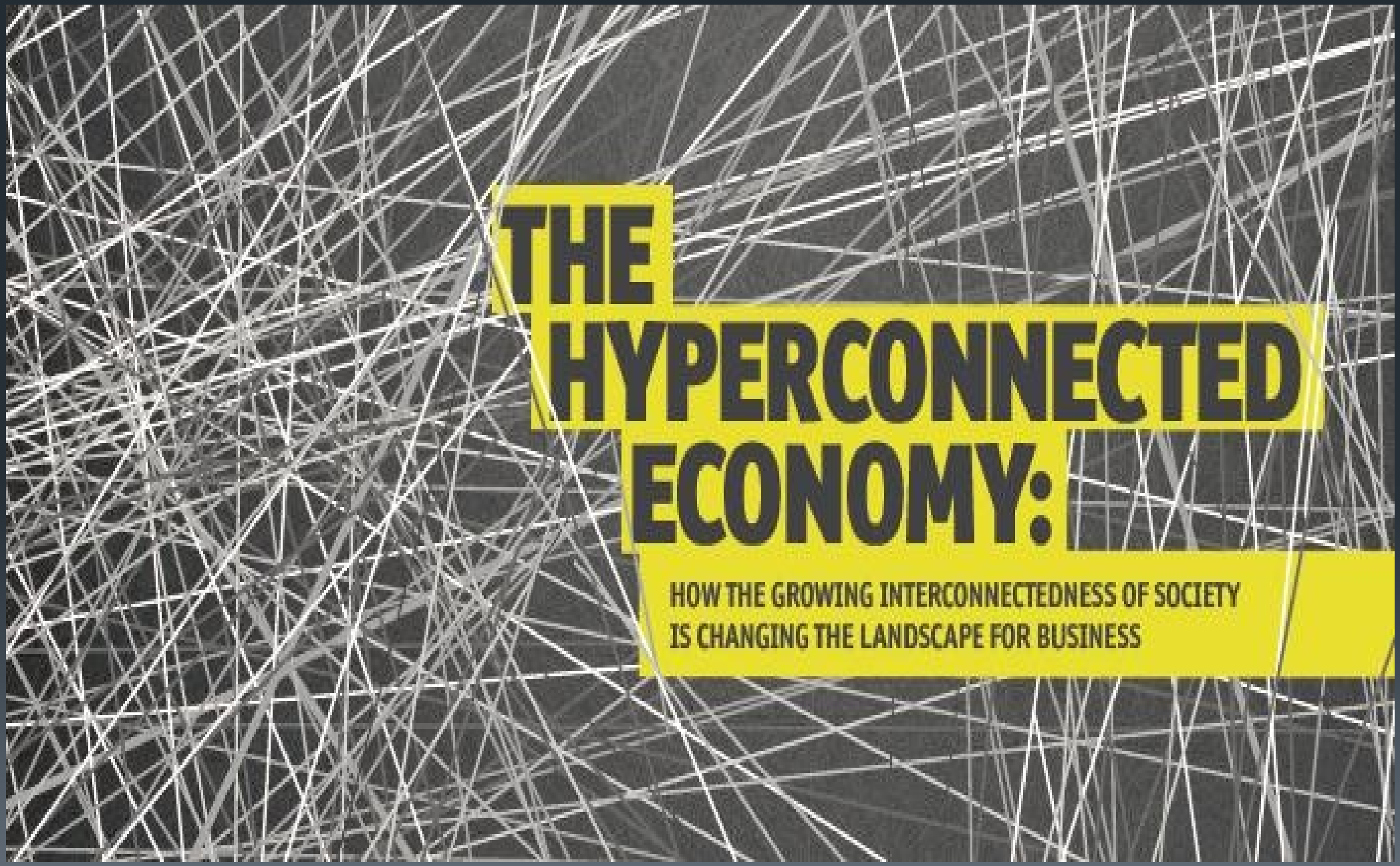
Block chain and IoT

- Blockchain and IoT
- Towards a Hyper-Connected Society
- Issues of Centralized IoT
- Evolution to Decentralization
- Blockchain
- Blockchain of Things
- The Future of Commerce
- Convergence of IoT, Blockchain, and AI
- Review Questions

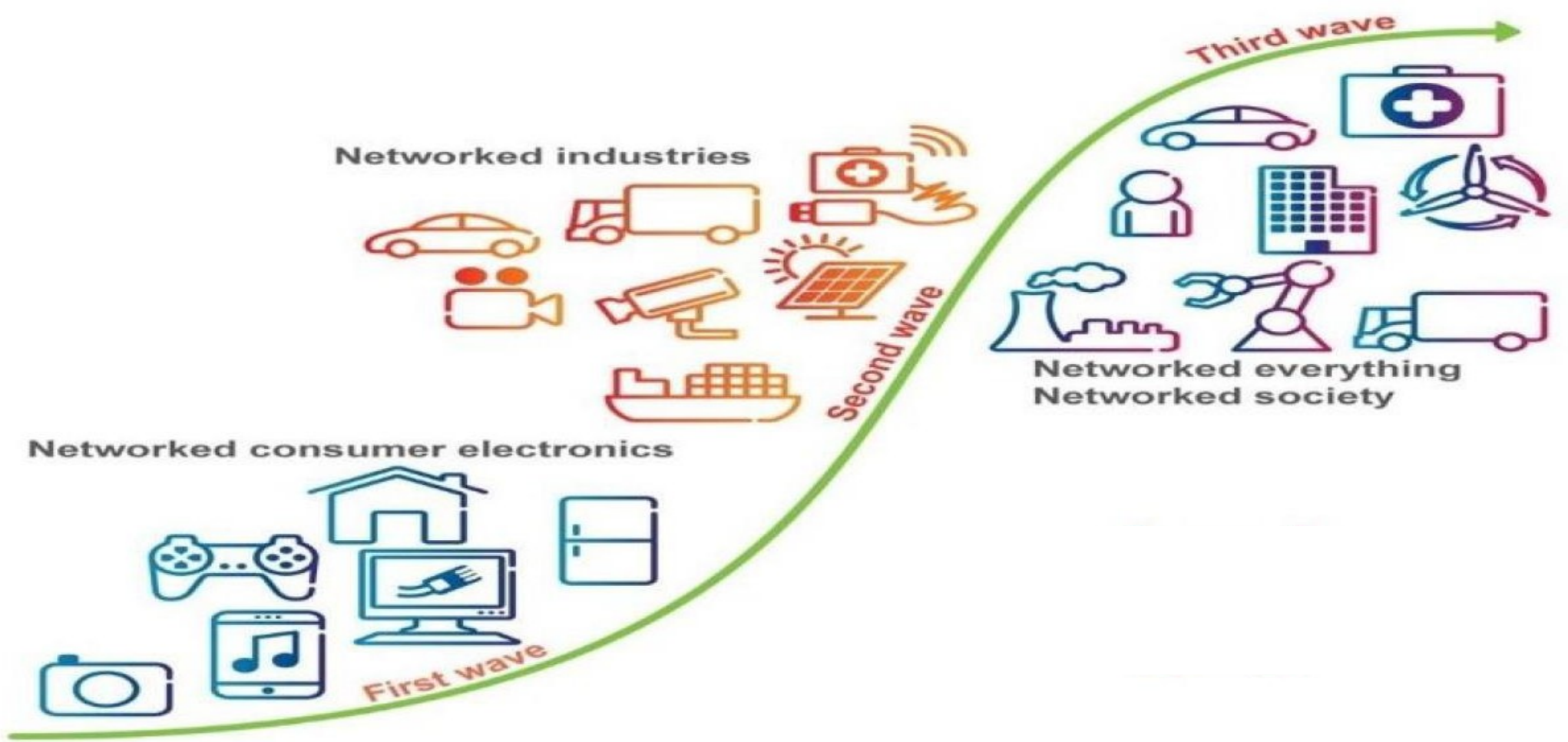
Internet devices will increase from 10 billion in 2014 to 30 billion in 2020 and 100 billion in 2050



Towards Hyper Connected Society



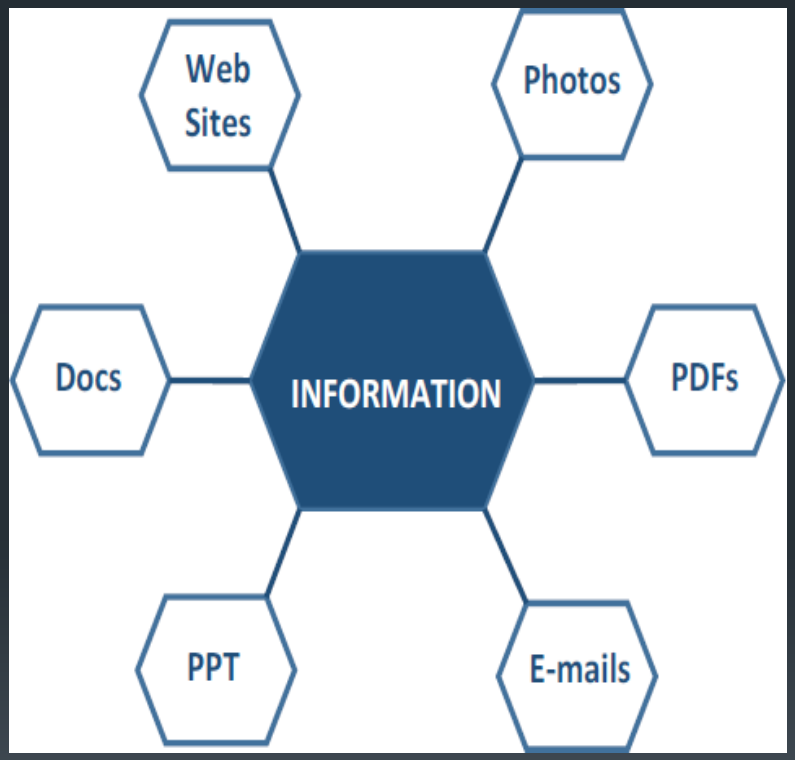
The emergence of a hyper-connected society will enable collaboration among network members without the involvement of third parties, and the development of a new type of platform capable of securing transparency and stability



Towards Hyper Connected Society

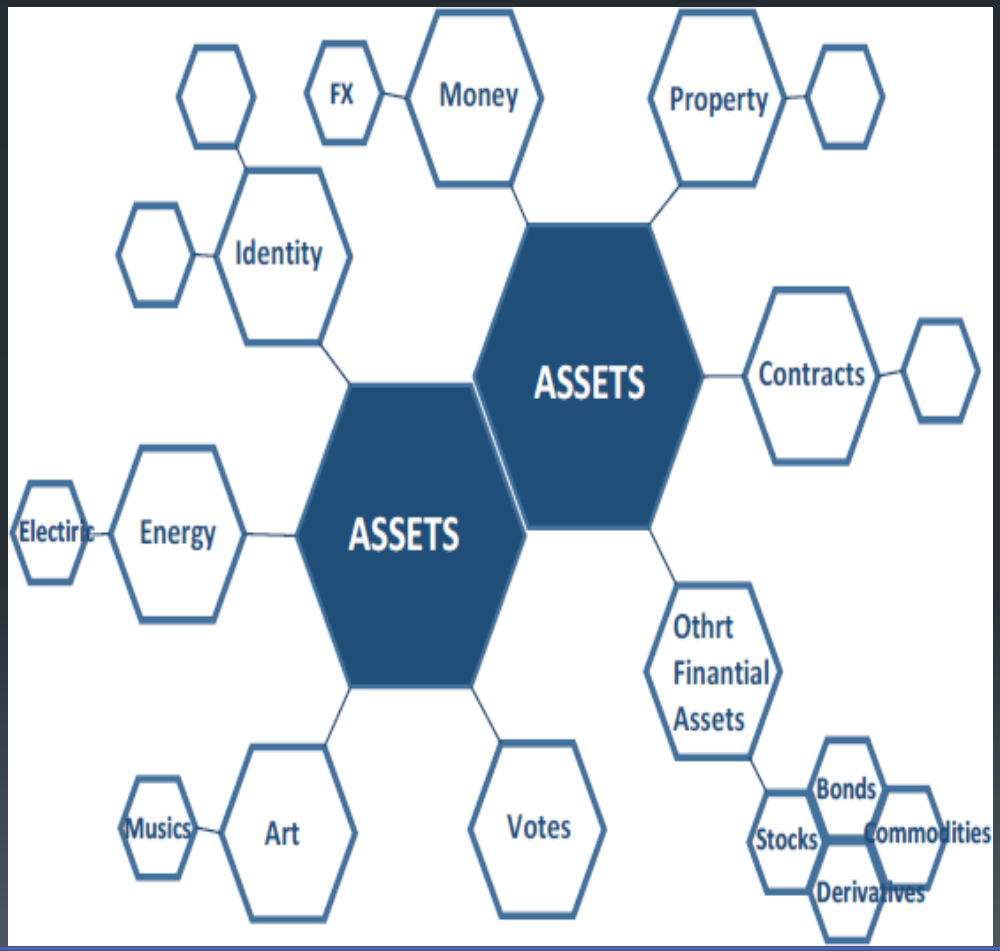
From Information Network to Value Network

