Blockchain based trust management for IOT/5G devices

Prof Rasool Asal
Chief Researcher
EBTIC (BT Research Centre, UAE)
British Telecommunications, UK

Agenda:

- Introduction to IoT
- Security Challenges and Data Breaches
- Basic Countermeasures
- The Role of the Ledger – Blockchain
- Blockchain-Based Data Clearing House

What Is the Internet of Things?

The *Internet of things* (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data (Wikipedia)

THE MARKET IS EXPECTED TO BE ASTRONOMICAL

2015:

10 billion connected things
$1.9 billion from IoT services

2020:

ABI: 250,000 connected cars
IDC: $7 billion from IoT services
Gartner: $300 billion from IoT products
IDC: Global IoT market $7.1 trillion
ABI: 40 billion IoT devices

2035

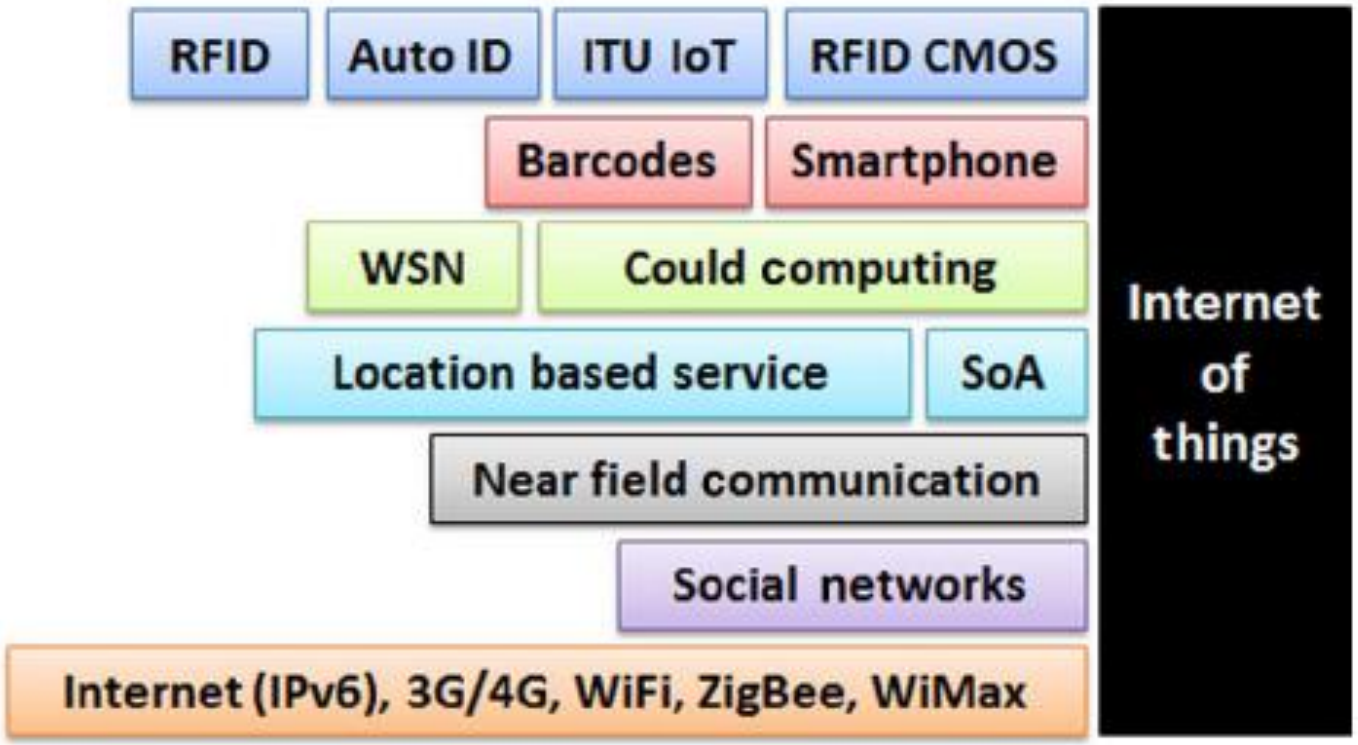
GE: $10-15 trillion added to GDP
Cisco: $19 trillion
ABI: 450 million IoT-cars

