Evolution of Blockchain Technology and Applications

Akter Ul Alam

CSO, F@H Ltd

Contents

I. Evolution of Blockchain Technology

II. Blockchain for Everything?

III. Applications

CONTENTS

I. Evolution of Blockchain Technology

II. Blockchain for Everything?

III. Applications

Technology Overview : Bitcoin vs Blockchain

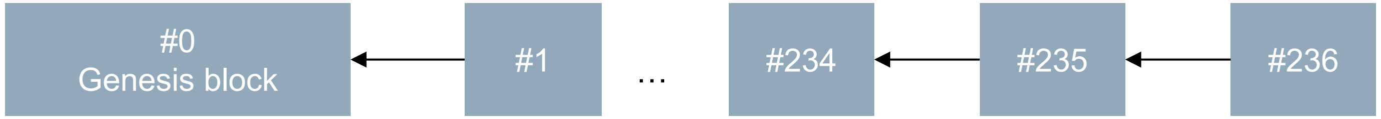
Blockchain is a digitized, distributed and secure ledger that guarantees immutable transactions and solves the trust problem when two parties exchange value.

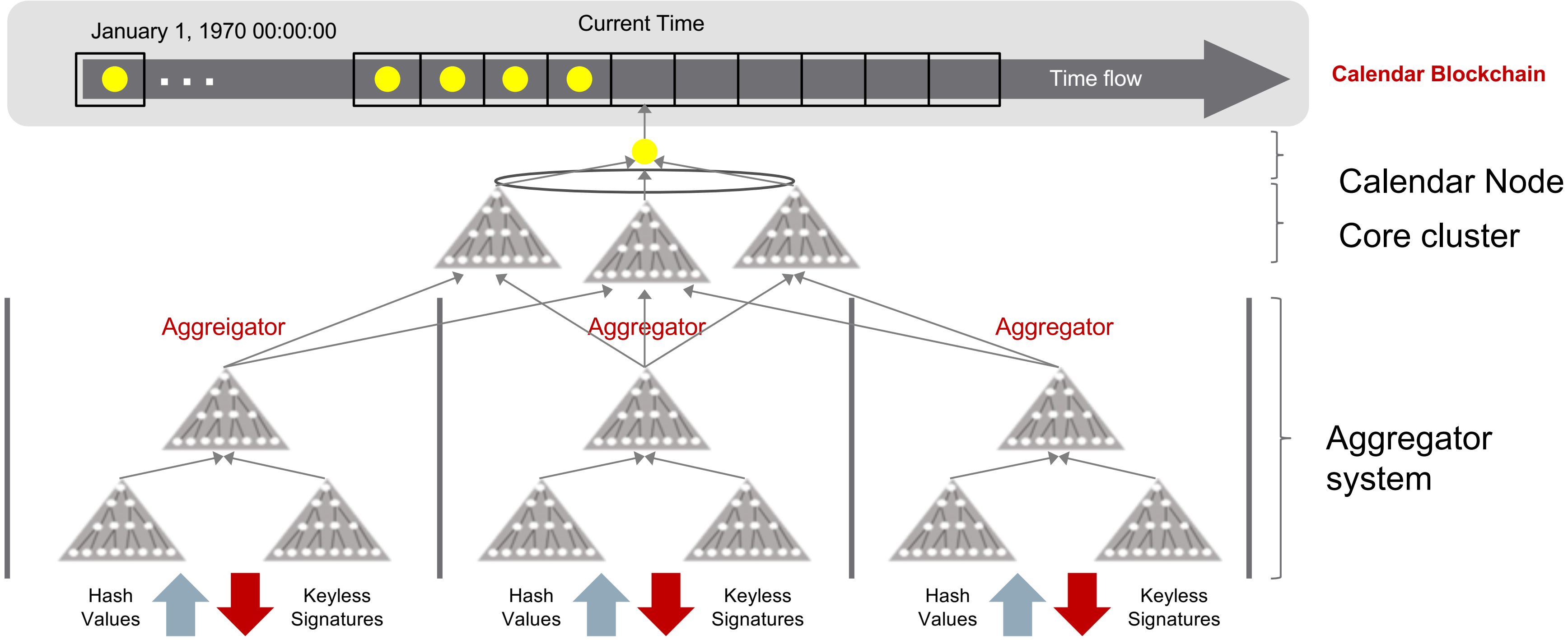
Cryptocurrencies like Bitcoin rely on blockchain to conduct transactions.

Yet blockchain transcends cryptocurrencies and offers many solutions that are likely to disrupt numerous industries with some profound implications.

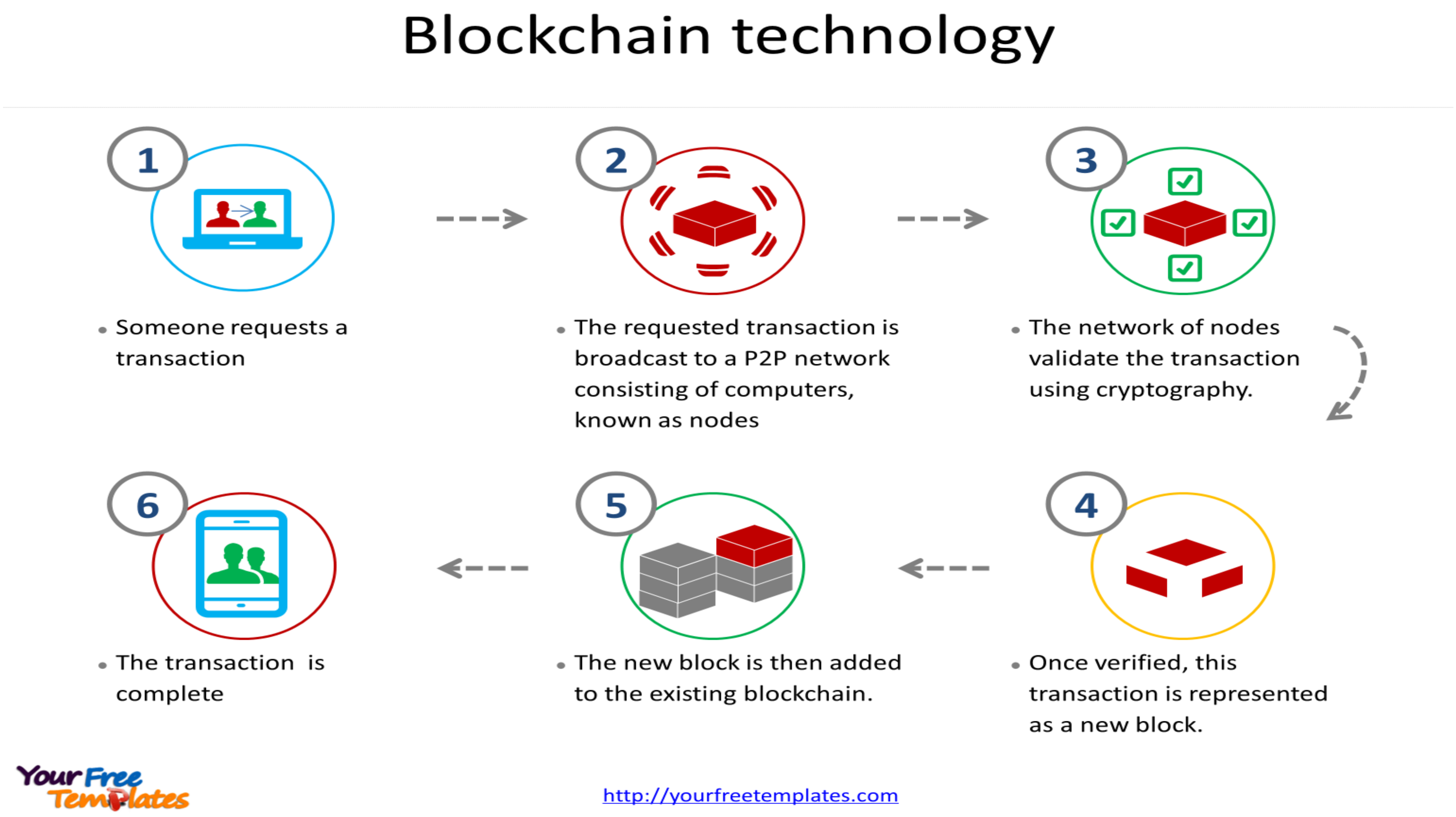
Technology Overview

- **A Chain(Sequence) of Transactions Block)**
  - Horizontal Structure(bitcoin, Hyperledger)
  - Vertical Structure (KSI)





How a Blockchain works?



Blockchain technology

1
- Someone requests a transaction

2
- The requested transaction is broadcast to a P2P network consisting of computers, known as nodes

3
- The network of nodes validate the transaction using cryptography.