Internet for Information



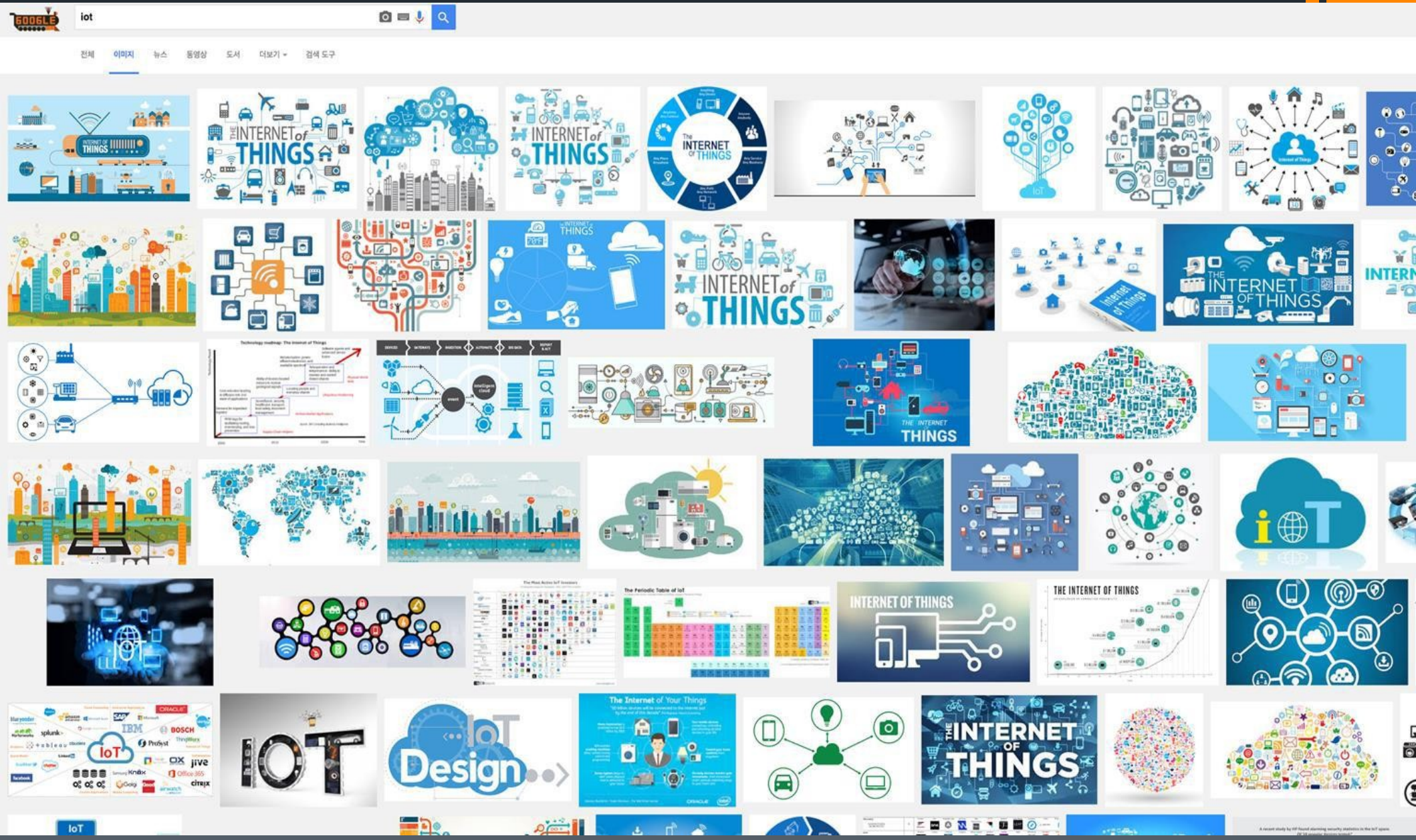
Information can be copied easily

Internet for Value

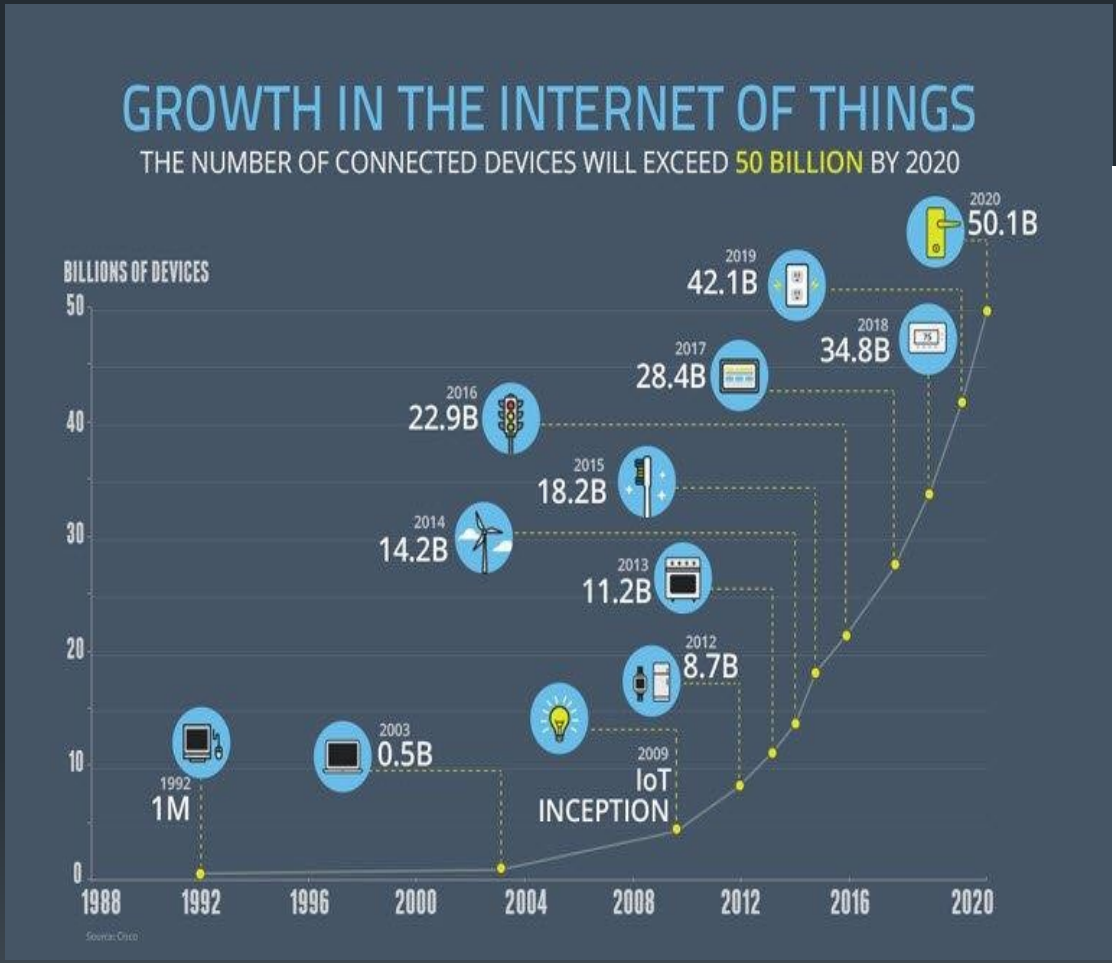


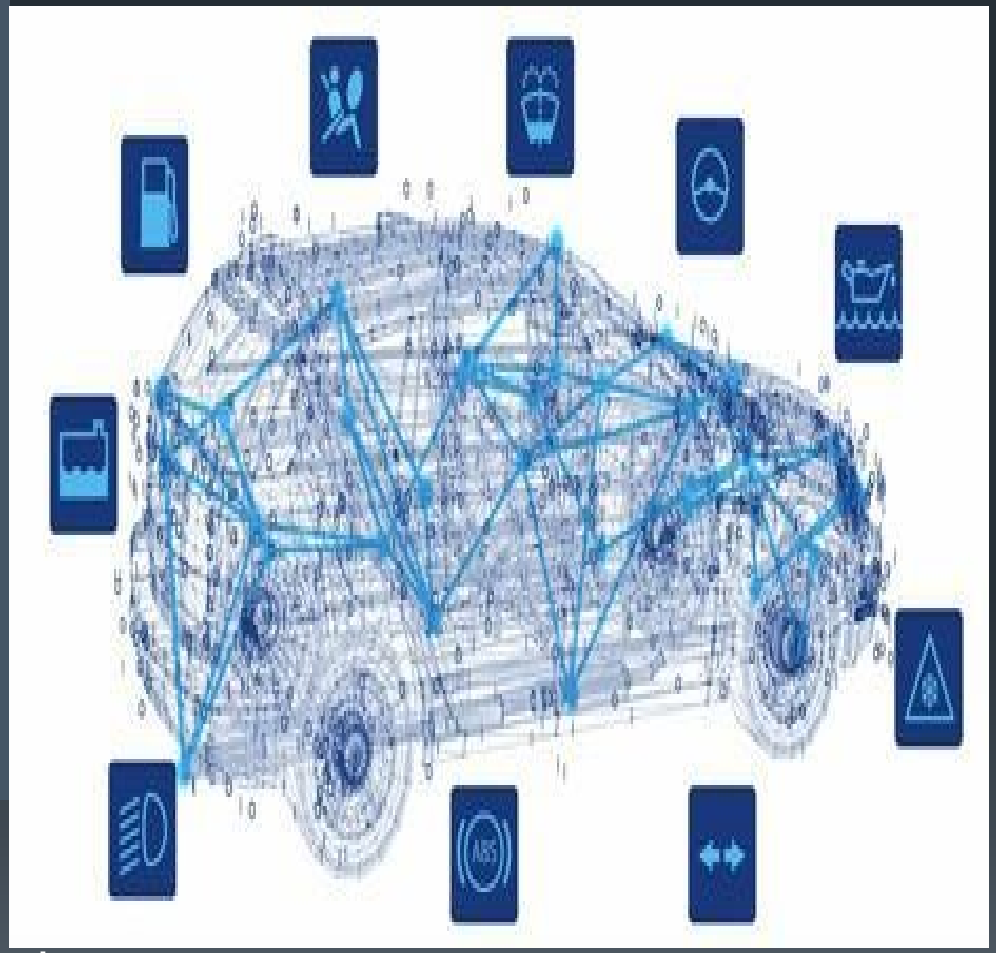
Can not send assets with purchasing power or value