Source: http://www.eetimes.com/auth or.asp?doc_id=1326597

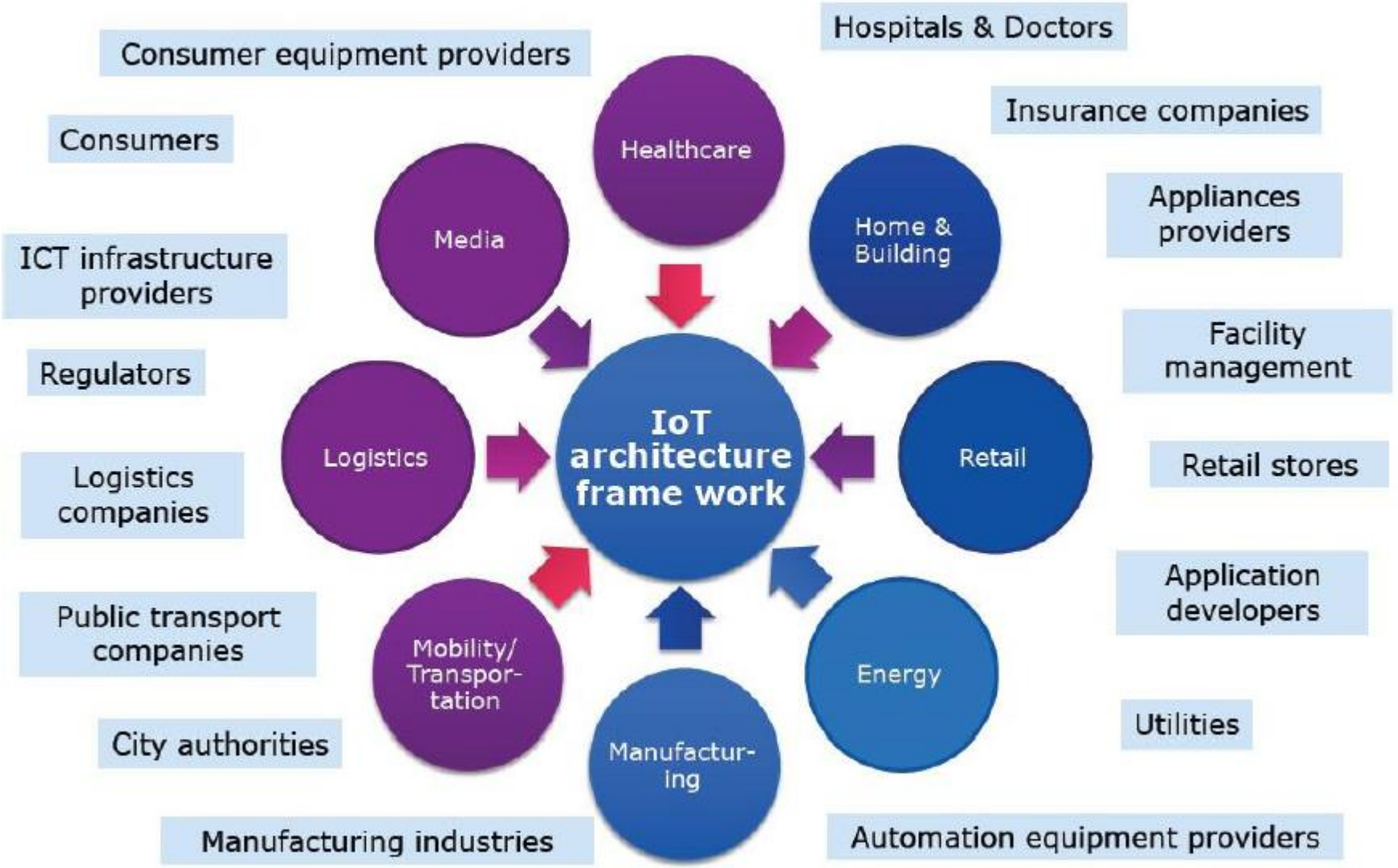
Why Now

- Low-priced microcontrollers, sensors and networking
- Consumers have something to read/control them – smart phones, tablets etc
- IP addresses now effectively infinite – IPv6
- Internet access more widespread. 900MHz 80211ah WiFi for reliable M2M
- Big investors and hungry wealthy suppliers e.g Cisco, Google, Samsung
- Many countries have significantly invested on IoT Initiatives

Technologies associated with IoT



IoT markets and stakeholders



IoT Security Challenges

Unique security challenges in the IoT landscape

- Constrained in memory and computer resources, IoT devices can’t always support complex and evolving security algorithms
- IoT products don’t include long-term support or automatic firmware updates despite being created with longevity in mind
- Most devices are, to the end user, like black boxes-few people know how everything works

