THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN

AUTOMOTIVE
LINUX SUMMIT

How We Can Expand the Utilization of Blockchain Technology: Security and Use Case Perspective

June 22, 2018

Toshiya Cho
Senior Evangelist / Managing Director
Financial Information Systems Sales Management Division
Hitachi, Ltd.

THE LINUX FOUNDATION

Contents

1. Hitachi’s Contribution to Open Source Community
2. For Wider Use of Blockchain: Security Aspect
3. For Wider Use of Blockchain: Use Case Aspect

1. Hitachi’s Contribution to Open Source Community

Major FinTech Business Areas for Hitachi

HITACHI
Inspire the Next

Hitachi focuses on 4 areas of technology in FinTech to realize Society 5.0 where multiple industries are interconnected as a Super-smart society. We believe that **Blockchain** is a key technology for that purpose.

1. Interface

Open API* enables new services connecting FSIs with FinTech firms and other industries.

2. Security / Authentication

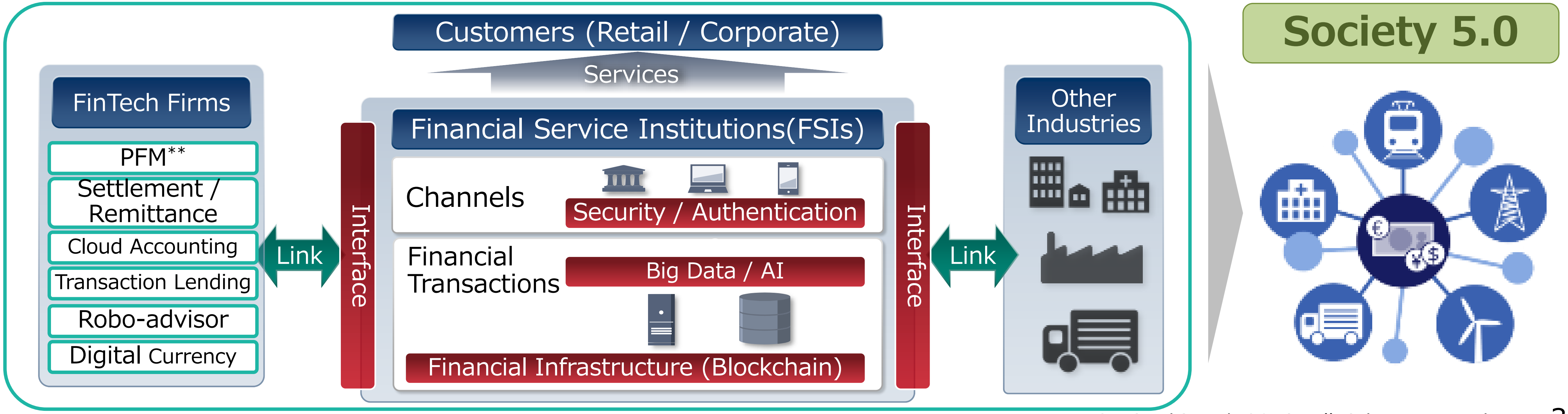
Wider usage of **Biometrics** enables services with higher security and more convenience.

3. Big Data / AI

Big data analytics and **AI** enable higher operational efficiency and new product / service development.

4. Financial Infrastructure

Blockchain is expected to bring huge impact on various industries not limited to finance.



Customers (Retail / Corporate)

Services

FinTech Firms

PFM**

Settlement / Remittance

Cloud Accounting

Transaction Lending

Robo-advisor

Digital Currency

Link

Interface

Financial Service Institutions(FSIs)

Channels

Security / Authentication

Financial Transactions

Big Data / AI

Financial Infrastructure (Blockchain)

Interface

Link

Other Industries

Society 5.0

*API: Application Programming Interfaces **PFM: Personal Financial Management

Hyperledger: Open Innovation in Blockchain

Hyperledger is an open source collaborative effort to advance cross-industry blockchain technologies. It is a global collaboration, hosted by the Linux Foundation with more than 250 organizational participants. Hitachi is a founding premier member of Hyperledger and makes a significant contribution to the development.