Issues of Centralized IoT



IoT
Scale

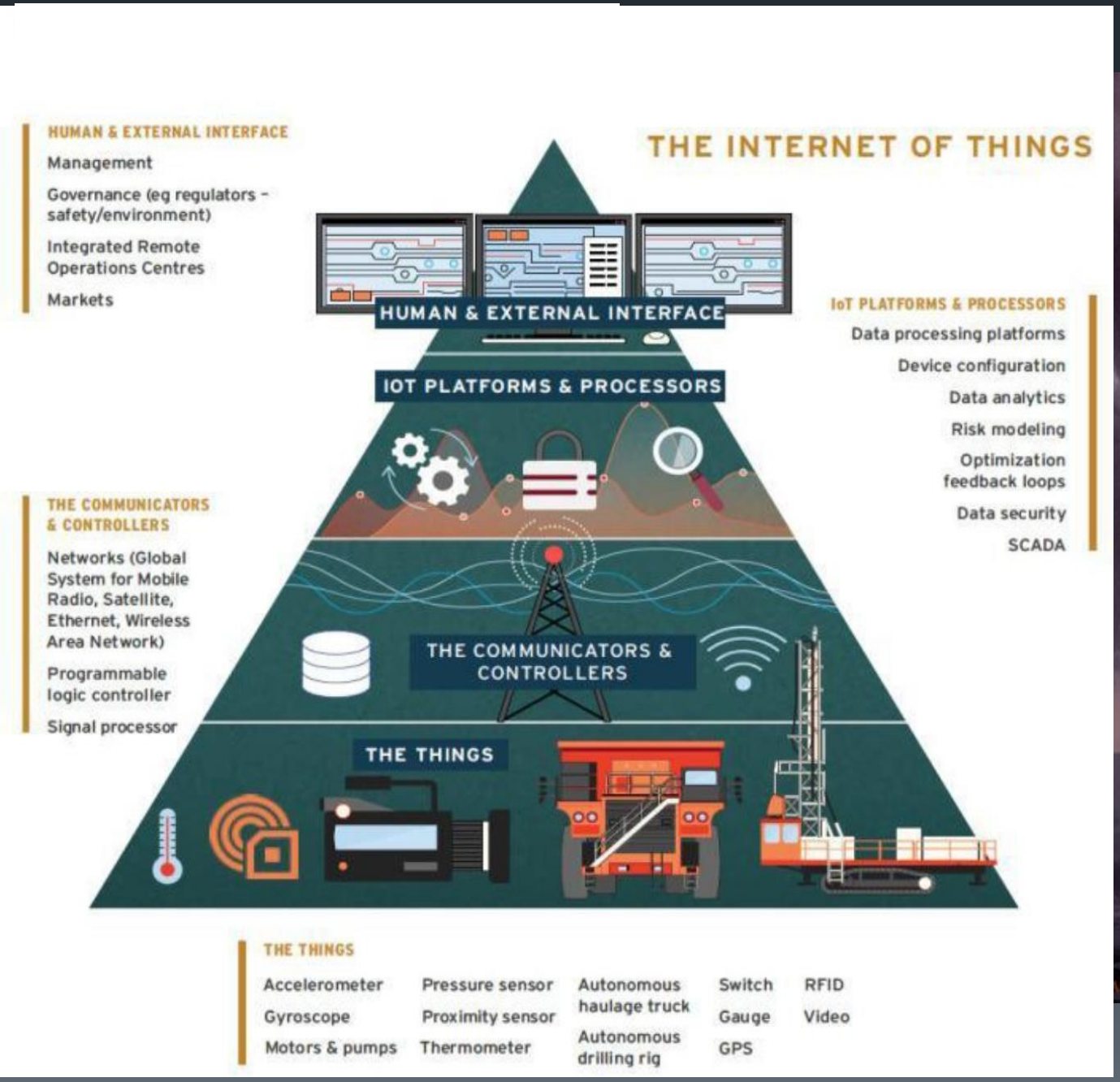




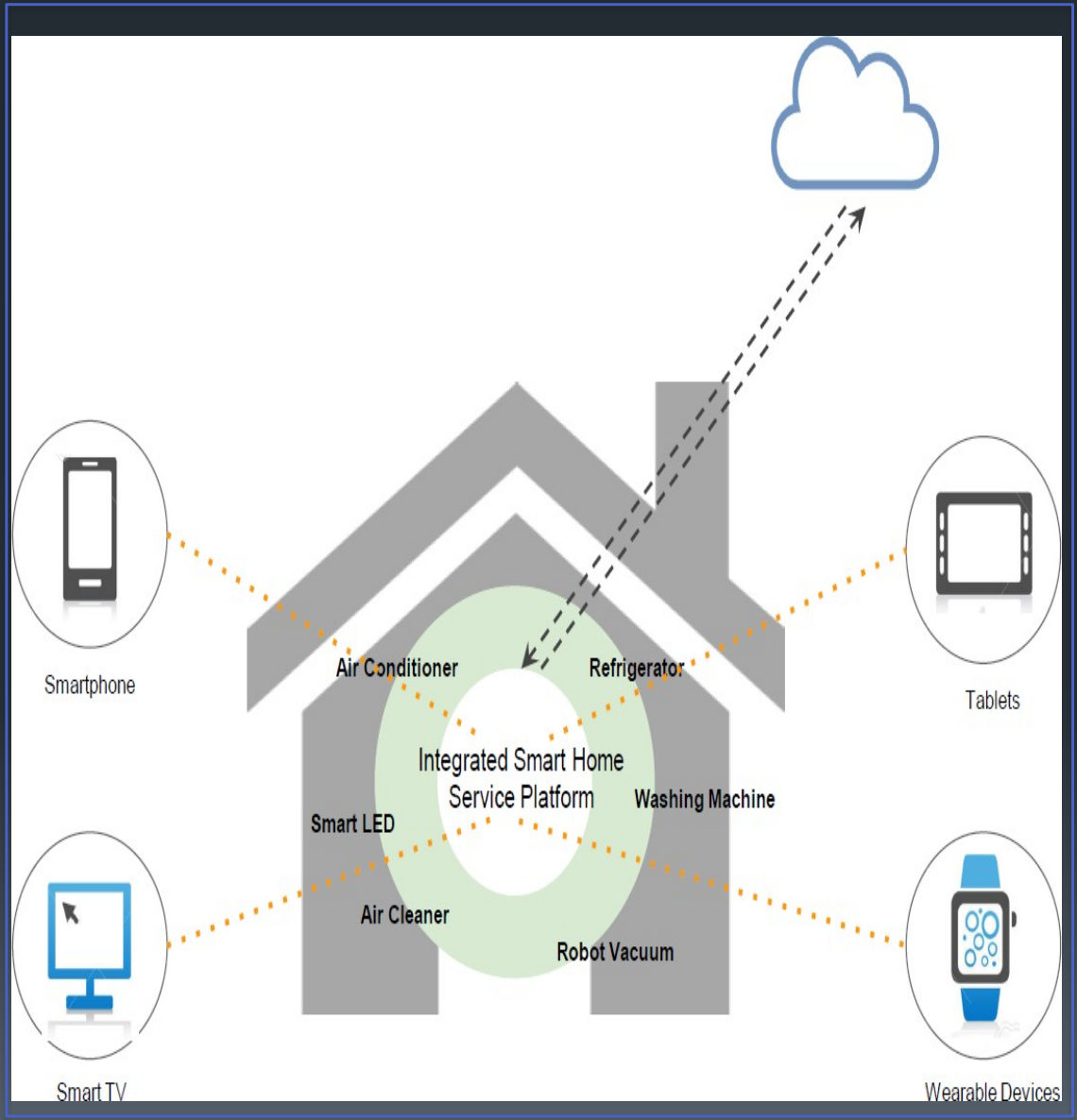
Future Connected Car to Send 25GB to Cloud Every Hour, Representing 130TB Per Year! - by Storage newsletter

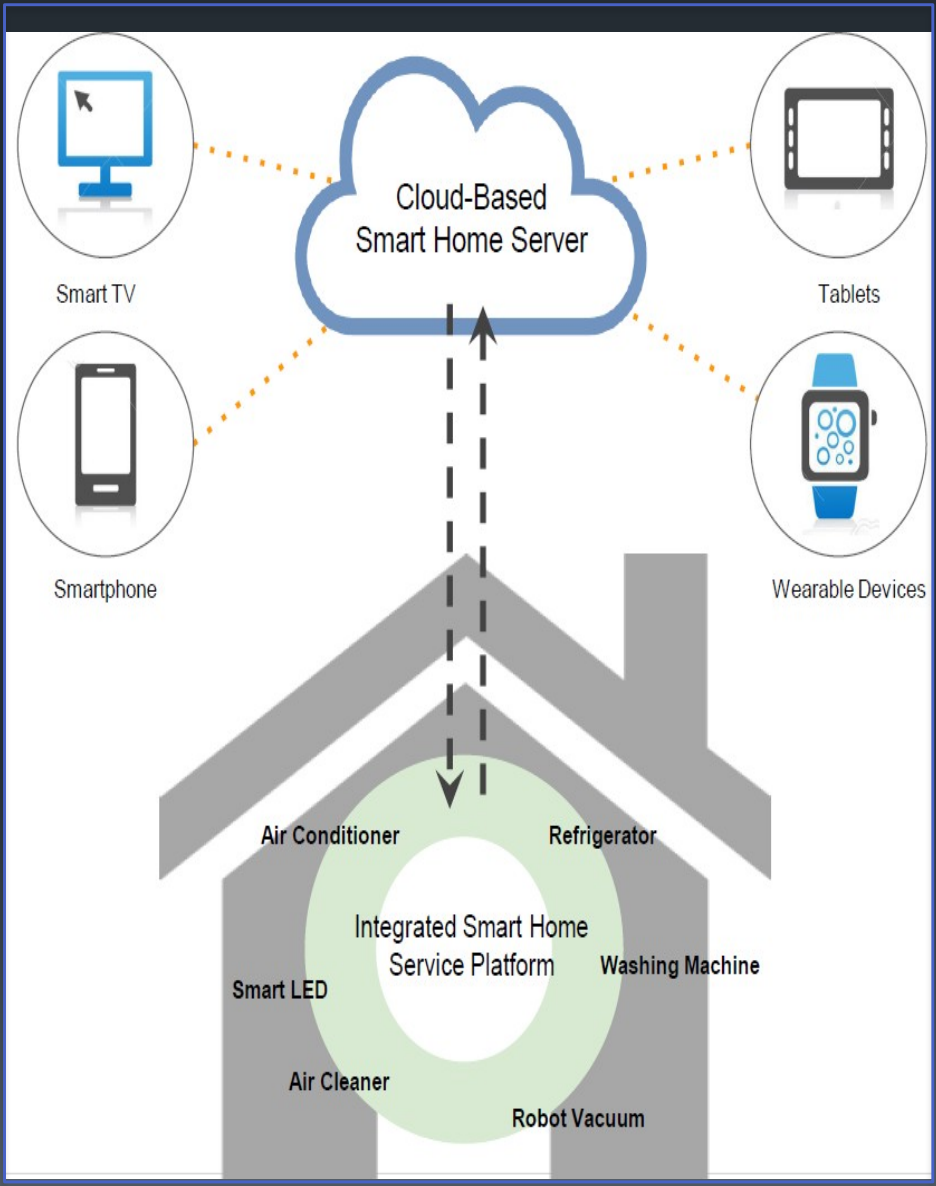
IoT

Scop


THE INTERNET OF THINGS
HUMAN & EXTERNAL INTERFACE
Management
Governance (eg regulators – safety/environment)
Integrated Remote Operations Centres
Markets
HUMAN & EXTERNAL INTERFACE
IOT PLATFORMS & PROCESSORS
IoT PLATFORMS & PROCESSORS
Data processing platforms
Device configuration
Data analytics
Risk modeling
Optimization feedback loops
Data security
SCADA
THE COMMUNICATORS & CONTROLLERS
Networks (Global System for Mobile Radio, Satellite, Ethernet, Wireless Area Network)
Programmable logic controller
Signal processor
THE COMMUNICATORS & CONTROLLERS
THE THINGS
THE THINGS
Accelerometer
Gyroscope
Motors & pumps
Pressure sensor
Proximity sensor
Thermometer
Autonomous haulage truck
Autonomous drilling rig
Switch
Gauge
GPS
RFID
Video

IoT
Dependency





IoT
Privacy

Issues of Centralized IoT

Solutions for the Issues

Problems of Centralized IoT	Solutions
Low security	• Distributed ledger technology to secure individual participant • Preventing hacker attacks with public key encryption
Privacy	• Using both the public key and private key secures privacy.
Information monopoly	• All information is shared anonymously without a central manager, making it difficult to monopolize information
High operating costs	• No centralized center, no separate operating costs