IoT Security issues

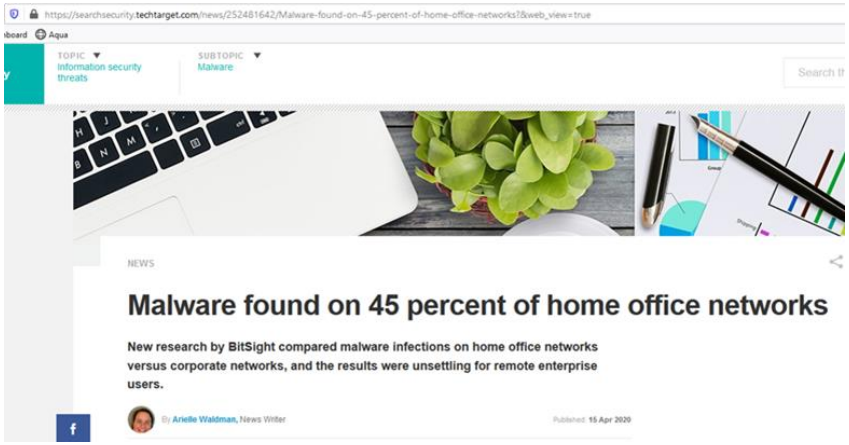
- Objects are not reachable
- Objects can be lost and stolen
- Objects are not crypto-engines
- Objects have finite life
- Objects are transportable
- Objects content need to be recognised by many readers

IoT Cyberattacks escalate in 2021

- IoT cyberattacks more than doubled year-on-year during the first half of 2021, according to anti-virus and computer security service provider Kaspersky

- From January to June this year, some **1.51 billion** breaches of Internet of Things (IoT) devices took place, an increase from 639 million in 2020

- Most attackers (around 60%) brokered access to IoT networks via the telnet protocol, a command line interface that enables remote communication with a device or server



Hacker's Motivation

- From a hobby to a profitable industry
- From annoying to destructive
- From playing to stealing
- From simplicity to complexity

Why it is not difficult to breach IoT Networks?

- Billions of connected devices
- Secure and insecure locations
- Security may or may not be built in
- Not owned or controlled by IT … but data flows through the network
- Any node on your network can potentially provide access to the core

Attacking IoT

- Default, weak, and hardcoded credentials
- Difficult to update firmware and OS
- Lack of vendor support for repairing vulnerabilities
- Vulnerable web interfaces (SQL injection, XSS)
- Coding errors (buffer overflow)
- Clear text protocols and unnecessary open ports
- DoS / DDoS
- Physical theft and tampering

Examples of IoT Cyber Attacks

- Mirai Botnet DDoS Attacks

Major cyber attack disrupts internet service across Europe and US

Denial of service attack from unknown culprits on domain name system company Dyn caused access to be severely restricted for users on Friday

Platforms affected by the attack included Twitter, Netflix, Reddit and Spotify. Photograph: Ross M. Horowitz/Getty Images

The breach of the popular kids' gadgets company Vtech

IoT Security Solutions

How can anyone secure the IoT?

Extrinsic Security

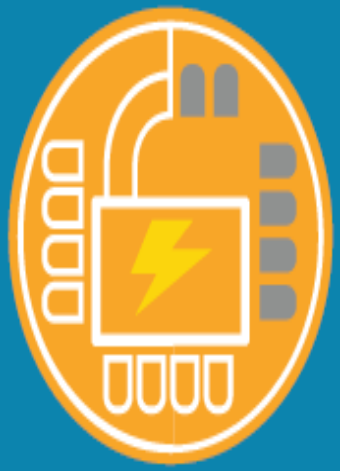
Add-on Security

PC/Datacenter Era

- Bolt-On Security
- Layers of Security added to PCs, Servers, Networks and Devices

Intrinsic Security

Security-by-Design



Internet of Things Era

- Built-In Security
- Security built into the device at manufacturing time

Source Symantec

How to Protect Connected Home Devices and Appliances from Cyber Attacks

Adding a few basic security capabilities can make IoT devices dramatically more secure, and greatly reduce the risk of falling victim to a cyber-attack including:

- Secure boot
- Secure remote firmware update
- Secure communication
- Data protection
- User authentication

Research Questions

Security	Can we protect devices and sensors from unwelcome access?
Integration	Can we combine data and devices across networks and platforms?
Data Ownership	Can we assign accountability for data stewardship and permission for data monetization?
Appropriate Data Use	Can we control how data will legally and ethically be captured, managed, and used?

Research Areas

- Energy inefficient/unsecure protocols
- Network location of smart objects

INTRODUCTION TO BLOCKCHAIN

BLOCKCHAIN HAS MANY MEANINGS

"To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general."

The TrustMachine, THE ECONOMIST, Oct. 31, 2015

What is BLOCKCHAIN?