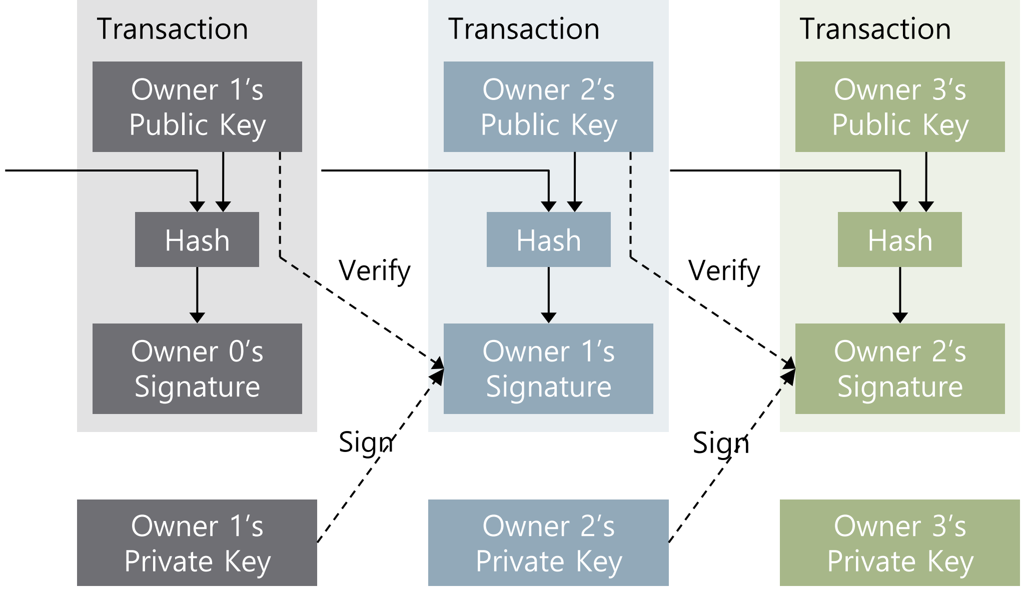
4
- Once verified, this transaction is represented as a new block.

5
- The new block is then added to the existing blockchain.

6
- The transaction is complete

http://yourfreetemplates.com

1st Generation Blockchain:BitCoin Model



Transaction

Owner 1's Public Key

Hash

Owner 0's Signature

Owner 1's Private Key

Verify

Sign

Transaction

Owner 2's Public Key

Hash

Owner 1's Signature

Owner 2's Private Key

Verify

Sign

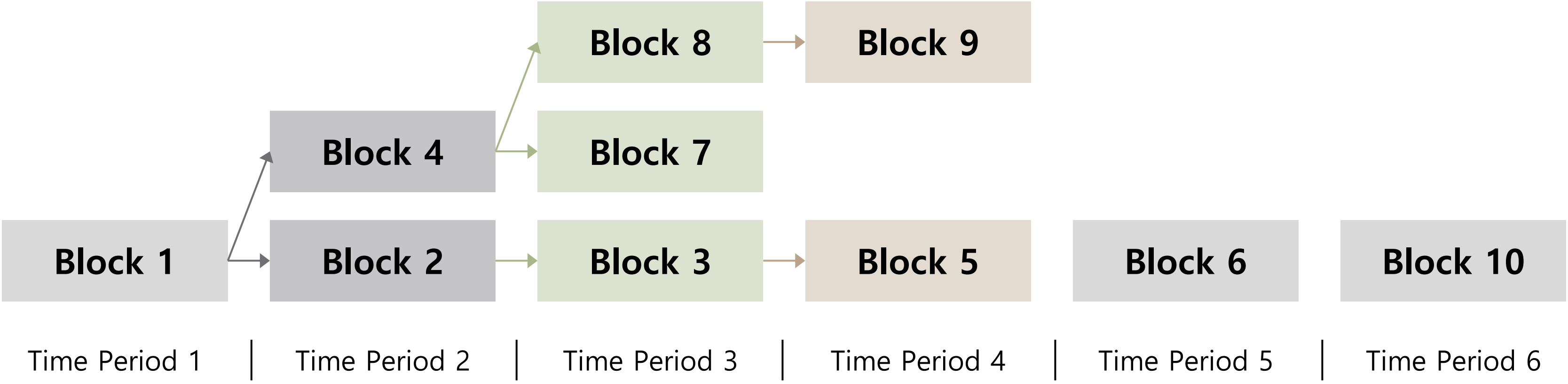
Transaction

Owner 3's Public Key

Hash

Owner 2's Signature

Owner 3's Private Key



Block 8

Block 9

Block 4

Block 7

Block 1

Block 2

Block 3

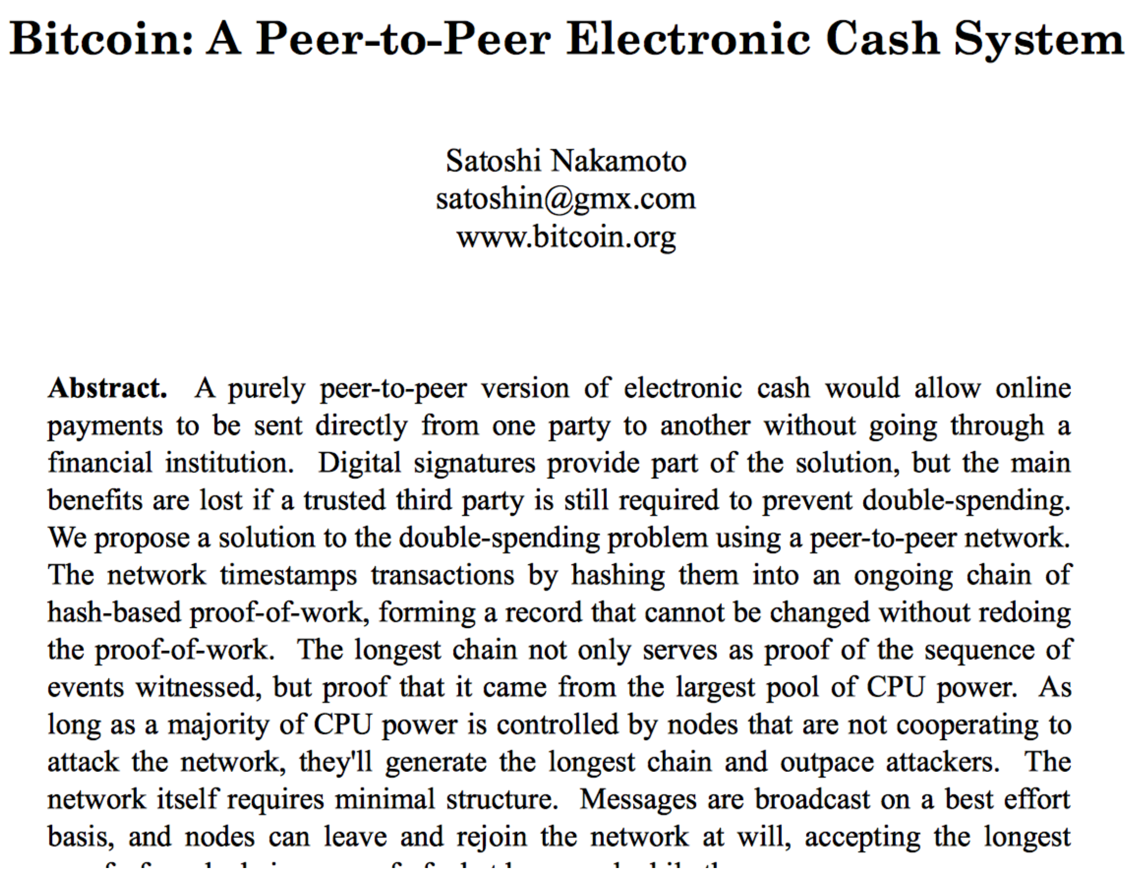
Block 5

Block 6

Block 10

Time Period 1 | Time Period 2 | Time Period 3 | Time Period 4 | Time Period 5 | Time Period 6

Bitcoin Whitepaper – 2008.10.31*



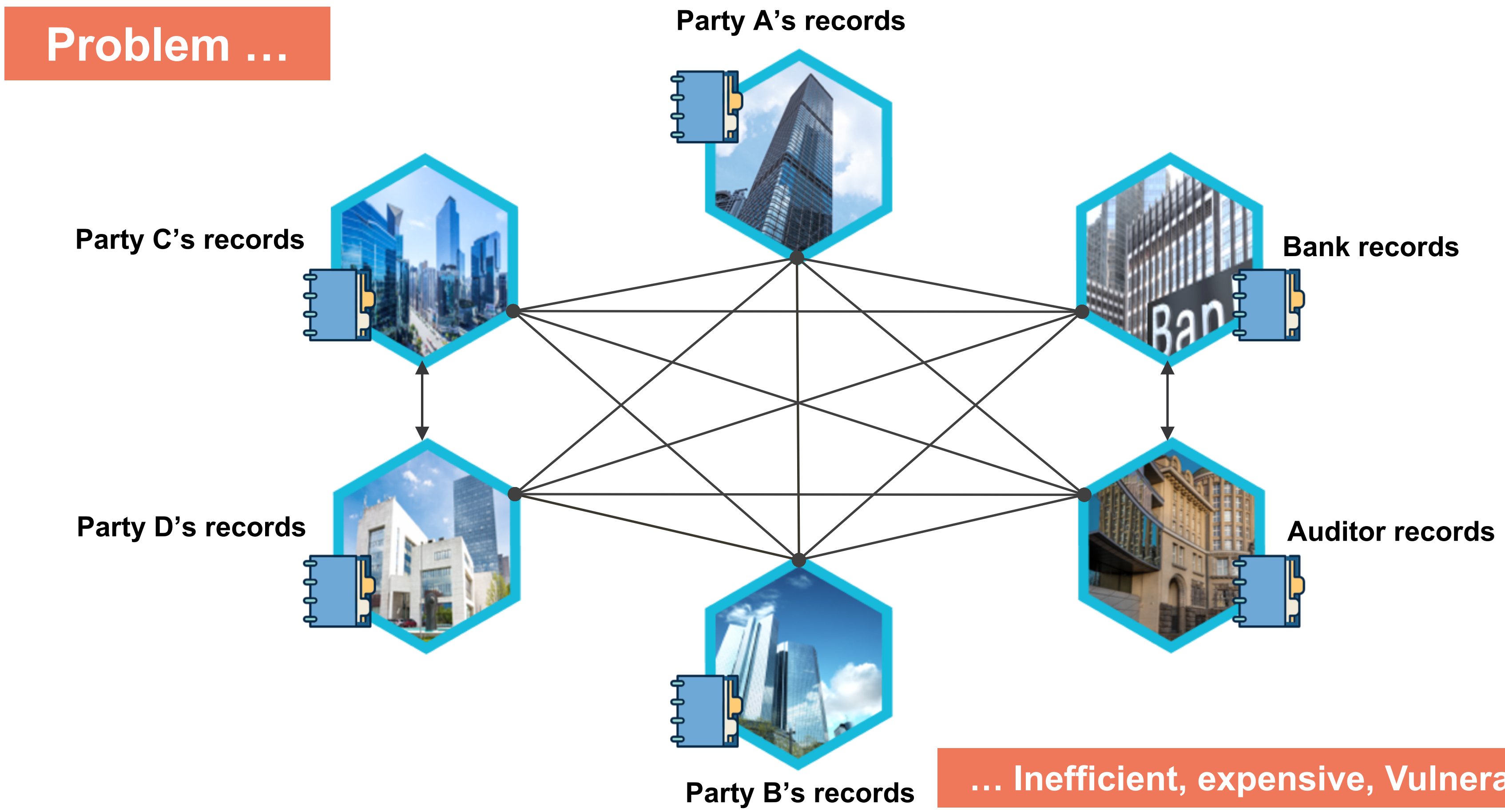
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