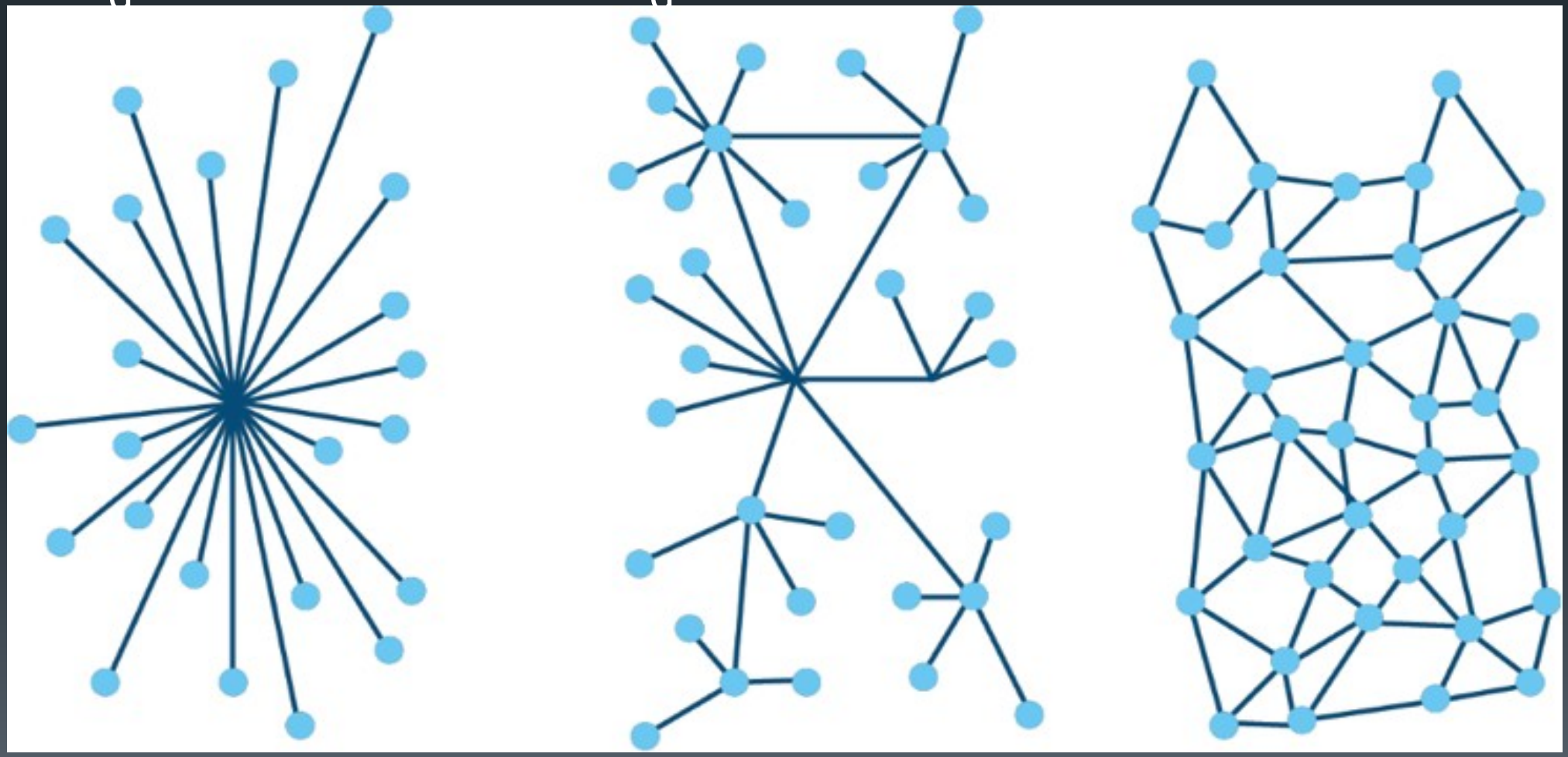
Evolution to Decentralization

The Network Alternatives

Centralized

Decentralized

Distributed



Evolution to Decentralization

Decentralized and Distributed Networks

Distributed Fog/Edge Computing and Blockchain Netwoks

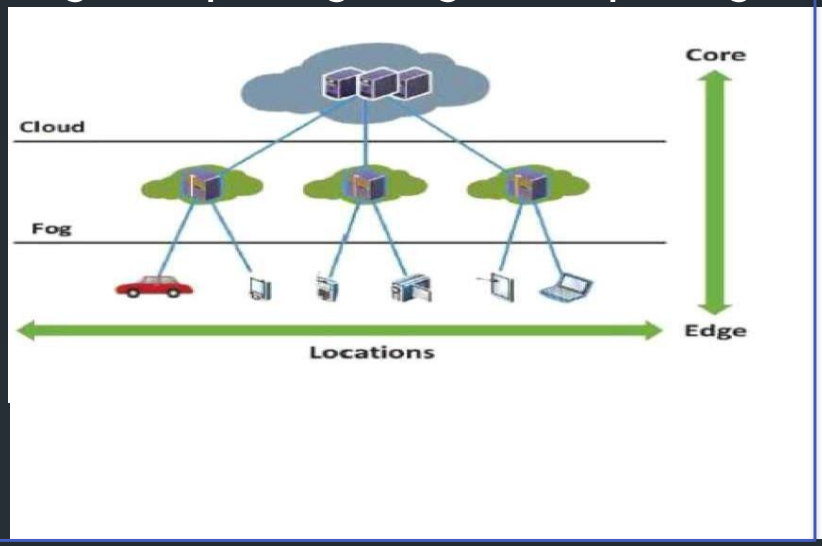
Advantages of Centralized Cloud

- High utilization due to virtualization
- Pay as much as you use
- Cheap power cost
- No restrictions on location
- Homogeneous computing, storage, network configuration
- Low OPEX cost

Disadvantages of Centralized Cloud

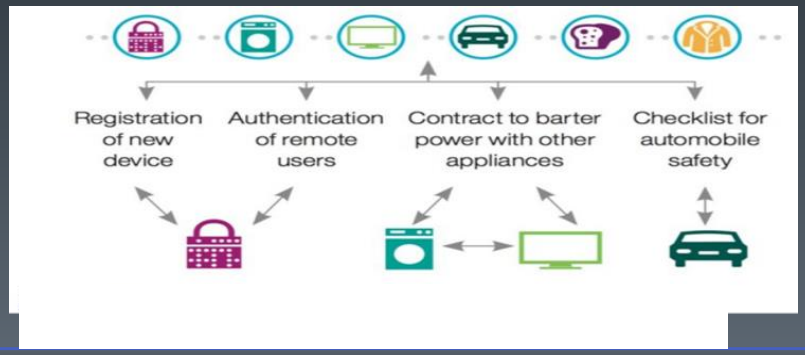
- High load due to function concentration
- Requires wide bandwidth to send and receive large amounts of data
- Needs to stay connected
- Problems in real-time processing application operation

Fog computing/Edge computing



Blockchain

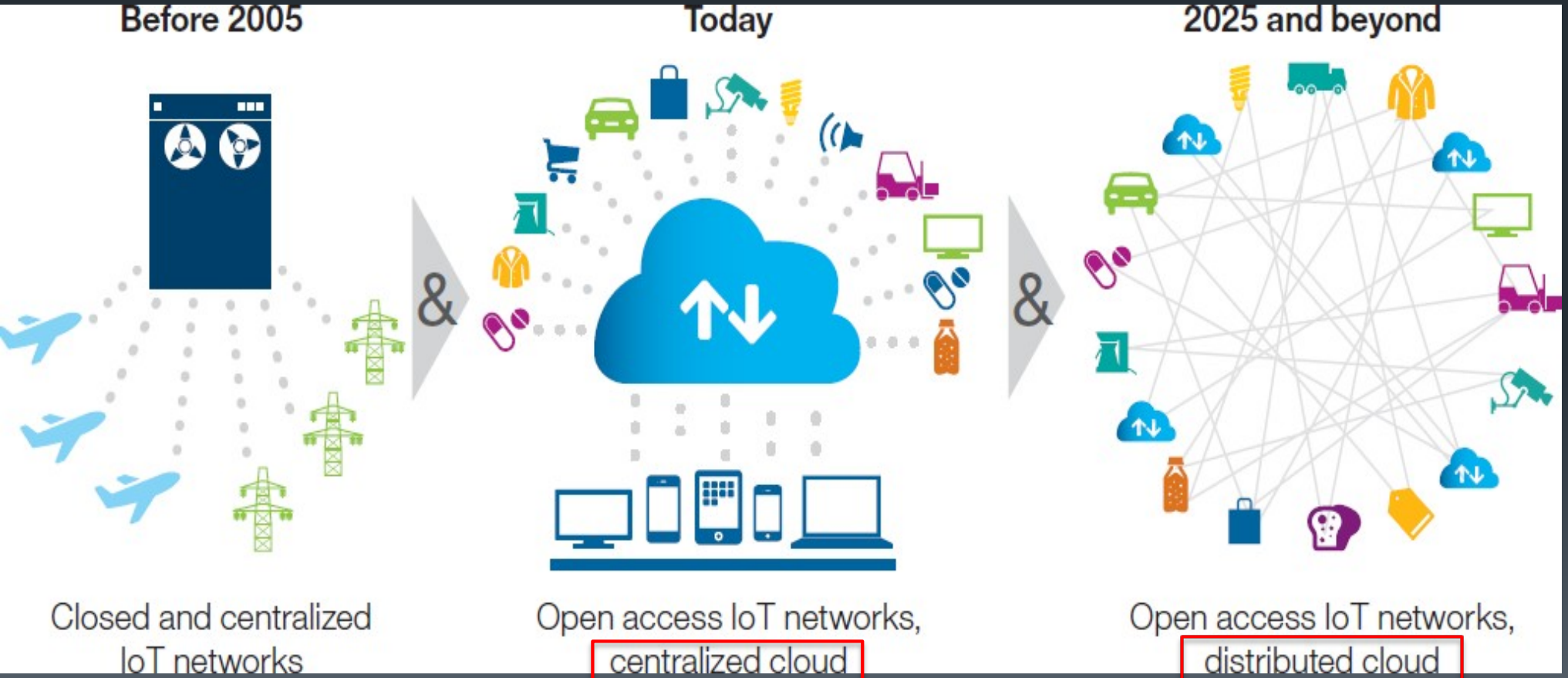
Distributed Assets Network



Evolution to Decentralization

From Centralized Cloud to Distributed Cloud

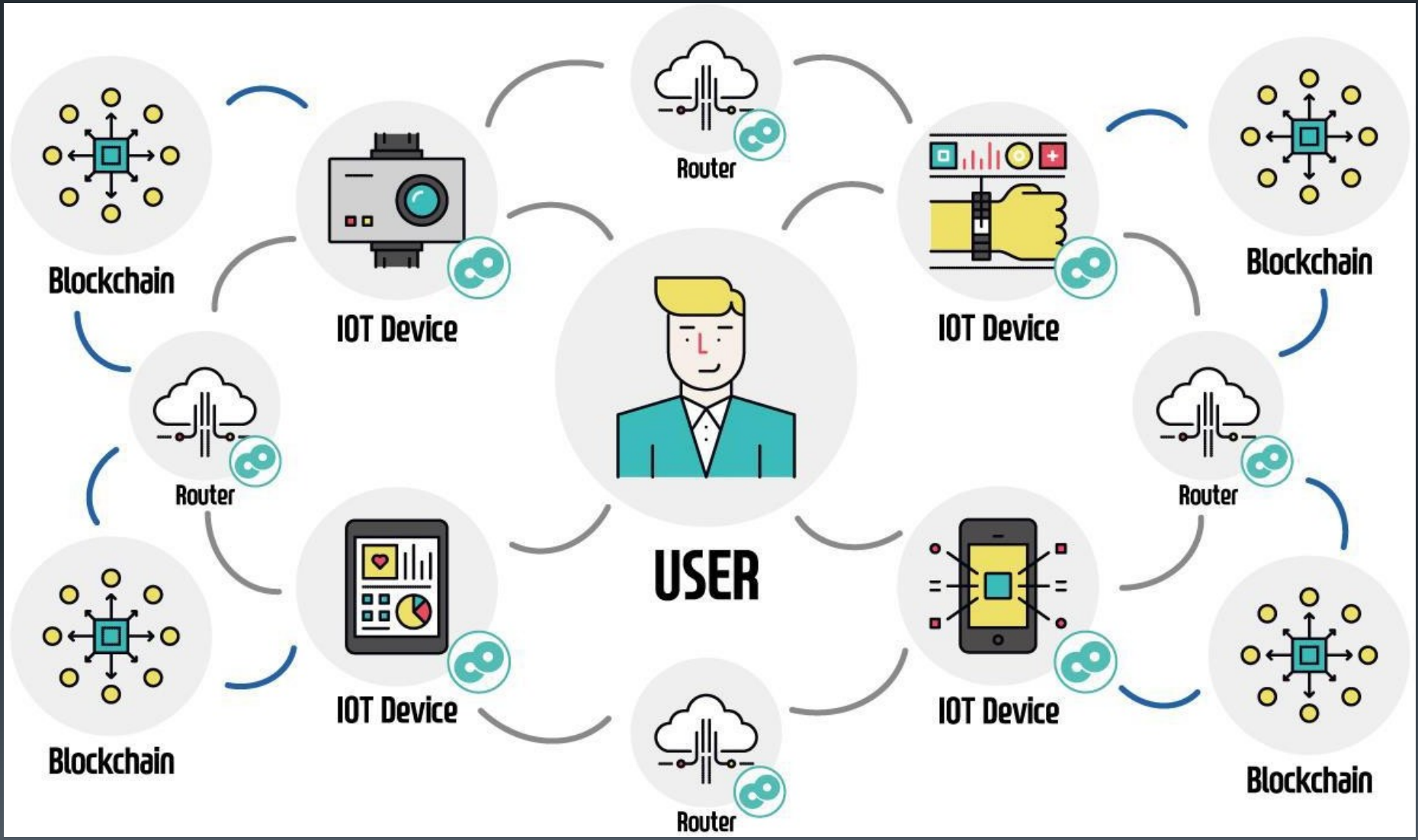
- The Hyper-connected society needs collaboration, transparency, knowledge sharing
- Distributed cloud has an optimized structure to support it