HYPERLEDGER
PREMIER MEMBER

accenture High performance. Delivered. | AIRBUS | AMERICAN EXPRESS | Baidu 百度 | CHANGE HEALTHCARE

CISCO | DAIMLER | Deutsche Bank | Digital Asset | DTCC Securing Today. Shaping Tomorrow.

FUJITSU | HITACHI Inspire the Next | IBM | intel | J.P.Morgan

NEC | SAP | TRADESHIFT | 万达·飞凡科技 WANDA FFAN TECHNOLOGY

(Alphabetical Order as of June 1, 2018. Corporate logo is registered trademark.)

Our Contribution to HYPERLEDGER FABRIC

- Hitachi has been contributing mainly to the Enhancement of the quality of Hyperledger Fabric and the acceleration of its releases.
- Hitachi is the **Second Largest Contributor** for Hyperledger Fabric for the latest stable release (v1.1) in the community.

Top Contributors to Hyperledger Fabric by Company between v1.0 and v1.1

Rank	Affiliation
1	IBM
(2)	Individuals / Affiliation Unknown
3	Hitachi
4	IT People
5	State Street
6	Hyperchain Technology

- Based on the number of commits between v1.0 and v1.1 release
- Calculated using the commits in the official Git repositories (*fabric, fabric-ca, fabric-sdk-node, fabric-samples, fabric-chaincode-node, fabric-chaintool*)

Hitachi's Ongoing Contributions

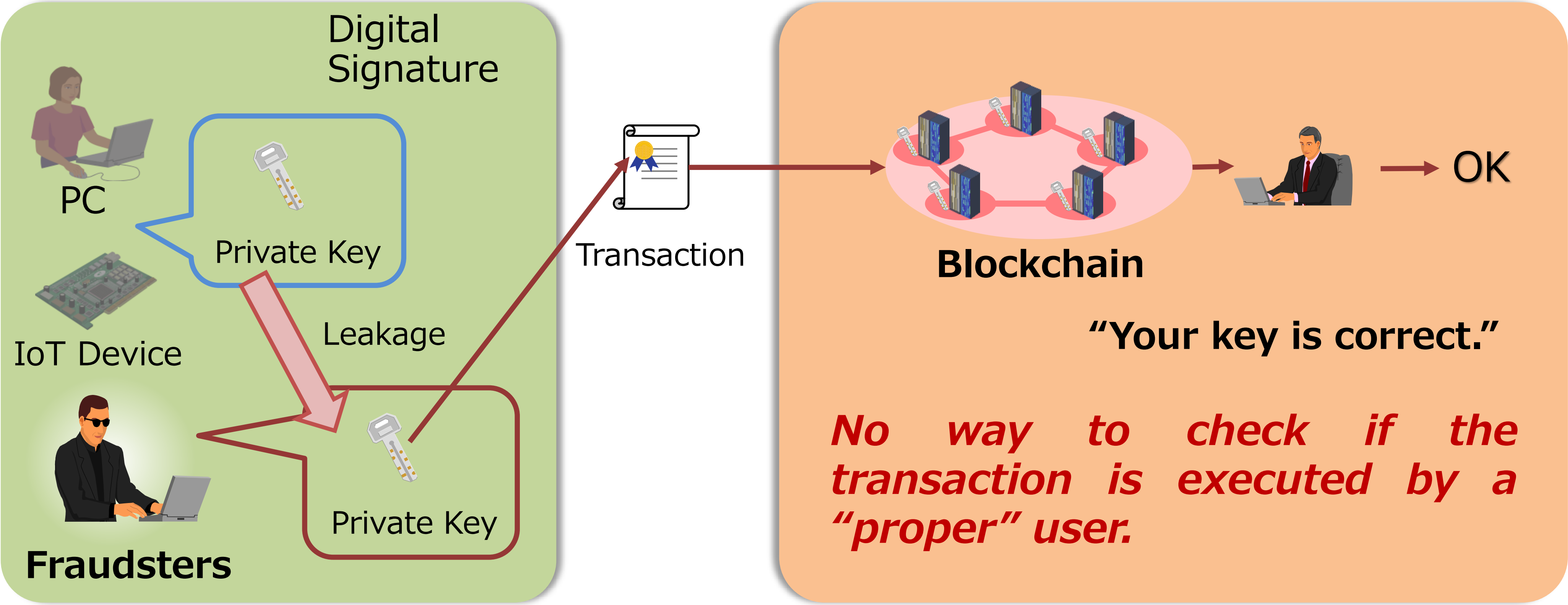
- **Quality Enhancement**
  - *Easier to Use Even for First-time Users*
    - ✓ Bug Fixes
    - ✓ Documentation Improvement
    - ✓ Test Improvement
- **Blockchain Integrity**
  - *For Auditable Blockchain Systems*
    - ✓ Integrity Checks
    - ✓ Evidence Extraction