Problem of BitCoin System

Problem …



… Inefficient, expensive, Vulnerable

Too Large Blocksize, and Too Slow for processing transactions, because of too many connections and expensive consensus, while privacy and confidentiality are at Risk

Technical Limit of Existing Blockchain

- **Handling massive data** : A new blockchain model should be developed to process massive data for IoT sensor data in smart-city, document, music, movie, etc.
- **Other Issues: transaction processing capacity, throughput, speed, access right control, and privacy protection**

Lower transaction processing speed and throughput

-BitCoin 7tps,
-Ethereum 15tps,
-Hyperledger1000tps
(practically 5~800tps)

Data size(Block): too small

Not Enough Storage

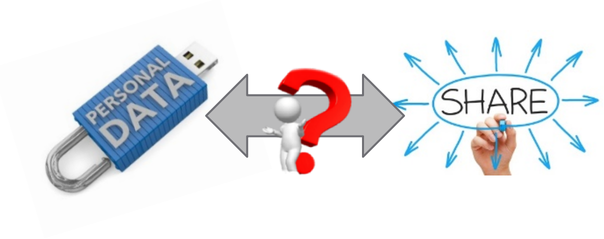
This iPhone cannot be backed up because there is not enough iCloud storage available.
You can manage your storage in Settings.

Close

Upgrade Storage

-issue of data size
-Blocksize (Maximum) 2GB(KT), bitcoin 1MB

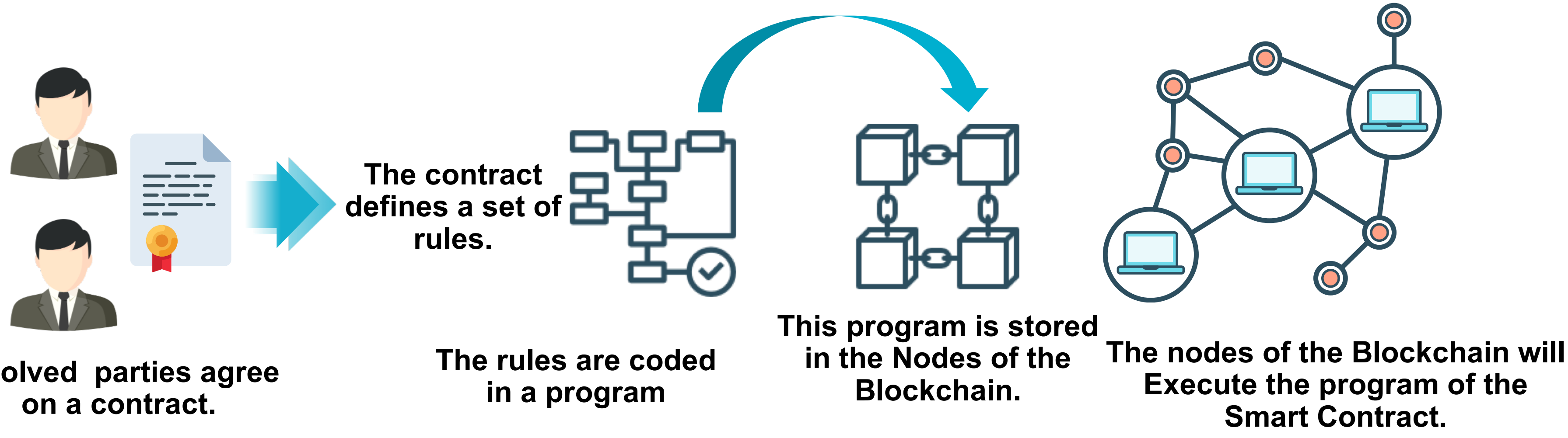
Privacy Protection Too Weak



-Public network to share data, no privacy protection
-Encryption algorithms can be easily broken with quantum computing

2nd Generation: Smart Contract (Ethereum)

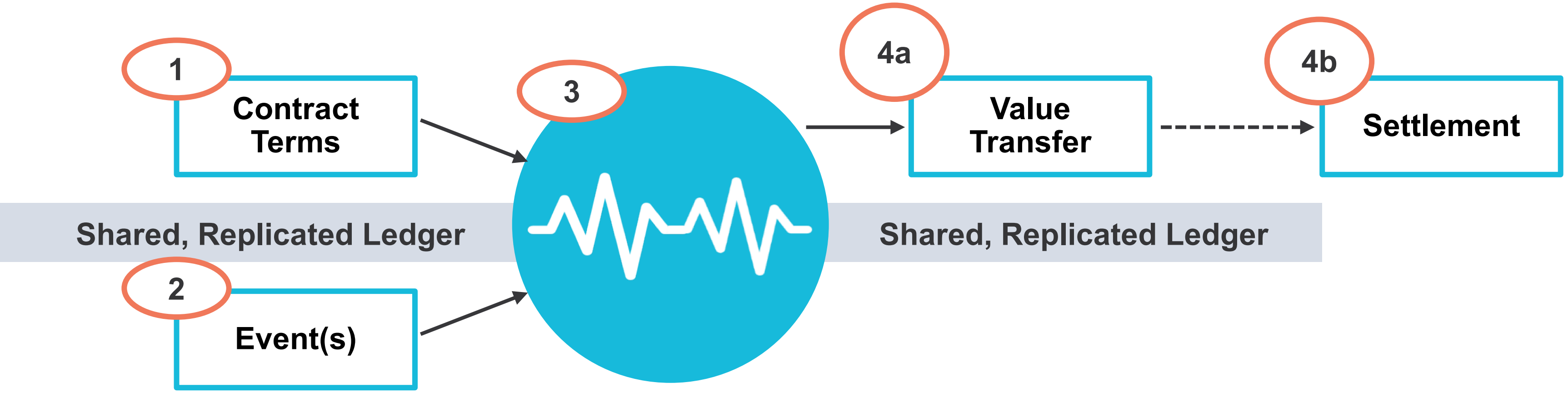
Smart Contracts can automatize execution of transactions


The contract defines a set of rules.
Involved parties agree on a contract.
The rules are coded in a program
This program is stored in the Nodes of the Blockchain.
The nodes of the Blockchain will Execute the program of the Smart Contract.

Smart contracts are useful in many occasions to **replace human intervention**

Risk : The code remains vulnerable and can be corrupted.

Applying Business Logic with Smart Contracts



1 Contract Terms

2 Event(s)

3

Shared, Replicated Ledger

Shared, Replicated Ledger

4a Value Transfer

4b Settlement

1

- Counterparties establish Obligations
- Assets put under custody of smart Contract
- Conditions for execution ("If…then…")

2

- Event triggers contract execution
- Event can refer to:
  - ✓ Transaction Initiated
  - ✓ Information Received

3

- Terms of contract dictate movement of value based on conditions met

4a

- Value transferred to intended recipient as dictated by contract terms
- For digital assets on-chain (e.g. Bitcoin) accounts are atomically settled

4b

- For assets represented off-chain (e.g. Securities, Fiat), value could be moved and settled in off-chain accounts per settlement instructions

Smart Contract-Ethereum

- Vitalik Buterin

Born: Jan 31, 1994(24 yrs)
Russian-Canadian
University of Waterloo
(dropped out)