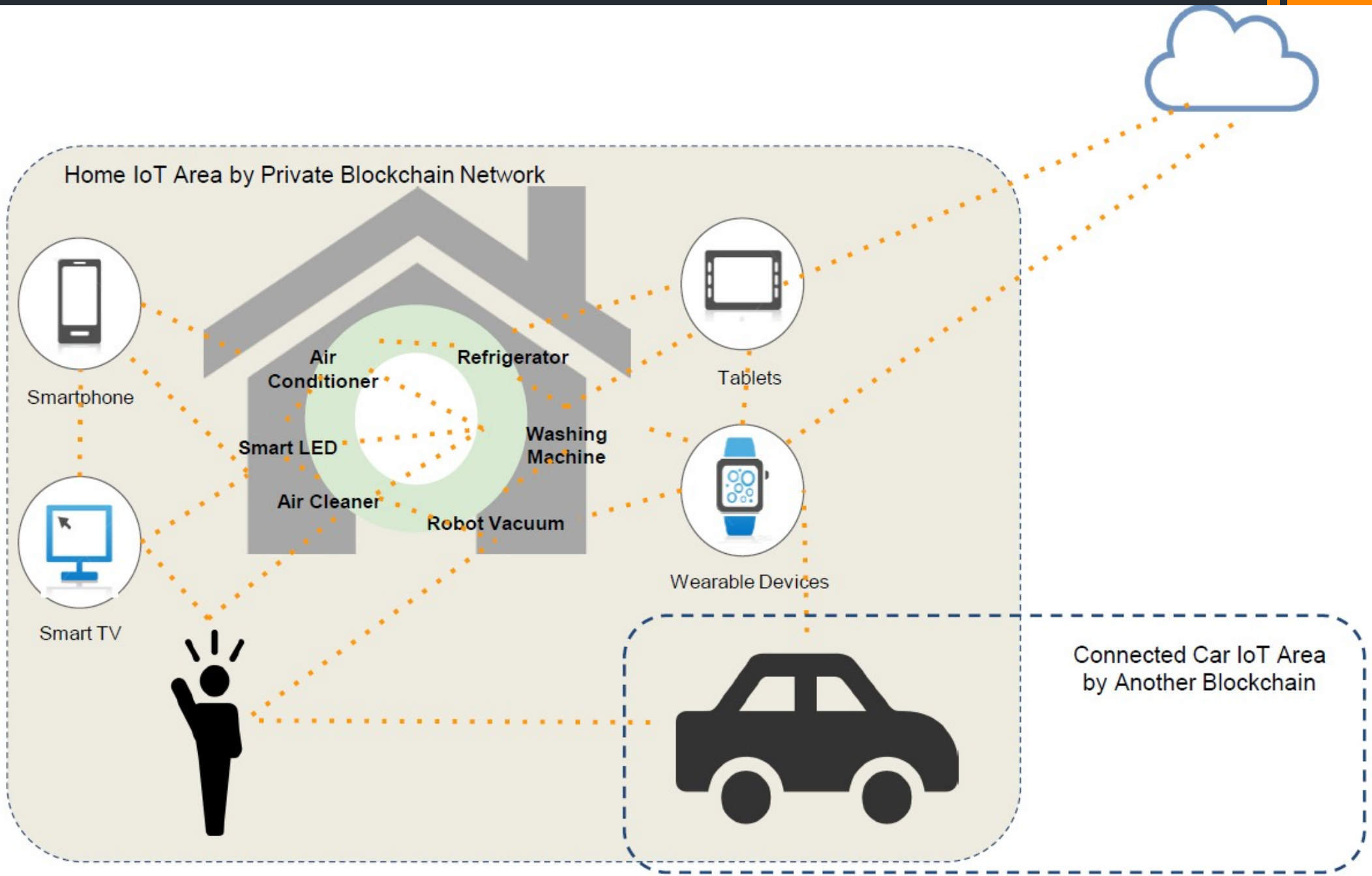


(Ubiquitous Sensor Network:USN
Machine to Machine Network: M2M)

Evolution to Decentralization

Smart IoT Device with Blockchain




Home IoT Area by Private Blockchain Network
Smartphone
Smart TV
Air Conditioner
Refrigerator
Smart LED
Washing Machine
Air Cleaner
Robot Vacuum
Tablets
Wearable Devices
Connected Car IoT Area by Another Blockchain

Blockchain

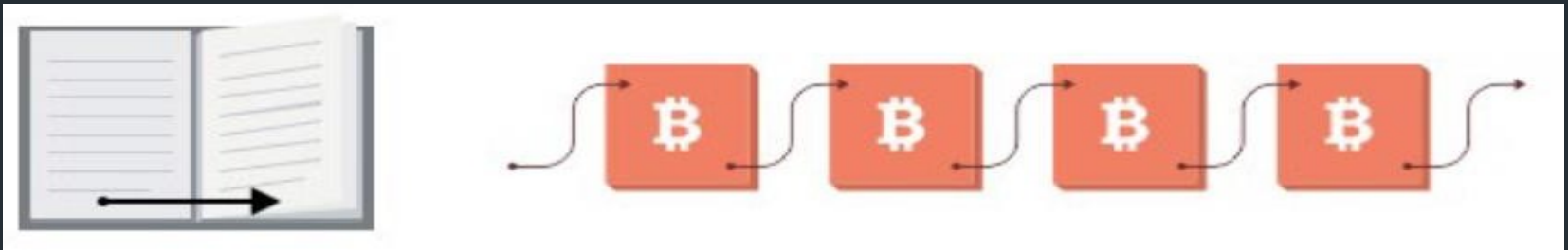
- Definition and Overview
- Evolution
- Concepts
- How Blockchain Works
- Types
- Protocols
- Virtual Currencies
- Ethereum
- Hyperledger

Definition

- Blockchain is the technology behind Bitcoin
- Bitcoin was created by Satosh Nakamoto in 2008
- A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography.
  - Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.
- A blockchain is immutable – no one can change the data once it's been written on the chain

Overview
(1/2)

- A Blockchain is just a file (data structure)
  - Blocks in a chain refer to previous blocks, like page numbers in a book



- Blockchain has become a new paradigm to change existing business processes.
  - One of the key technologies to lead the era of the Fourth Industrial Revolution (World Economic Forum: WEF, 2016)

- Means a digital ledger that is encrypted among the network members by encrypting transaction information that occurs in the public or private network

- Each time a copy of the transaction ledger is distributed to each network member and a new transaction occurs, the transaction is authenticated

Overview
(2/2)

- Because transaction information based on blockchain can not be arbitrarily changed, transaction reliability is enhanced and information tracking is easy
- Blockchain technology will be applied not only in the field of finance but also in logistics and distribution, and also in government public and administrative services.
- Theoretically, Blockchain technology can be applied to the registration, storage and trading of all kinds of assets.
  - System development using blockchain is active all over the world

Evolution

Blockchain 1.0

- Blockchain 1.0 is the ***CURRENCY***, the deployment of cryptocurrencies in apps related to cash, and financial transactions
- Blockchain 1.0 is the decentralization of money and payments

Satoshi Nakamoto

Blockchain 2.0

+ Smart Contracts

- Blockchain 2.0 is ***CONTRACTS,*** the deployment of smart properties, digital assets, and smart contracts
- Blockchain 2.0 is the decentralization of markets
- Typical platform is ***Ethereum***