A technology that:

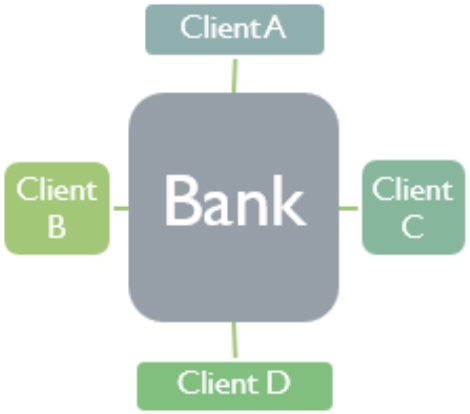
permits transactions to be gathered into blocks and recorded;

cryptographically chains blocks in chronological order; and

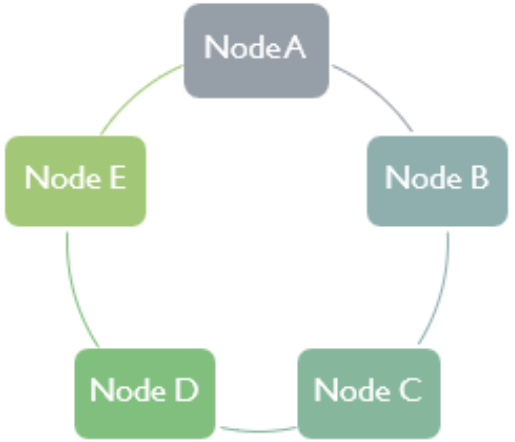
allows the resulting ledger to be accessed by different servers.

WHAT IS A DISTRIBUTED LEDGER?