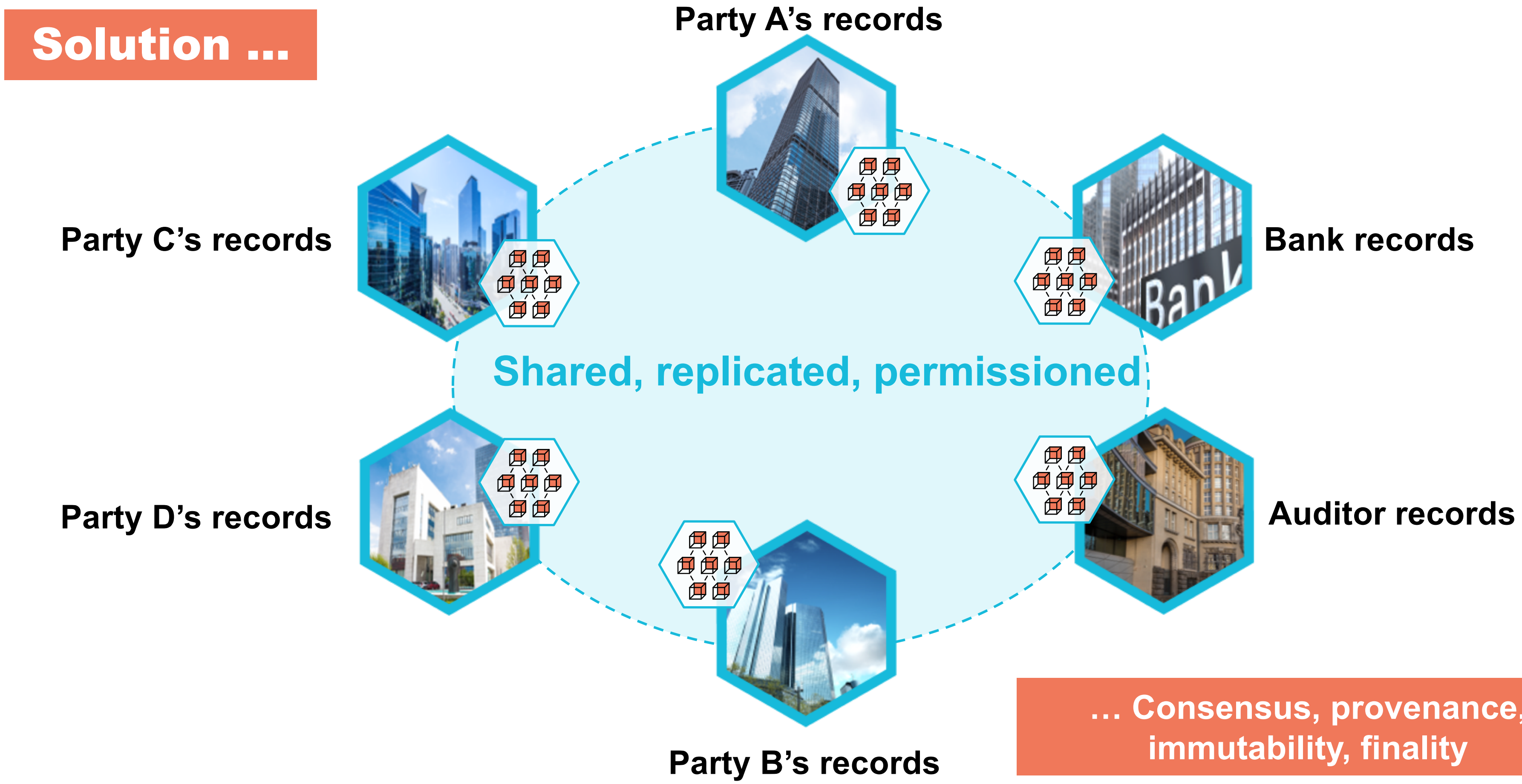
- Bitcoin is a platform for decentralised currency while Ethereum is a platform for decentralised currency and engine for applications which can be run without a need of trusted third party (some central server).

- Smart contract—is a piece of code which is stored in the blockchain network (on each participant database). It defines the conditions to which all parties using contract agrees. So if required conditions are met certain actions are executed.

- First in the Market: July 30, 2015
- Languages: Go, C++, Rust, Solidity

3rd Generation： Hyperledger Blockchain

Solution …



… Consensus, provenance, immutability, finality

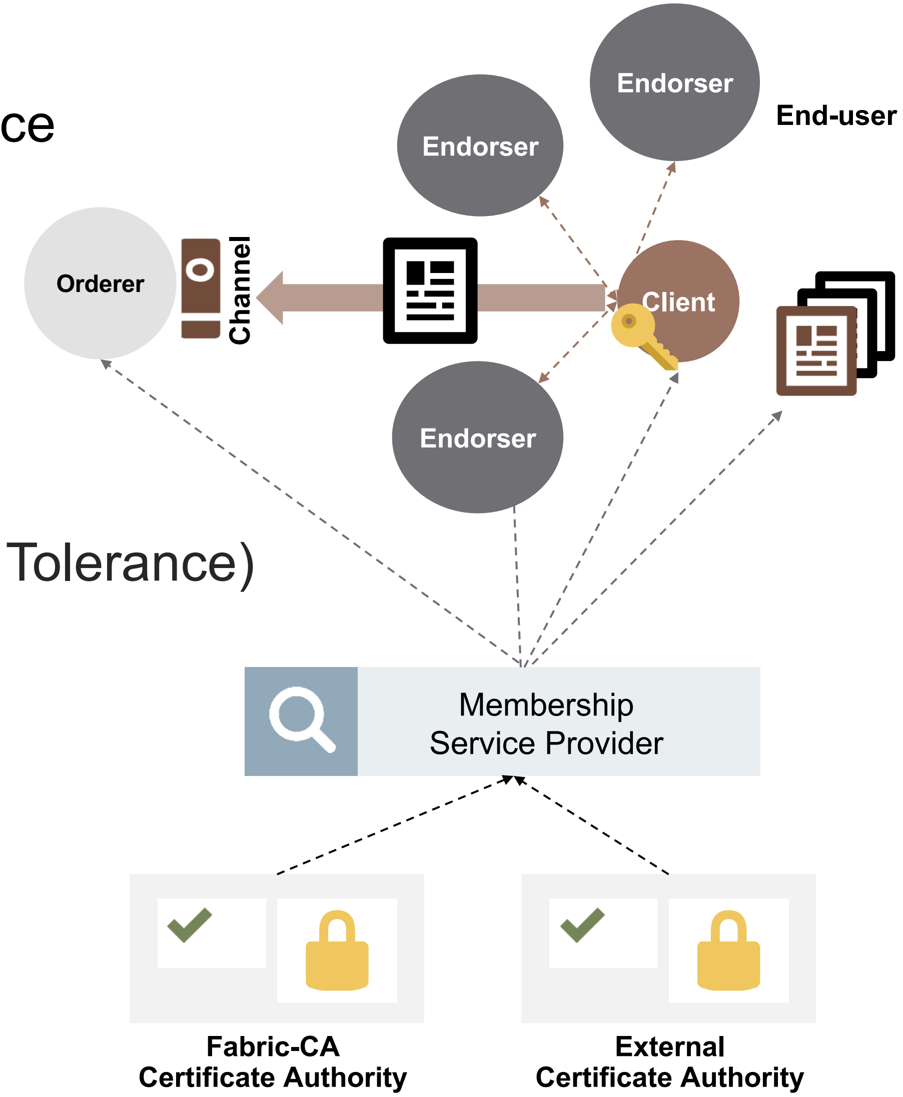
permissioned, distributed, and shared ledger, while providing a secure, robust model for identity, auditability and privacy