Vitalic Buterin

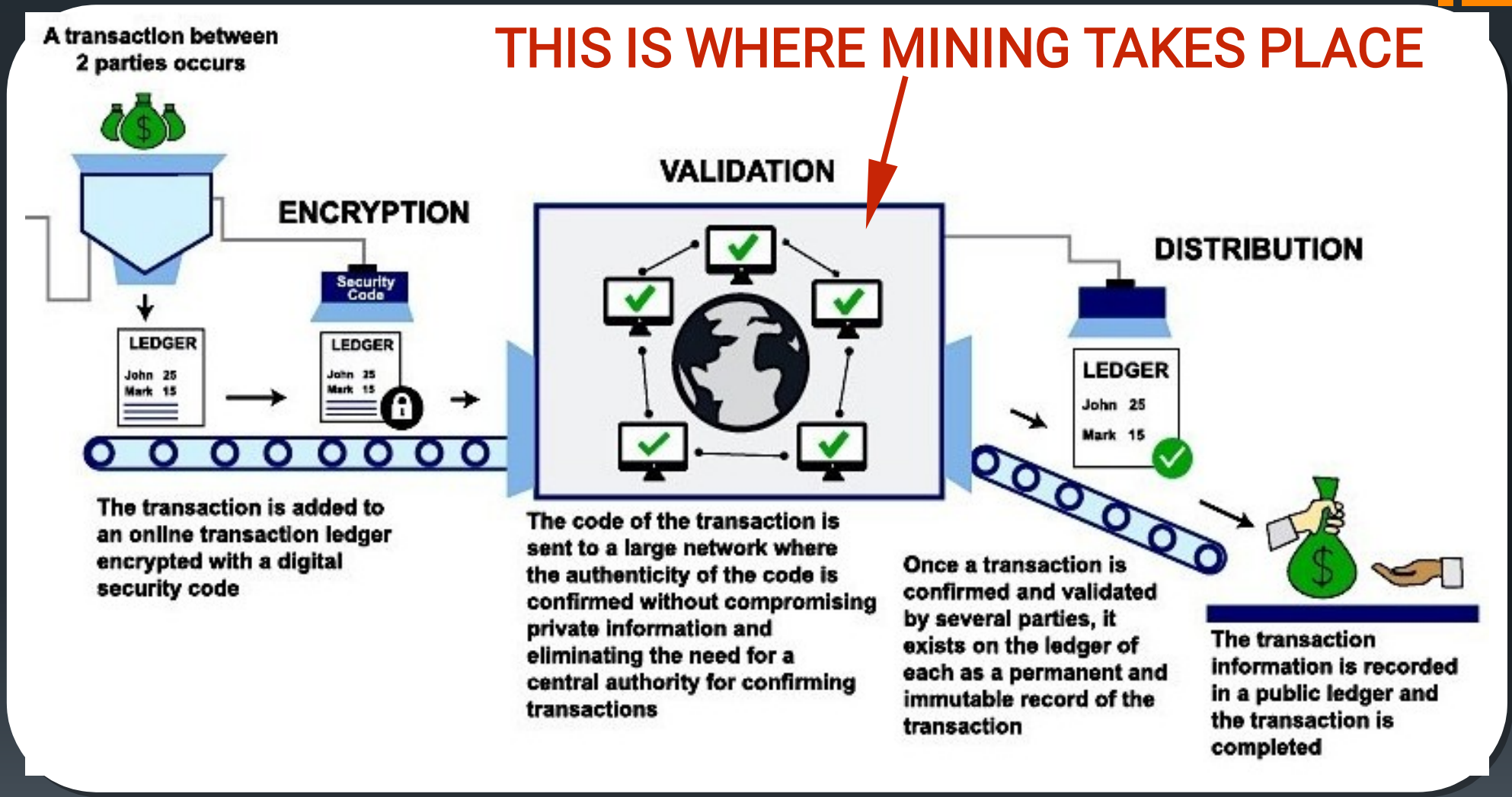
Blockchain 3.0

+ Cloud Servicing

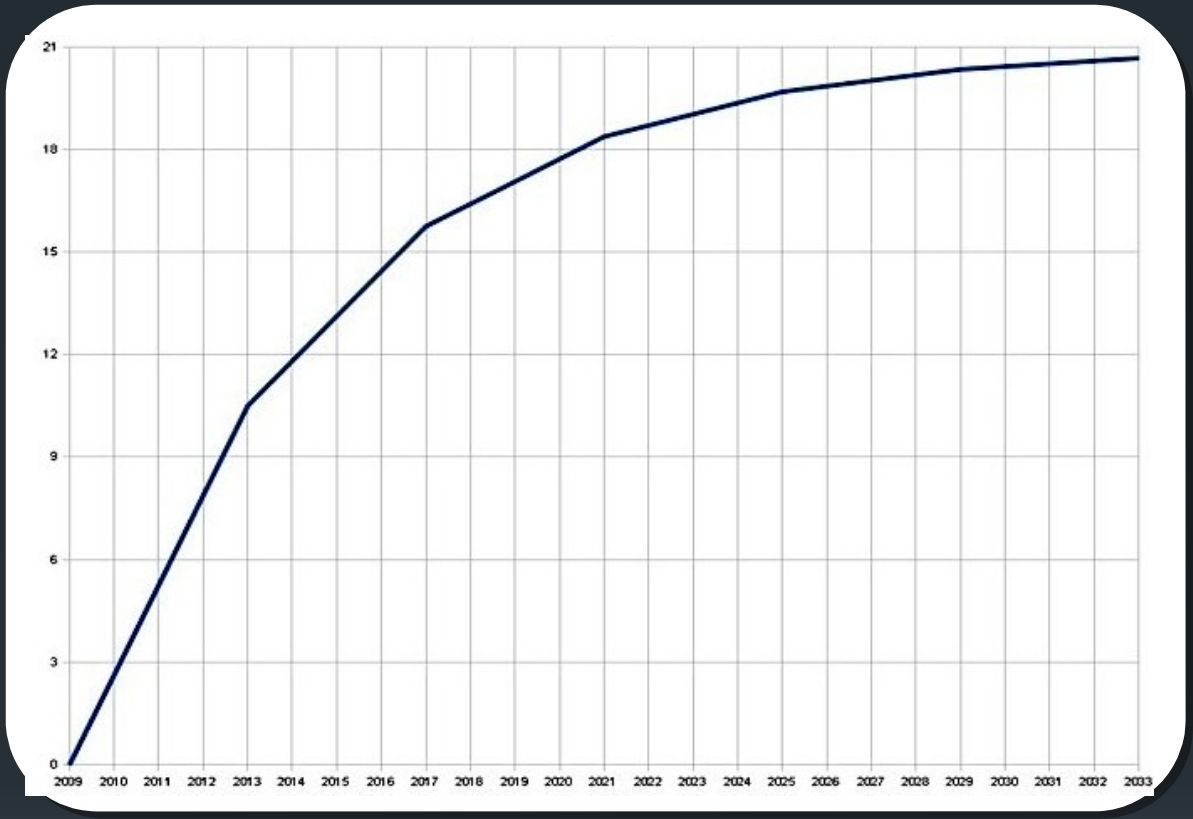
- Blockchain 3.0 is ***APPLICATIONS,*** in new areas of smart cities, IoT.M2M, government ,health, science, and art.
- Typical application is ***Solidity***

Enterprise Applications (E.g. Hyperledger)

HOW DOES BLOCKCHAIN WORK?



MINING – FUNDAMENTAL TO TRUST’



Total of bitcoin generated

Transactions are bundled into **blocks** - enormous amount of computations to prove (confirm),

only small amount of computations are required to verify as “proven”

this is **MINING**

Mining creates new bitcoins in each block - it’s created by a code, limited number (halved every 4 years), difficulty increases every 4 years.

Mining creates trust - by ensuring that transactions are confirmed only when enough computational power was devoted to the block that contains them. More blocks mean more computation, which means more trust.

HISTORY OF BLOCKCHAIN AND GROWTH

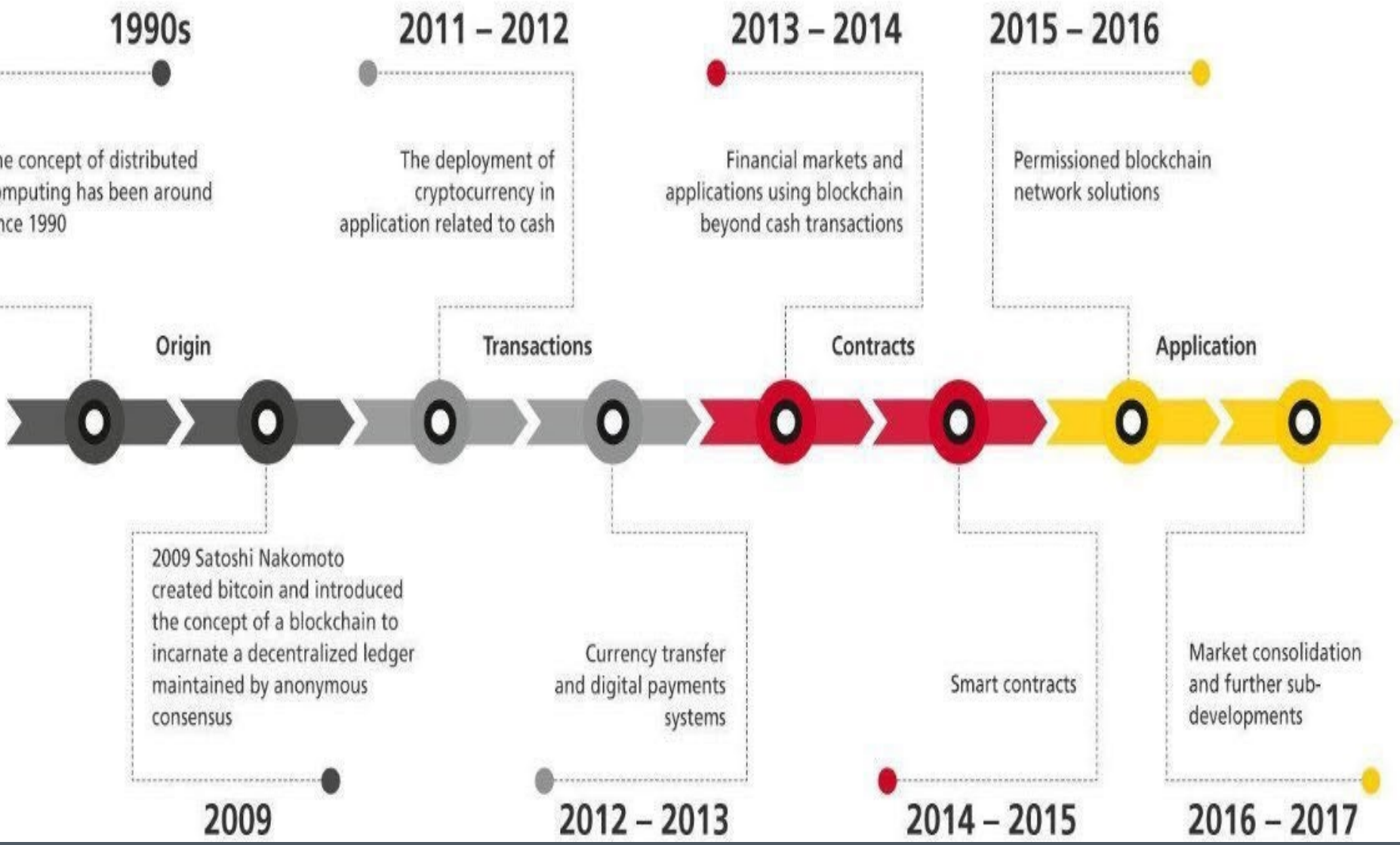
B

T I Idea was exercised much earlier:

1991-1998: first work on a cryptographically secure chain of blocks.

- **1992:** Dwork and Naor provided the first work into the usage of a cryptographic proof of computational expenditure ("proof-of-work") as a means of transmitting a value signal over the Internet.
- **mid 1990s:** CyberCash implemented SET (a standard developed by VISA and MasterCard and other tech companies) and introduced a digital cash product called CyberCoin (a micropayment system). CyberCash suffered from Y2K bug and went bankrupt in 2001; the IP was acquired by Verisign who turned it around and sold to PayPal.
- **1998:** Nick Szabo introduced bit gold as a mechanism for a decentralised digital currency and smart contracts.
- **2000:** Stefan Konst introduced a general cryptographic

BLOCKCHAIN HISTORY

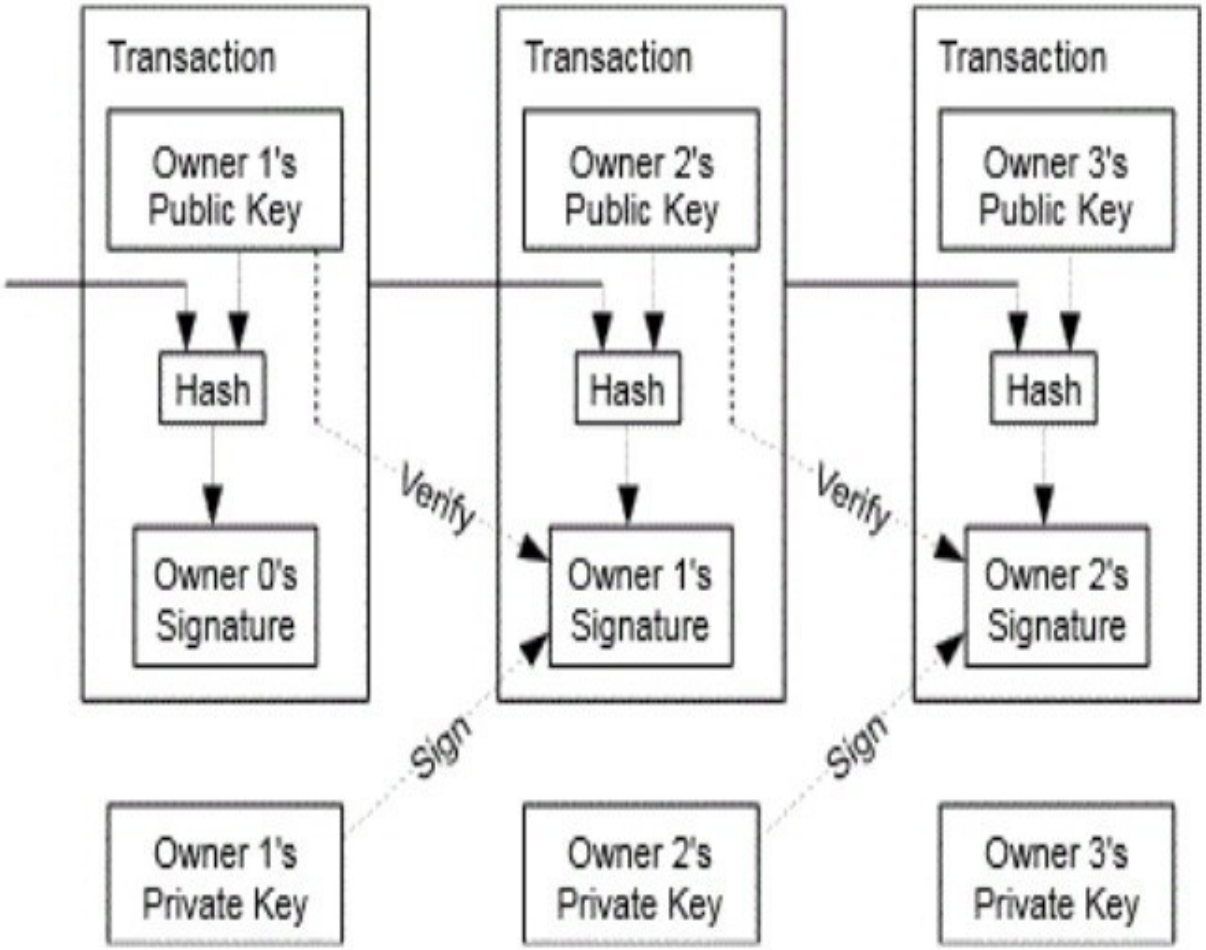


DISTINGUISHING FEATURES OF BLOCKCHAINS

(MURCK, 2017)

- **Distributed ledger** Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information.
- **Peer-to-Peer Transmission** Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.
- **Transparency with Pseudonymity** Every transaction and its associated value are visible to anyone with access to the system. Each node has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.
- **Irreversibility of Records** Once a transaction is entered the records cannot be altered, because they're linked to every transaction record that came before them (hence the term "chain"). Computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.
- **Computational Logic** The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions

Transactions – How they look?