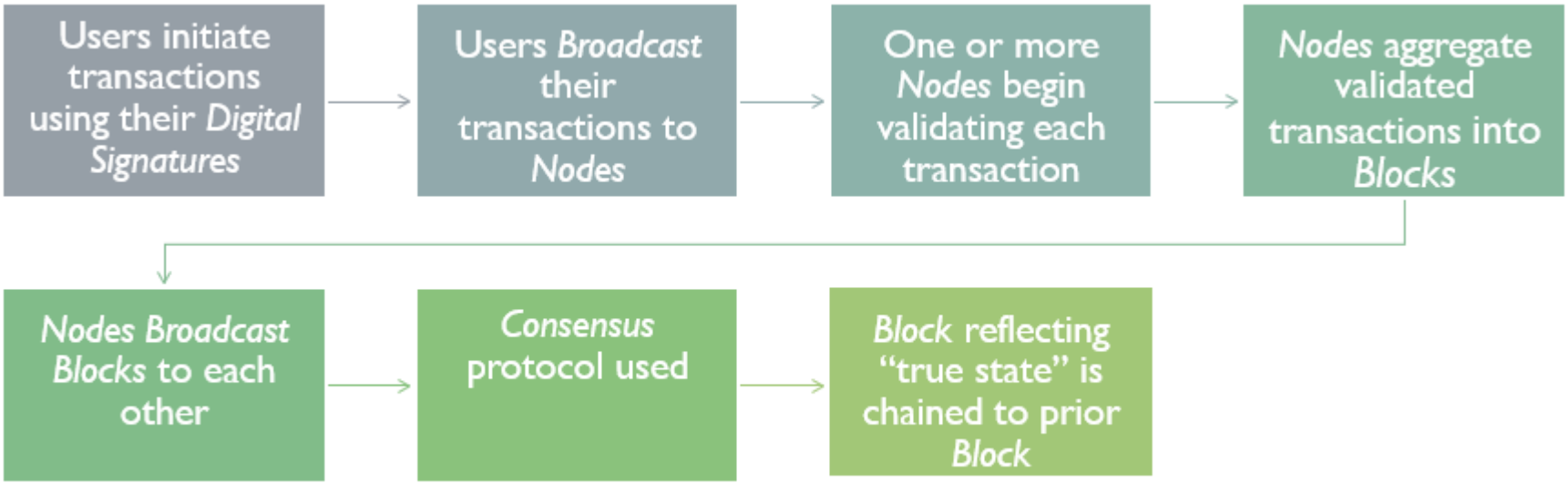
Centralized Ledger



Distributed Ledger

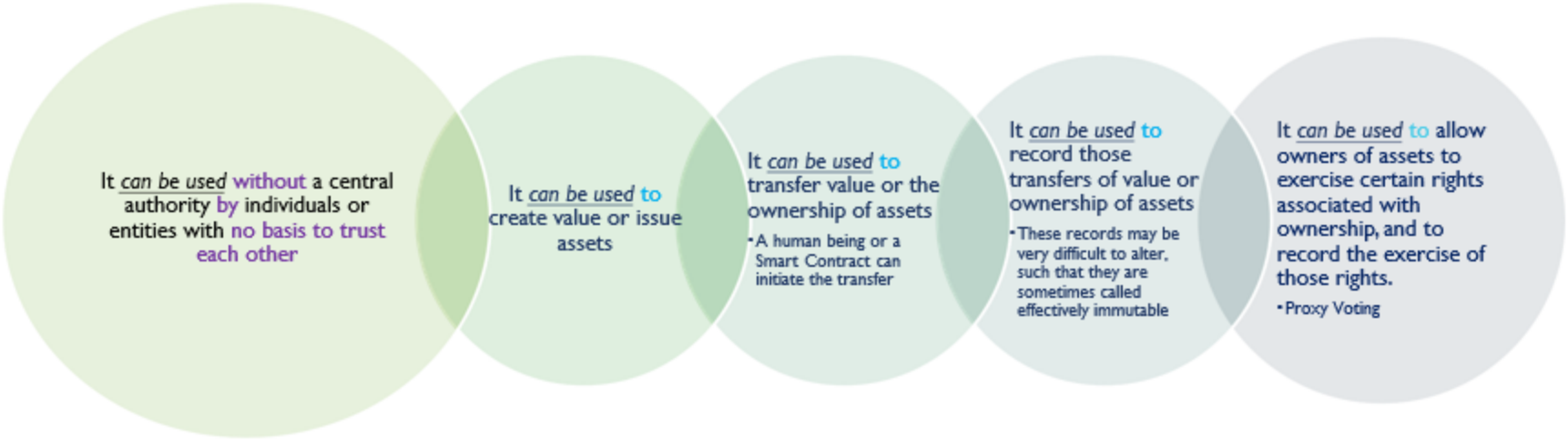


HOW A DISTRIBUTED LEDGER WORK?



Source: "A brief introduction to blockchain", Nancy LIAO, 2005

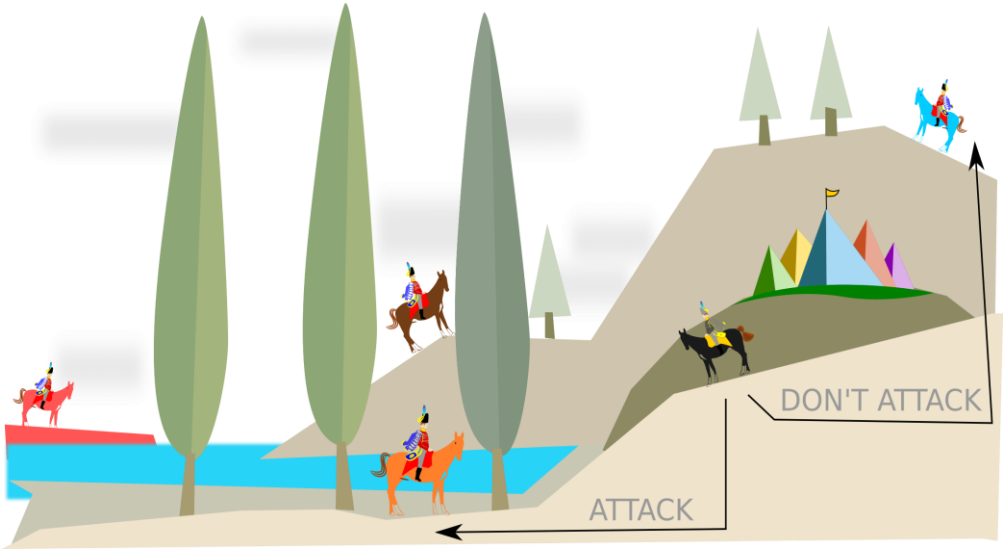
THE POWER OF DISTRIBUTED LEDGERS



Source: "A brief introduction to blockchain", Nancy LIAO, 2005

Byzantine Agreement

The challenge of reaching an agreement between multiple nodes of a network that have limited trust in one another is well described by the"Byzantine Generals Problem", proposed by computer research already in the 1980s.