Hyperledger Blockchain

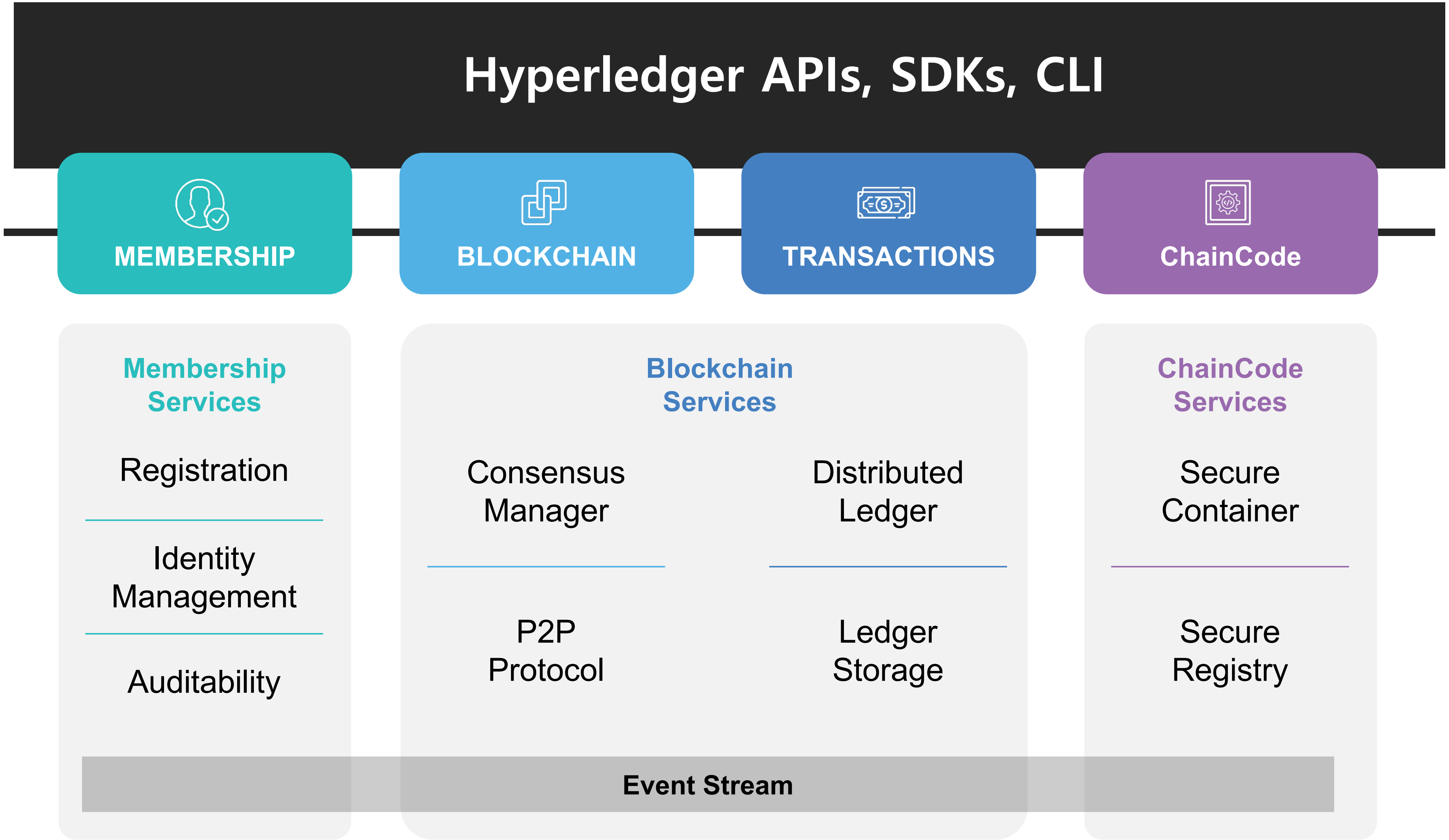
Founded at Dec 17, 2015

30 founded members, Open Source

- Permissioned Chain
- Privacy and Confidentiality
- No Miner or Coin
- Modular Framework
- PBFT(Practical Byzantine Fault Tolerance)
- Smart Contract(ChainCode)
- Searchable
- Auditable



Hyperledger : Services



Hyperledger APIs, SDKs, CLI

MEMBERSHIP

BLOCKCHAIN

TRANSACTIONS

ChainCode

Membership Services

Registration

Identity Management

Auditability

Blockchain Services

Consensus Manager

Distributed Ledger

P2P Protocol

Ledger Storage

ChainCode Services

Secure Container

Secure Registry

Event Stream

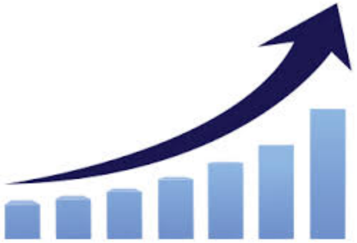
Why Hyperledger?

- **Practical Structure Suggested for existing Transactions**
- **Optimize Conflicting Goals**

Privacy & Confidentiality

Auditability & ‘Searchable’

Transparency



scalability

Modularity

(Source: IBM, Hyperledger Fabric)

Hyperledger : Practical Requirement (1)

- Privacy and Confidentiality
  - Privacy: ID, behavior, transaction and conditions, and parameters of other nodes should not be disclosed to network participants except parties directly involved
  - Secret data in transaction should be decrypted and readable to only interested parties
  - Only involved parties can decrypt and read transaction contents (data and documents)
  - Cryptographic security should be guaranteed so that business logic operates at the runtime of the business
- Searchable

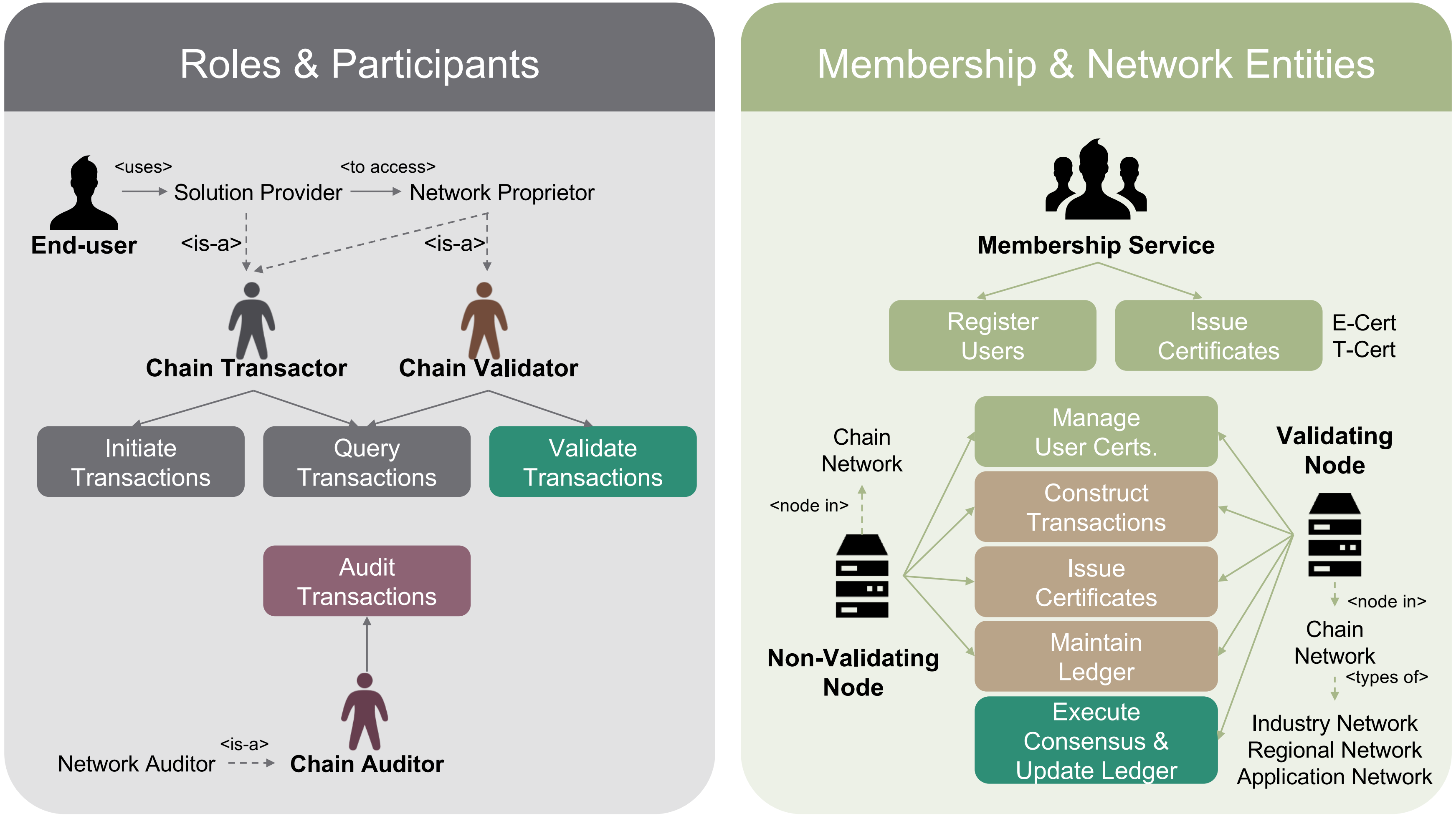
Confidentiality should be kept while contents of the ledgers should be searchable to the involved parties

Sellers to join the bidding should reveal offers in ledgers to Buyers in the network

Hyperledger : Practical requirement(2)

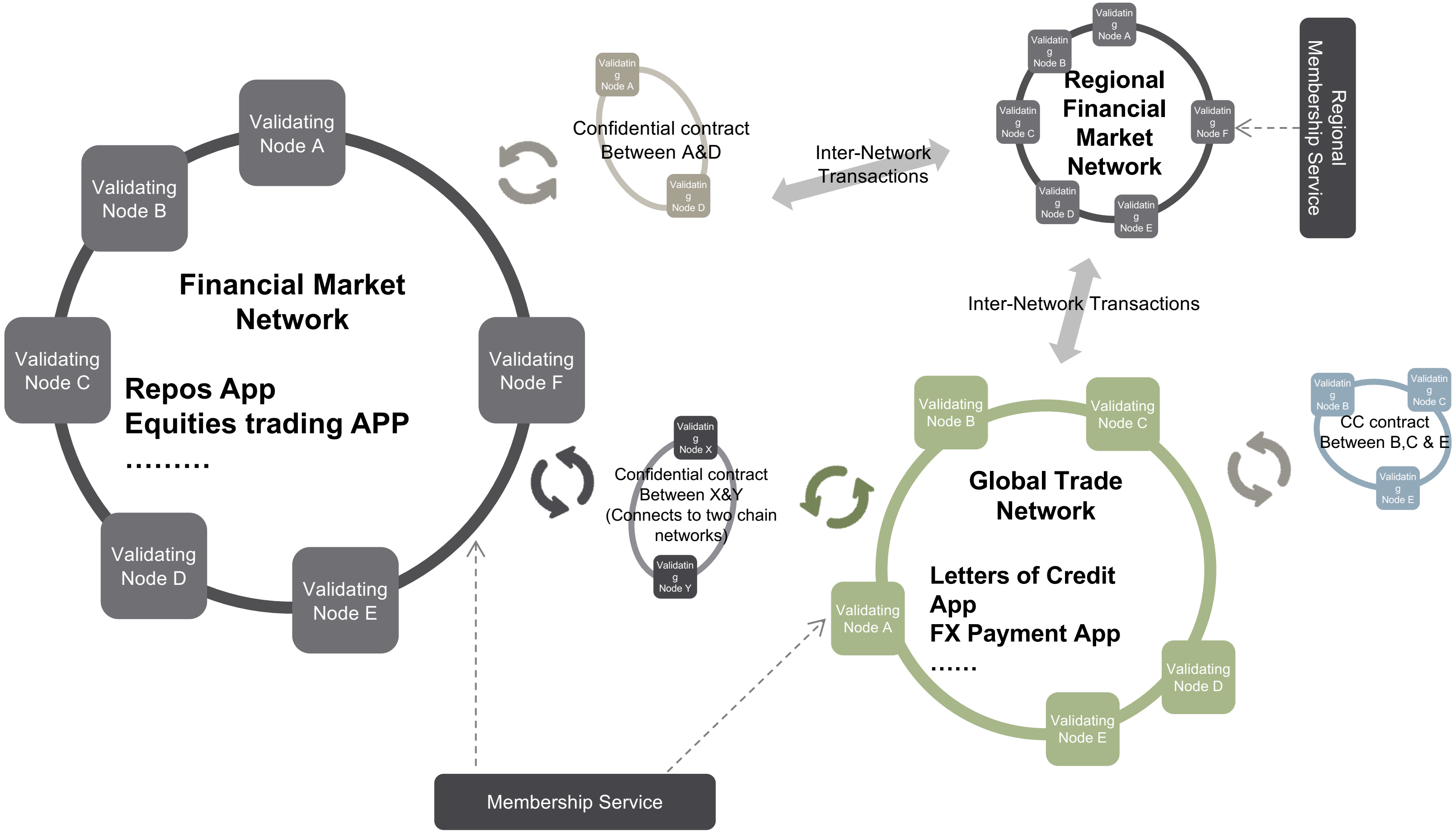
- **ID Management Principle: All the transactions should follow regulations and thereby should be accessed and investigated by Regulators**
  - All activities are initiated with cryptographic Certificates which can put into user's confidential data
  - Register issue ID for network participation
  - Network members can participate into transactions with key issued by ID membership, while users joining transaction can hide ID to keep privacy
- **Modular Consensus**
  - All participants in the network should be able to select consensus algorithms and therefore the algorithms should be pluggable.
  - Consensus algorithm should comply to Byzantine Fault Tolerance(PBFT)
- **Performance, Scalability**
  - Performance: all the ledgers should operate in the time frame of search, authentication, conflict resolution, and others for more than 100 years
  - Scalability: It should be assumed that number of nodes and networks can enormously extend, while it can operate without degradation of functions and assumptions, with time passage