Reference:
https://bitcoin.org/bitcoin.pdf

© TeckTalks, 2016

Simple use case on blockchain

Alice

Bob

Simple use case on blockchain - continued

Let's take an example where Bob performs a periodic maintenance service at Alice's home. Alice pays Bob at the end of the month by counting the number of visits Bob has made.

Now there are different ways of handling this account.

Option 1 : Alice maintains a record and every time Bob does a maintenance, Alice writes an entry into the record.

Option 2: Bob maintains a record and every time Bob does the maintenance, he updates the record

In Option 1 - Bob has to trust Alice about the entries and should trust Alice about maintaining it right and in a timely manner and also expects Alice not to tamper the record.

In Option 2 - The situation is reversed- Alice has to now trust Bob about the record. In both these options, if there is a dispute in the payment, it can lead to a tough and lengthy audit procedure to figure out who is right.

Simple use case on blockchain – Smart contract

Option 3 : Alice and Bob decides to keep the record with a common friend George,

Now, Bob decides to give Alice a discount of 10% in price for his services after the 10th visit in a calendar month. This is a contract between Alice and Bob. What does that mean from a system point of view?

This means, apart from keeping the count in a distributed ledger, there should be a logic which should get executed based on the trusted data.

Option 4 : The record is kept by Alice, Bob, George & also few others. All have the same record, and everybody validates the record before writing an entry on their copy of the record. All the parties who have the record has to come to an agreement that this new entry or change is valid.

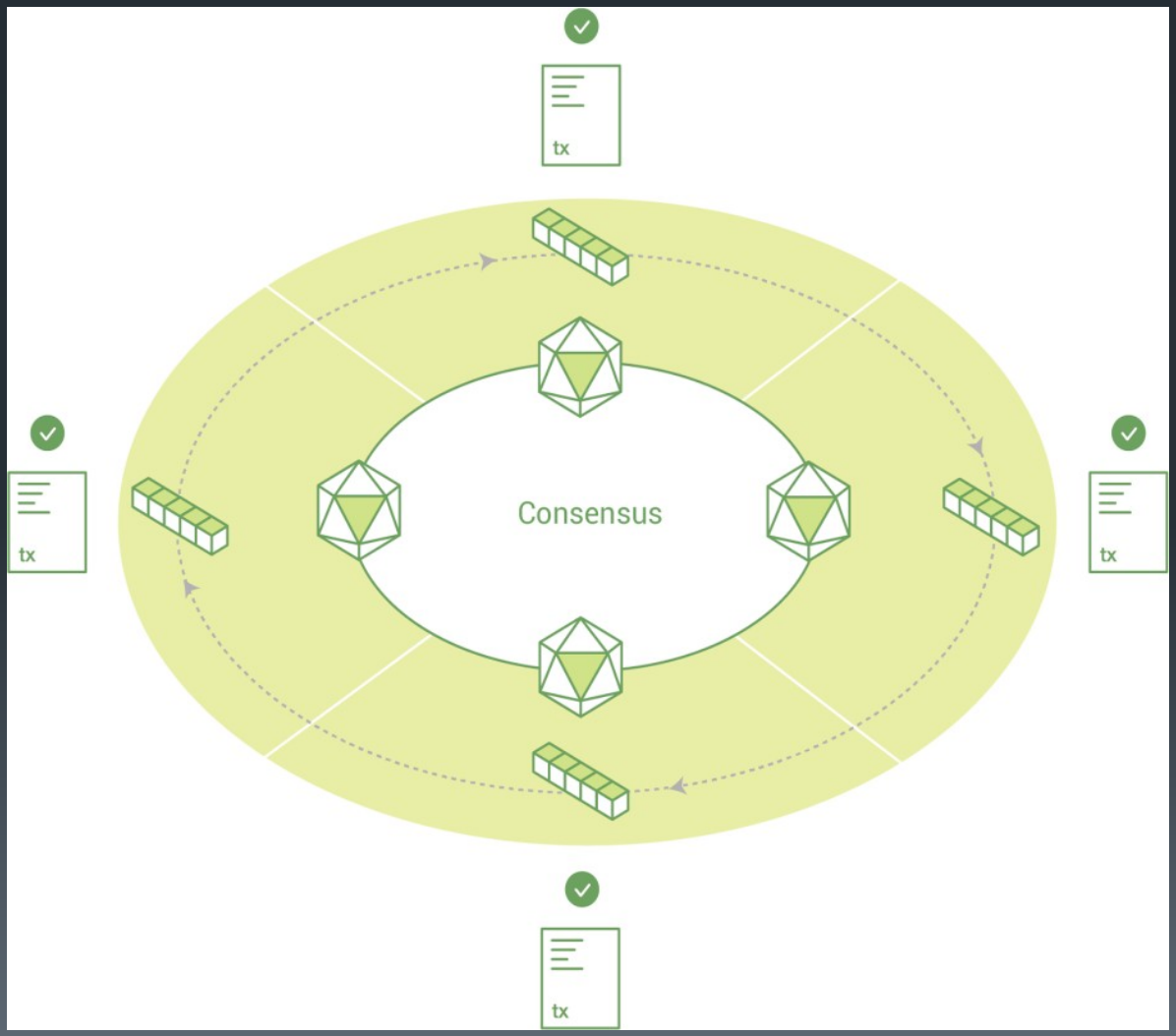
This record which all of them holds is nothing but a distributed ledger. All the parties coming to an agreement is the consensus.

The execution of the specific logic based on the number of entries is the smart contract / or chaincode.

Simple network

Consensus

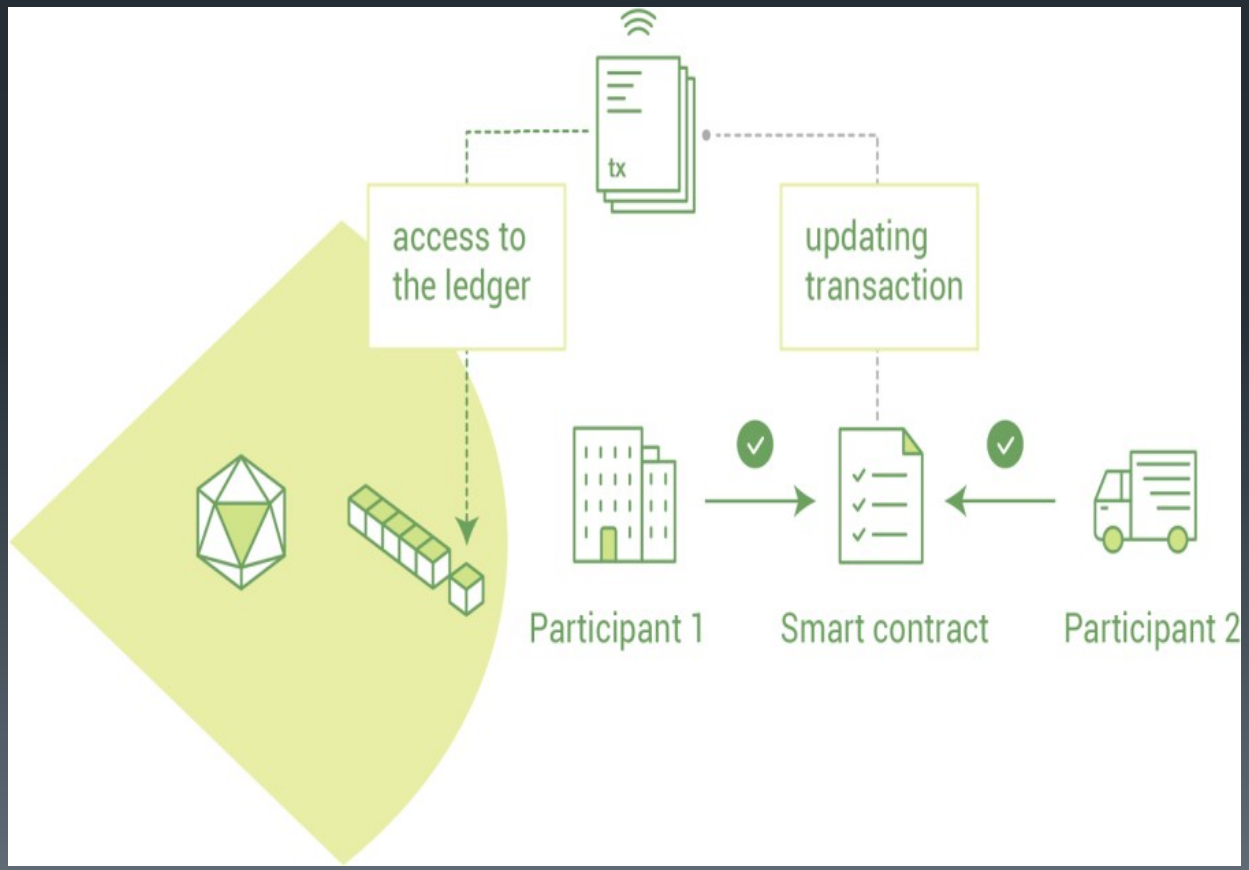
The process of keeping the ledger transactions synchronized across the network – to ensure that ledgers only update when transactions are approved by the appropriate participants, and that when ledgers do update, they update with the same transactions in the same order – is called **consensus**.



Smart Contracts / Chain code

To support the consistent update of information – and to enable a whole host of ledger functions (transacting, querying, etc) , a blockchain network uses **smart contracts / chain code** to provide controlled access to the ledger.

Smart contracts are not only a key mechanism for encapsulating information and keeping it simple across the network, they can also be written to allow participants to execute certain aspects of transactions automatically.



PUBLIC vs PRIVATE BLOCKCHAINS

Certain virtual currencies operate on **public distributed ledger systems** that capture “blocks” of transactions – there is no inherent trust in this decentralised system.

Virtual currencies create an economic incentive for dispersed, independent, computers, or groups of computers, around the world to confirm transactions and perform verifiable “work” (that creates consensus) to publish a new block of transactions on the public ledger in exchange for a payment of the applicable virtual currency.

Private / permissioned distributed ledger networks typically have some degree of trust between participants.

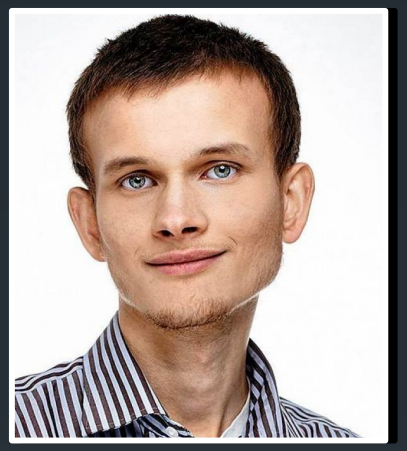
Private ledger systems allow a network of known participants to share transaction information between themselves more efficiently.

While cryptography and consensus may still be involved in private ledger systems, these systems do not necessarily involve a virtual currency that may serve as the economic incentive for miner or validator participation in public networks.

ETHEREUM, VITALIK BUTERIN AND GAVIN WOOD

Ethereum blockchain enables Smart Contracts on Blockchain – contracts that are written in a code I**f this happens, then that will happen…**

The Ethereum platform is built with a Turing-complete language that is functionally different from Bitcoin. It allows rules to be written in a way that can be expressed by code and enables smart cont



Vitalik Buterin was 19 years old when he co-founded Ethereum

Vitalik is Peter Thiel's Fellow (VC, the founder of PayPal)

Dr Gavin Wood (MSc, PhD), co-founder of Ethereum, coder of the first functional implementation of Ethereum (PoC1) and inventor of the Solidity programming language.