Consensus

The technique for reaching distributed consensus called Proof-of-Work (PoW) is based on the generation of messages that cannot be changed without investing computational effort, because they integrate solutions to complex mathematical problems

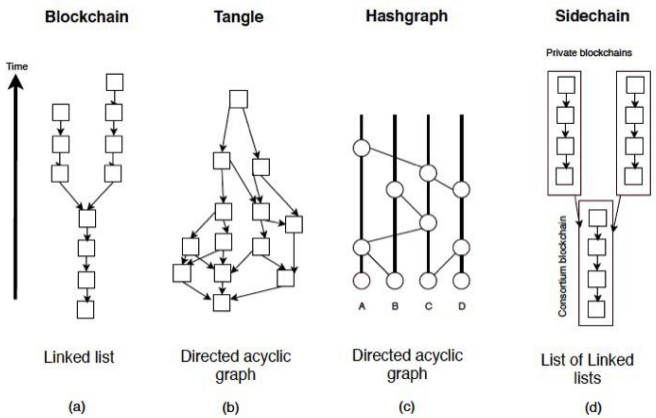
Consensus

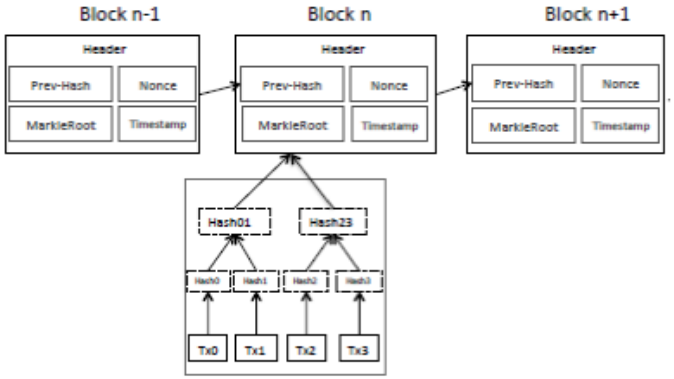
Over the years, various alternative consensus mechanisms have been proposed to improve the efficiency of distributed consent protocols.

- Byzantine Failure Tolerance - BFT

- Paxos is a deterministic algorithm to reach the consensus that works in asynchronous systems and tolerates f <n / 2 block-type failures, where f is the number of participating nodes that can go in block.

Data Structure





DLT Components

- Transaction Records
- Blocks
- Ledger or Distributed Ledger (DL)
- Mechanism for consistency checking
- Mechanism for edit control
- Intelligent contracts
- Libraries
- Mechanism for distributed consent

Consensus Algorithms

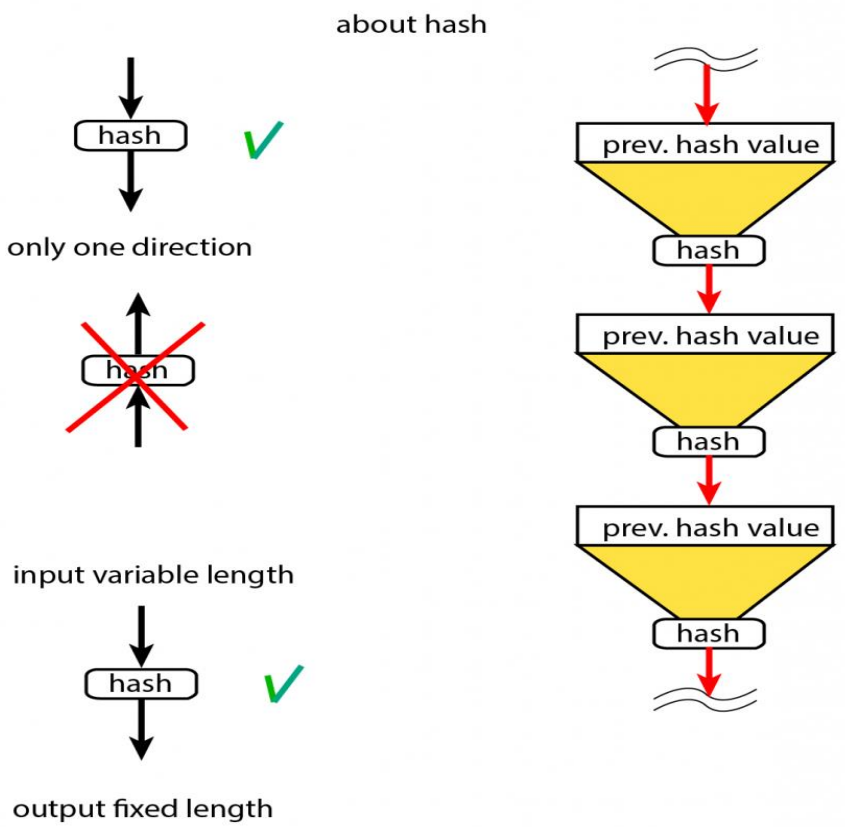
This property identifies the consent protocols used by the DLT

- Proof-of-Work
- Proof-of-Stake
- Proof of Space (PoSp)