Hyperledger : System Context



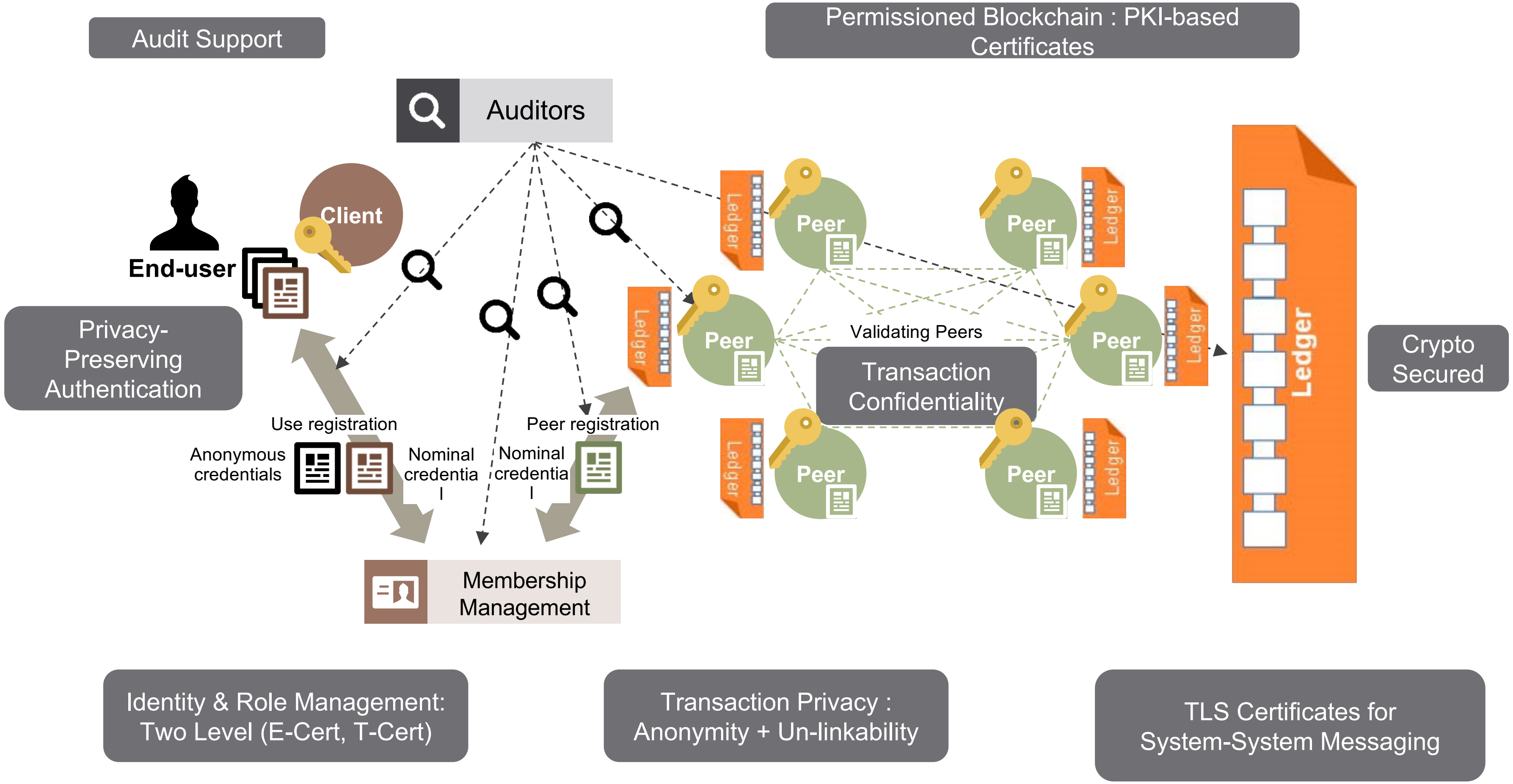
(Source: IBM, Hyperledger Fabric)

Hyperledger Blockchain Networks



(Source: IBM, Hyperledger Fabric)

Hyperledger : Security Review



Audit Support

Permissioned Blockchain : PKI-based Certificates

Privacy-Preserving Authentication

Crypto Secured

Identity & Role Management: Two Level (E-Cert, T-Cert)

Transaction Privacy : Anonymity + Un-linkability

TLS Certificates for System-System Messaging

(Source: IBM, Hyperledger Fabric)

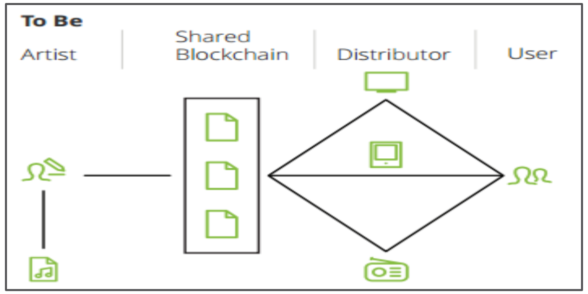
CONTENTS

I. Evolution of Blockchain Technology

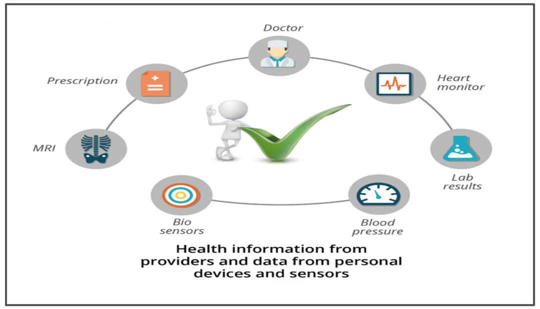
II. **Blockchain for Everything?**

III. Blockchain Applications

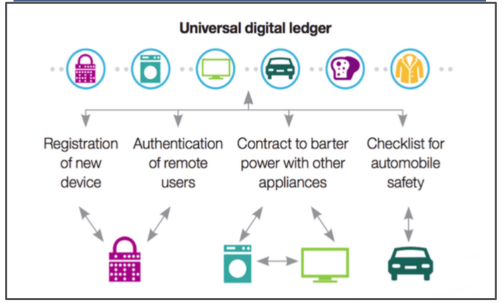
Media blockchain



Medical blockchain


Doctor
Prescription
Heart monitor
MRI
Lab results
Bio sensors
Blood pressure
Health information from providers and data from personal devices and sensors