SMART CONTRACTS: BANKING SECTOR EXAMPLE

Capital Markets and Investment Banking

- Corporate Finance:
  - Initial Public Offers (IPOs),
  - Private equity
- Structured Finance: Syndicated loans, leveraged loans
- Stock exchange market infrastructure

Commercial and Retail Banking

- Trade Finance:
  - Supply-chain documentation, invoicing and payments
- Mortgage Lending
- Loans and crowdfunding for startups and small and medium enterprises

Insurance

- Automated claims processing in motor insurance, crop insurance, etc.
- Fraud prevention in luxury goods
- New products: insurance for the sharing economy, autonomous vehicles, peer-to-peer insurance, cyber insurance

Regulatory reporting and compliance;
Know Your Customer (KYC) and Anti-Money Laundering (AML)

Source: https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf

W.E.F. ON INDUSTRIES AFFECTED BY BLOCKCHAIN

- "According to the World Economic Forum (WEF), the blockchain ecosystem will store 10% of the world's GDP ($101 trillion) by 2025. If the WEF is correct, this means the total market capitalisation will be $10.1 trillion by 2025.

- The predictable areas blockchain technology is set to transform cover financial services, insurance, cybersecurity, elections, energy, logistics, identity, legal, governance, and healthcare, for example.

- If the estimates by the WEF turn out to be accurate, the expected growth for the blockchain ecosystem should be approximately 13,333% within the next eight years. Anything above this percentage construes a bubble, hence we still have a long way to go."

Source: https://www.inc.com/brian-d-evans/is-ethereum-in-a-bubble-heres-what-you-need-to-know.html

BLOCKCHAIN PROJECTS IN 2017

How many projects are in the network?

86,034
projects

9,375+ projects
by companies, research institutions, and start-ups

Finding: Projects of organizations are five times more likely to be *forked* (copied).

How fast is it growing?

Averaging
8,603
per year but with
26,885 in 2016

Finding: Projects developed by organizations register fastest adoption rate: 20% compound annual growth rate.

Project survival?

Only 8% of projects are actively maintained

Only 5% of forked projects survive

Projects have average life span of
1.22 years

Finding: There are very few projects with high longevity.

Source: Deloitte analysis of GH Torrent data and GitHub API data, as of October 12, 2017.

BANKS EXPLORING BLOCKCHAIN

WHAT IS A CRYPTOCURRENCY?

A math-based, decentralised convertible virtual currency that is protected by cryptography—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy (CMPI/Merrill Lynch, 2017)

- **Decentralised** - no central issuing authority, as there is with, say, the US Dollar.
- **Convertible** - can be converted into real world (fiat) money.
- **Virtual currency** - a digital representation of value which is not issued nor guaranteed by any jurisdiction, fulfils the above functions only by agreement within the community of users of the virtual currency.
- **Protected by cryptography** - the blockchain, hashing and mining are the means by which bitcoin is protected, but other coins use different methods.
- **Distributed** - there is no one canonical database, there are instead a number of "nodes" with full copies of the data.
- **Trustless** - not only are there more than one instances of the database, the decision as to which version is "right" is for the overall community not one trusted entity.
- **Secure** - a result of the cryptographic work.

Gist of Blockchain

- Blockchain is a shared, distributed, replicated data and transaction system which is updated via smart contracts / chain codes and kept consistently synchronized through a collaborative process called consensus.

  Distributed ledger / data across the network : Every participant has the same view of the data The data cannot be corrupted as it's not possible to corrupt the data store of all the parties Uses advanced cryptography to ensure security

  No central point of control and no central point of failure

Why blockchain ?

Faster processing times for transactions which needs high level of trust
Lower cost of operations - due to ease of audits and evolution of common applications High level of Security - due to cryptography

The elimination of central points of attack and failure.

Types of Blockchain

Permissioned and public block chains

Permissioned block chains

- Permissioned blockchain is a blockchain network where only authenticated users can participate in writing to the blockchain or perform transactions
- Permissioned gives more importance on efficiency and immutability over anonymity and transparency. It's a network operated by known entities or stakeholders in a value chain, with agreed set of rules and guidelines to inter-operate.

Public block chains

- Un-permissioned blockchain is a public blockchain where anyone can participate in a transaction
- Public blockchain gives highest importance in anonymity, immutability and transparency over efficiency. An example public block chain is Bitcoin.

This leads to why a permissioned blockchain is ideal for enterprises over a public blockchain.

Types of Blockchain

Similarities of Permissioned and public block chains

- Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions.

Differences between common blockchains

	Bitcoin	Ripple	Ethereum	Hyperledger Fabric
Purpose	Transfer of value (Bitcoin currency)	Payment processing	General purpose for many applications	General purpose for many applications
Governance	Bitcoin	Ripple Labs	Ethereum foundation	Linux foundation
Consensus	Mining - PoW	Ripple proprietary protocol	Proof of stake(PoS)	BFT Consensus (Byzantine fault tolerence)
Network	Public	Consortium	Public	Permissioned
Mining	Yes	None	Yes	None
Smart contract capability	Not relevant	None	'Solidity' programming language	Programming languages like Java, GO.

Need of an enterprise grade blockchain

- Data Privacy and confidentiality:
  - *Enterprises have confidential data which cannot be shared with the entire world even though it needs to be shared with multiple entities. Enterprises have specific agreements with certain partner organizations which needs sharing of information but not necessarily to everyone like public blockchains.*
- Efficiency and speed of transactions:
  - *Enterprises have high volume transactions, but cannot afford delays for a transaction to commit due to business reasons.*
- Modular design approach:
  - *One size fits all is not pragmatic when it comes to enterprise ready solutions. Enterprises have existing frameworks which needs to be leveraged. A typical example is the reuse of LDAP or any identity management capability an enterprise already have.*
- Hybrid approach:
  - *As an enterprise, there are key processes in the value chain which can greatly benefit from Distributed Ledger Application and needs to integrate and coexist with the other process within the enterprise.*
- B2B focus:
  - *In large enterprises, one of the key technology challenges relates to B2B scenarios or working with partners. This is mainly due to the difference in technology each of these parties in the ecosystem which makes data sharing and integrations painful and expensive.*
- Mining and legal restrictions on location of nodes:
  - *Enterprises often have legal regulations or policies on where the data can reside. There are specific regulations in North America for certain industries and similar regulations exists in European Union. Publically mined blockchain is not an option due to these considerations.*
- Alignment with the vision of going digital:

  Digital transformation is on the way. Blockchain adoption needs to be complementary to digital transformation investments in an enterprise.

Above concerns are critical in any selection process for an enterprise grade solution. Such an evaluation is the key for discerning one technology over another.
HyperLedger answers all these concerns for enterprise and promises to be a solution for many of its use cases.

Key use cases - Financial services & Government

- Payments – Asset transfer
- KYC
- Clearing and settlement
- Digital Identity management
- Trading platforms
- Trade finance
- Regulatory Compliance and Audit
- Insurance
- Peer to peer lending
- Taxation (Government)
- Record keeping

Key use cases - Retail and Consumer goods

Preventing fraud in a supply chain

Tracking and visibility across the chain Same source of truth for all

Easy audits and dispute management

Potential integration with regulatory bodies for cross border movements

Provenance for high value goods

Managing claims, returns, warranty services (probably for high value goods)

Potential integration with smart devices and sensors in the supply chain (IoT & blockchain) - transportation vehicles, temperature monitoring etc.

Preventing identity fraud

Loyalty management

Key use cases - Pharma & Healthcare

Patient master record management
Smart prescriptions and pharmacy

Drug supply chain and provenance

Health care and insurance - Claims adjudication and billing management

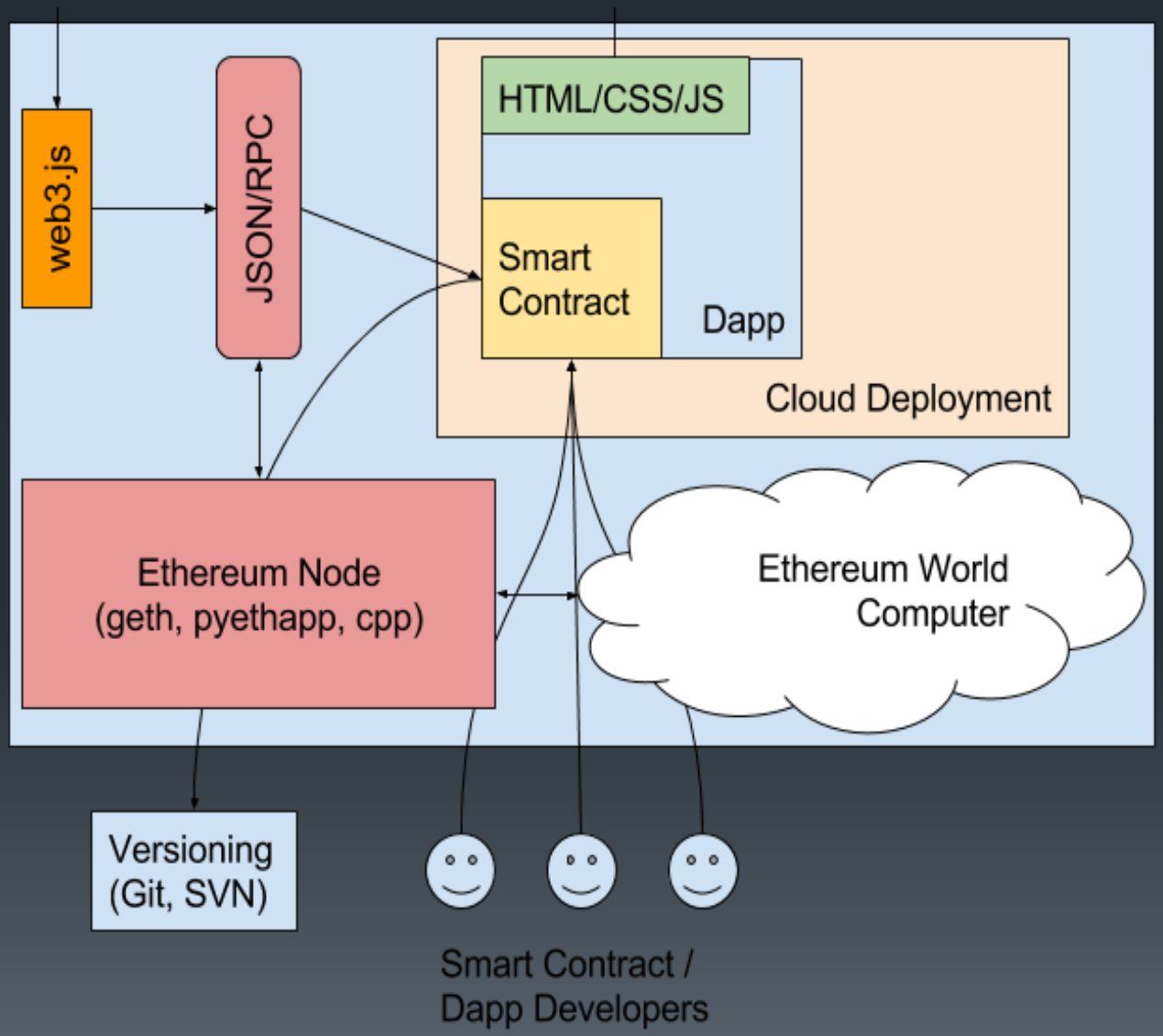
Main value drivers

- Ease of multi party environment where management and collaboration is the key
- Time to process and processing cost reduction by operational simplicity
- Risk, compliance and fraud reduction
- Regulatory and efficiency improvement
- Settlement time reduction and accuracy
- Authenticity and provenance

Benefits include :

- Saves time - Transaction time from days to near instantaneous
- Removes cost - Overheads and intermediary costs
- Reduces risk & Improves compliance - Tampering, fraud, smart compliance
- Increases trust - Through shared processes and recordkeeping

Ethereum Development



Aspect: Solidity Env.

Aspect: JavaScript Env.

Aspect: IDE

Aspect: Versioning

Aspect: Collaboration

Aspect: Deployment

Ethereum Development:

- Ethereum is a platform that is intended to allow people to easily write decentralized applications (Đapps) using blockchain technology.

- Ethereum blockchain can be alternately described as a blockchain with a built-in programming language. protocol that actually handles internal state and computation is referred to as the Ethereum Virtual Machine (EVM).

There are two types of accounts:

- Externally owned account (EOAs): an account controlled by a private key, and if you own the private key associated with the EOA you have the ability to send ether and messages from it.

- Contract: an account that has its own code, and is controlled by code.