Consensus Issues

- Fork
- Lack of consensus
- Predominance of a single node
- Fraud
- Poor performance

Focus on hash-chaining



Focus on consistency

Merkle trees are often used to ensure consistency, while limiting the amount of data exchanged across the network

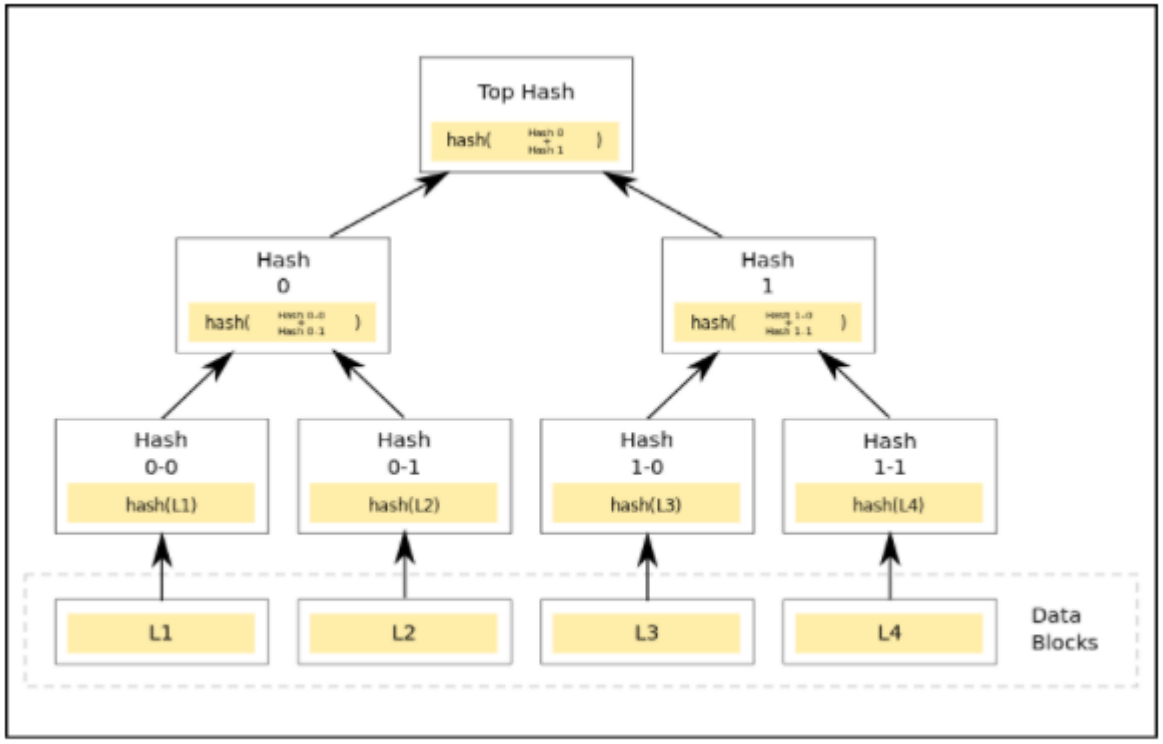


Image Courtesy: Wikipedia

Focus on Tokenization

Tokenization: format of data representation as a token in the DL.

There are several standards that define token:

- **ERC 1329: Inalienable reputation token:** 1329 Reputation tokens are issued and burned by a contract depending on the actions of the holders of the balances and their consequences (e.g. There is evidence of the Byzantine behaviour of the owner).

This format was recently developed to manage reputation. If reputation can be transferred, it can be sold, breaking economic incentives, creating different Nash equilibria and generally protecting worse from evil actors (less Byzantine tolerance)

- **ERC 20** This specification can improve the interchangeability of ERC20-based tokens and perform the same operation on Dapp. ERC20 avoids the problems of users of the Ethereum community by creating unique Tokens and functions, solving the problem of destroying smart contracts and hacking attacks when tokens move