IoT blockchain

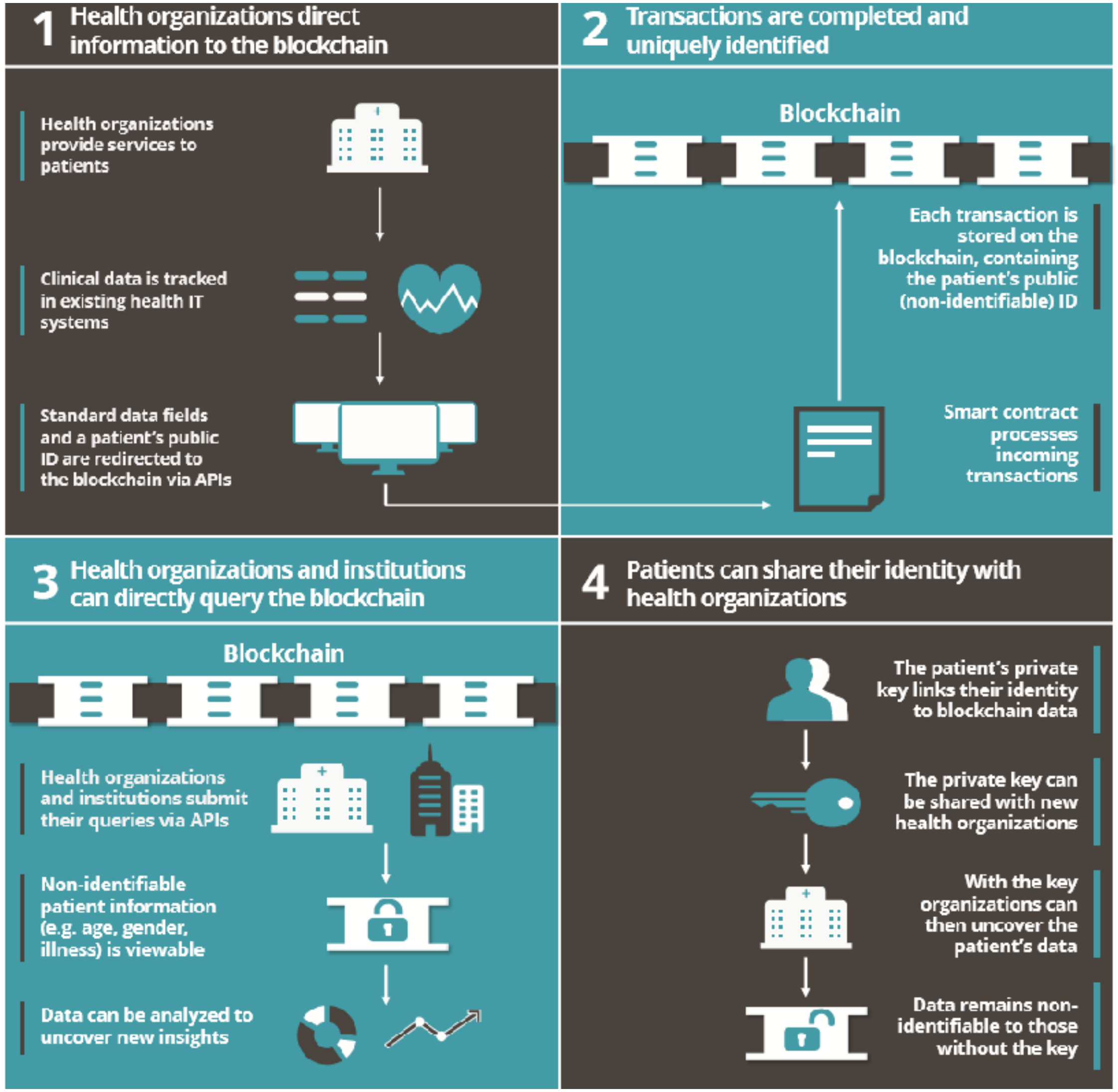

Universal digital ledger
Registration of new device
Authentication of remote users
Contract to barter power with other appliances
Checklist for automobile safety

Medical Blockchain

- **In your life, you have to visit 1925 days hospital & clinics**
- **Life Cycle**
  - **Before birth: testing for deformed baby or others**
  - **0 year ~ youth: health test, dental testing, Vaccination, disease treatment , etc.**
  - **Adult: medical test, cancer test, life shifting test, vaccination, Genome inspection, disease treatment, etc.**
- **Disease treatment includes**
  - **type: treatment, diagnosis, testing, prescription.**
  - **insurance: health insurance, medical benefits, cancer insurance, accidents insurance, unemployment insurance, occupational health and safety insurance**

- Currently, medical records are scattered between heterogenious IT systems (clinic and hospitals). Example: in Boston area, patent’s records are stored in 26 systems which can use different languages. In case of emergency, the data and records cannot be exchanged even in critical situation. (http://dataconomy.com/2017/12)
- Other problems: (1) single point of failure (2) Easy targets for hackers and other malicious individuals

American Health Care Block Chain



1 Health organizations direct information to the blockchain

Health organizations provide services to patients

Clinical data is tracked in existing health IT systems

Standard data fields and a patient's public ID are redirected to the blockchain via APIs

2 Transactions are completed and uniquely identified

Blockchain

Each transaction is stored on the blockchain, containing the patient's public (non-identifiable) ID

Smart contract processes incoming transactions

3 Health organizations and institutions can directly query the blockchain

Blockchain

Health organizations and institutions submit their queries via APIs

Non-identifiable patient information (e.g. age, gender, illness) is viewable

Data can be analyzed to uncover new insights

4 Patients can share their identity with health organizations

The patient's private key links their identity to blockchain data

The private key can be shared with new health organizations

With the key organizations can then uncover the patient's data

Data remains non-identifiable to those without the key

- Now is probably the right time in our history to take a fresh approach to data sharing in health care

- Higher security and privacy, less admin time for doctors so there's more time to spend on patient care, and even better sharing of research results to facilitate new drug and treatment therapies for disease

P2P Banking in the world

- A largest UNICORN start-up came into global financial world, making everyone in financial community nervous

- ANT Financial: 150 B USD (Wall street Journal), the world largest bank in the world, surpassing Goldman Sachs, PayPal.

- ANT Financial is a P2P bank. Will use blockchain for banking transactions

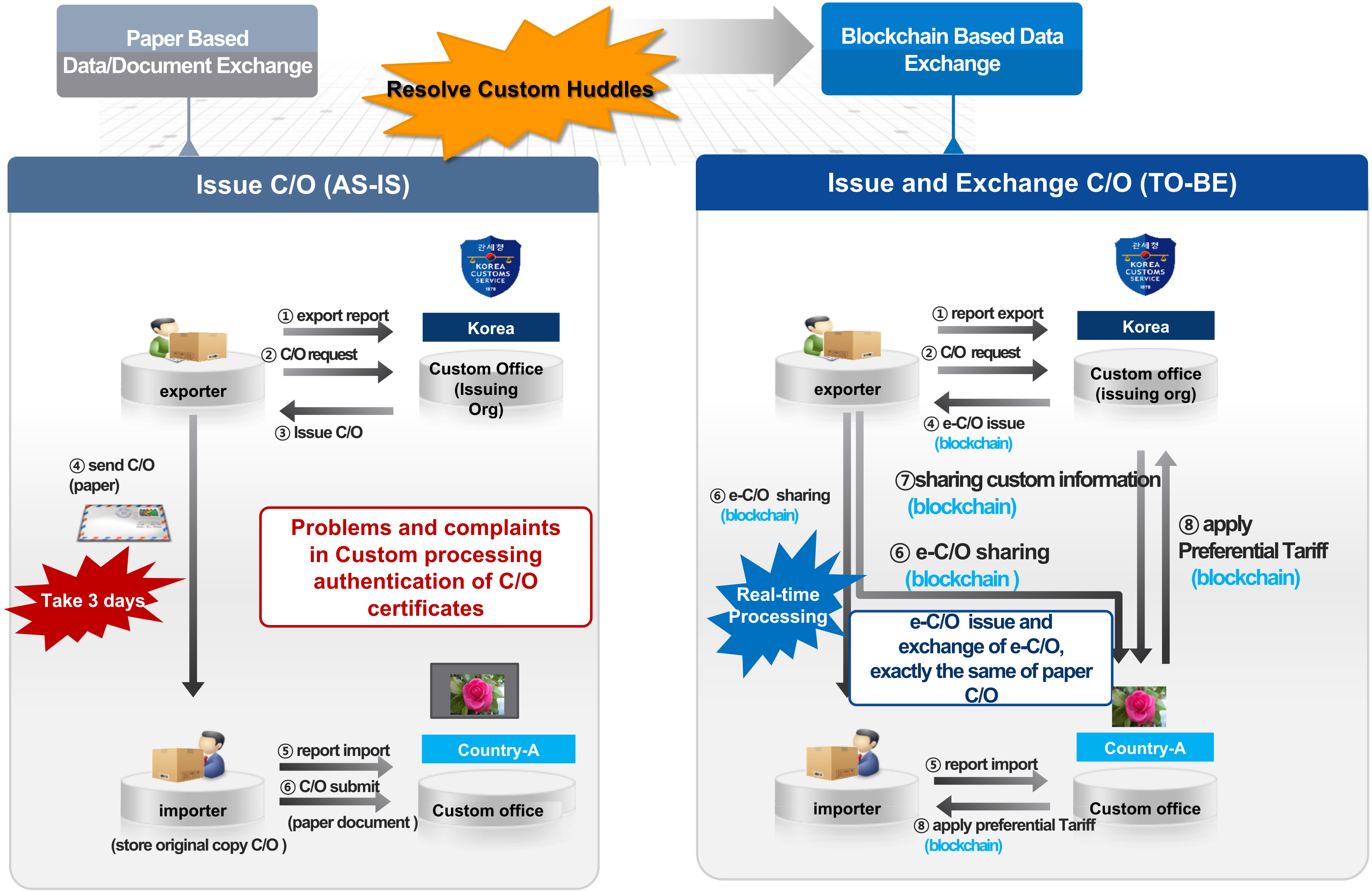
CONTENTS

1. Evolution of Blockchain Technology

2. Blockchain for Everything?

3. Blockchain Applications

(1) Blockchain Based Certificate of Origin (C/O) System



Paper Based Data/Document Exchange

Resolve Custom Huddles

Blockchain Based Data Exchange

Issue C/O (AS-IS)

exporter

① export report

② C/O request

③ Issue C/O

Korea

Custom Office (Issuing Org)