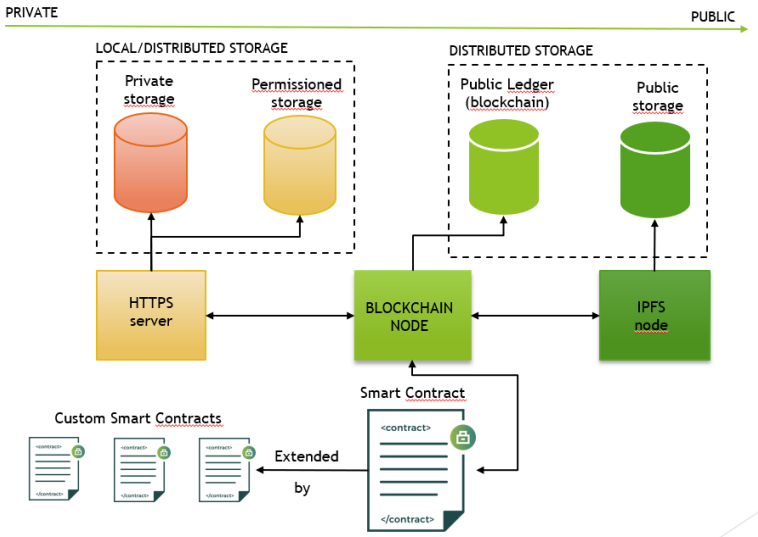
- **ERC 721** is a specific alternative to ERC20 which defines non-interchangeable tokens. Each token has an independent ID that can be used in the asset and tracking transaction.

Non Functional Features

- Decentralization
- Distribution
- Immutability
- Verifiability
- Confidentiality
- Pseudo-anonymity
- Fault tolerance
- Critical mass
- Scalability and Interoperability

Types of Distributed Ledgers

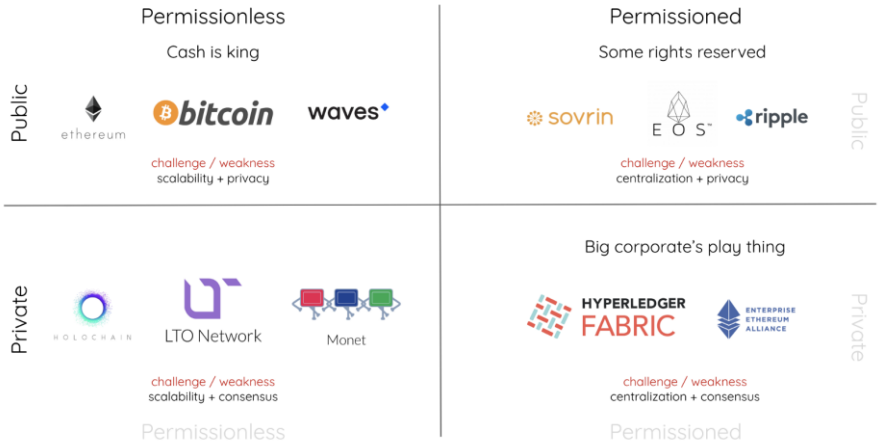
- Public
- Private
- Mixed (Public / Private)



Authorization

This property None functional goals is related to the read / write rights of the participants

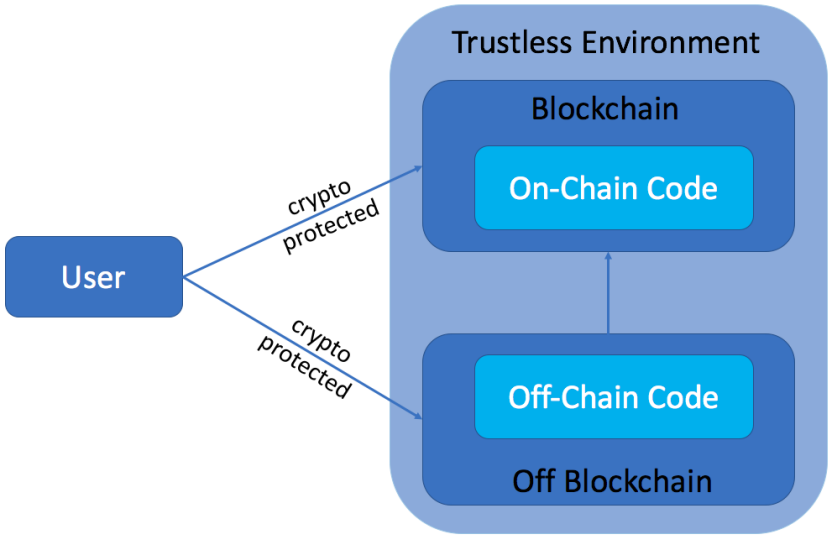
- Without permits
- With permits



Location of business logics

This property refers to the methods execution of the automatisms

- On-chain
- Off-chain



Distribution

This property identifies the actual data distribution adopted for the DL

- Complete node
- Full miner + slim actor

Incentives

This property concerns the presence of a payment mechanism for interacting (making transactions) with the DL

- No commission:
- With commission (variable, fixed)

Sustainability

The decentralized components of the DL require a higher computing power per update operation and are therefore more expensive in terms of energy. The PoW consensus mechanisms are admittedly energy-intensive.

Any Questions ?

Thank you!