④ send C/O (paper)

Take 3 days

Problems and complaints in Custom processing authentication of C/O certificates

importer

(store original copy C/O)

⑤ report import

⑥ C/O submit

(paper document)

Country-A

Custom office

Issue and Exchange C/O (TO-BE)

exporter

① report export

② C/O request

④ e-C/O issue (blockchain)

Korea

Custom office (issuing org)

⑥ e-C/O sharing (blockchain)

⑦sharing custom information (blockchain)

⑥ e-C/O sharing (blockchain)

⑧ apply Preferential Tariff (blockchain)

Real-time Processing

e-C/O issue and exchange of e-C/O, exactly the same of paper C/O

importer

⑤ report import

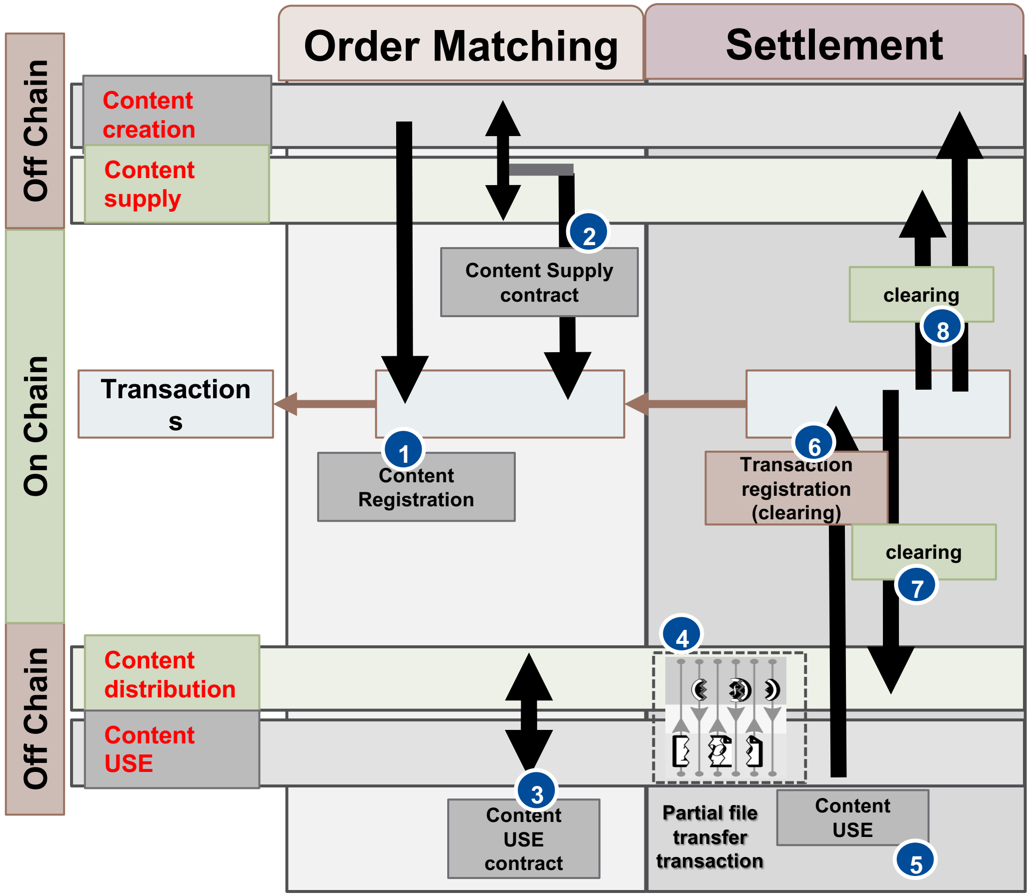
⑧ apply preferential Tariff (blockchain)

Country-A

Custom office

(2) Blockchain Based Content Distribution: Media Chain

- Integrated system architecture for content creation, P2P collection, P2P distribution, use, and clearing



Massive data transaction technology (capacity) ① ④

- Development: Massive Data Off-chain transfer protocol and file structure
- A Hybrid P2P protocol for Massive Data Off-chain

High-speed real-time transaction processing technology (speed) ⑥

- High-speed synchronization technology for real-time processing
- Off-chain transaction authentication technology (KIDS)
- Development of Transaction compression technology for processing off-chain Micro transactions

Privacy preserving Data storage and Search Technology ⑤

- **Quantum Safe encryption technology (Homomorphic, attribute)**
- **Group access control based on Domain certificates**
- Quick response and high-speed scanning based on Cached distributed DB

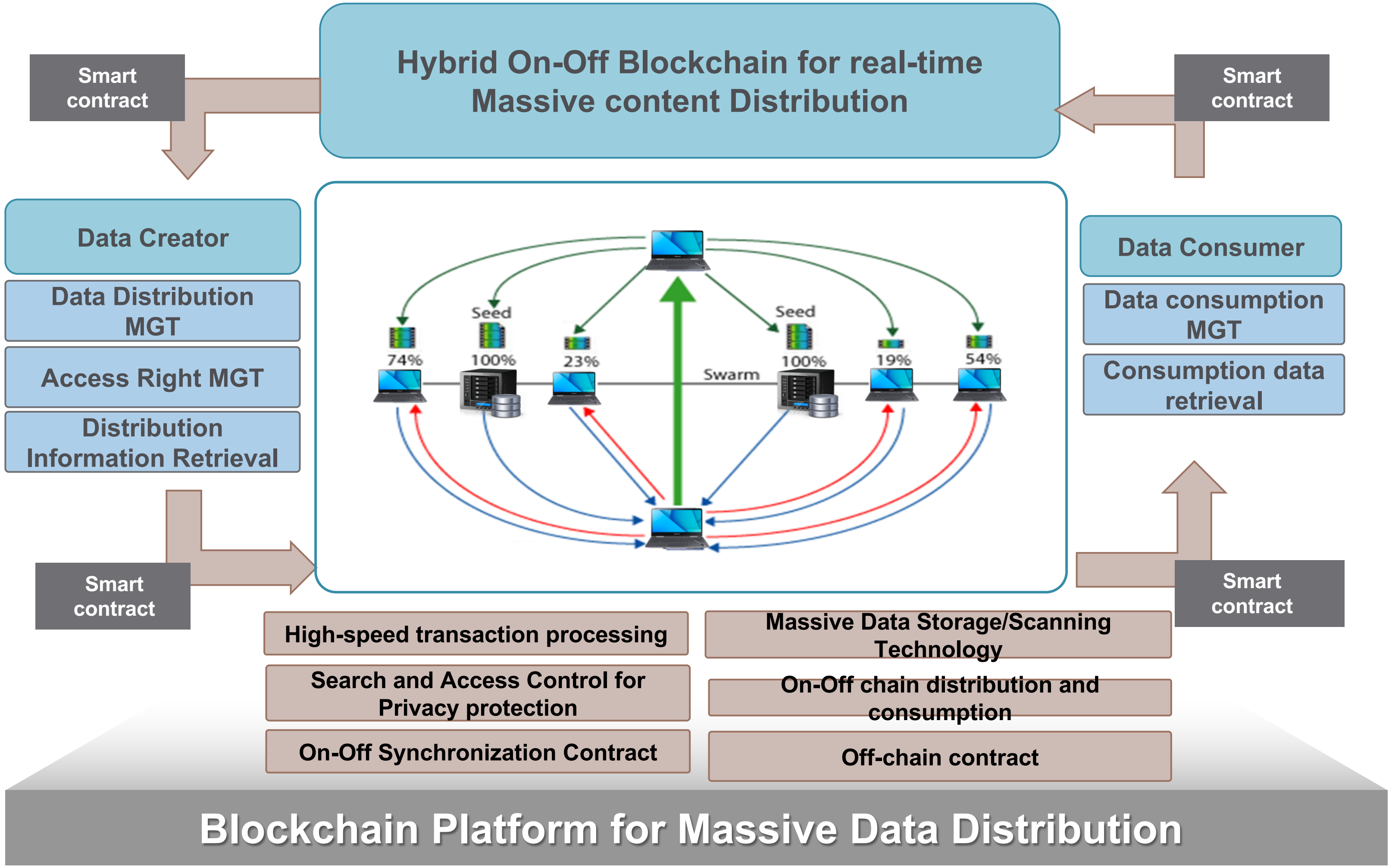
On-off distribution contract ② ③

- On-Off chain data distribution contract synchronization technol ⑦ ⑧
- **Template based Smart Contract Framework**
- Off-chain data contract processing

CID embedding technology for On-Off chain synchronization ① ⑤

- CID embedding, extraction technology for text, image, audio, video
- **Synchronizing On-Off chain transaction with CID**

(2) Blockchain Based Content Distribution:Media Chain



Hybrid On-Off Blockchain for real-time Massive content Distribution

Smart contract

Smart contract

Data Creator

Data Distribution MGT

Access Right MGT

Distribution Information Retrieval

Data Consumer

Data consumption MGT

Consumption data retrieval

Smart contract

Smart contract

High-speed transaction processing

Massive Data Storage/Scanning Technology

Search and Access Control for Privacy protection

On-Off chain distribution and consumption

On-Off Synchronization Contract

Off-chain contract

Blockchain Platform for Massive Data Distribution

Blockchain Evolution Summary

Yet to complete

Blockchain 200

BitCoin 2008

Ethereum 2013

Hyperledger 2015

Thank you