2. For Wider Use of Blockchain: Security Aspect

Private Key Issue on Blockchain

A transaction in blockchain network is generated using digital signature by the private key. And a verifier in blockchain confirms the authenticity of the key with the digital signature in the transaction.

However, a verifier has no way to check the authenticity of transactions. If fraudsters obtain a private key, they can execute a transaction using that key.



"Your key is correct."

No way to check if the transaction is executed by a "proper" user.

Private Key Management Issues on Blockchain

Existing Methods and Issues

1. Storing password or fingerprint on smartphone

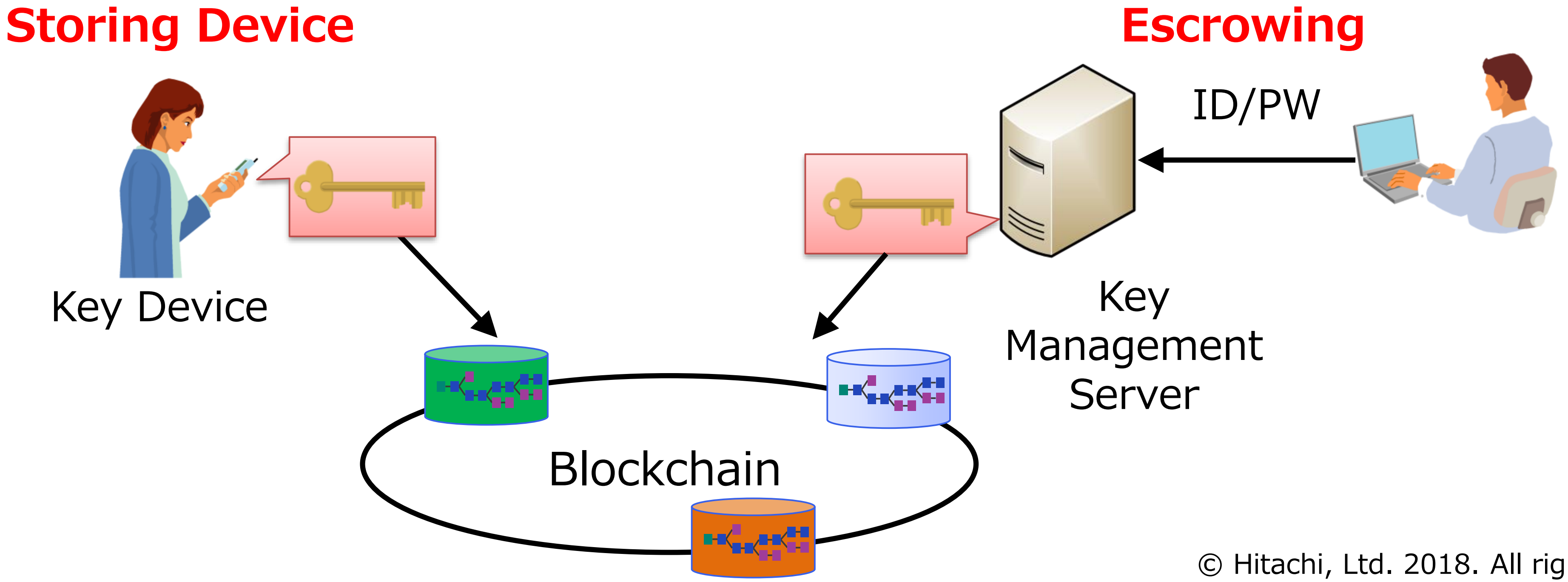
⇨ If the owner loses the smartphone, s/he also possibly loses assets managed on Blockchain.

⇨ There is no alternative device.

2. Escrowing on Key Management Server

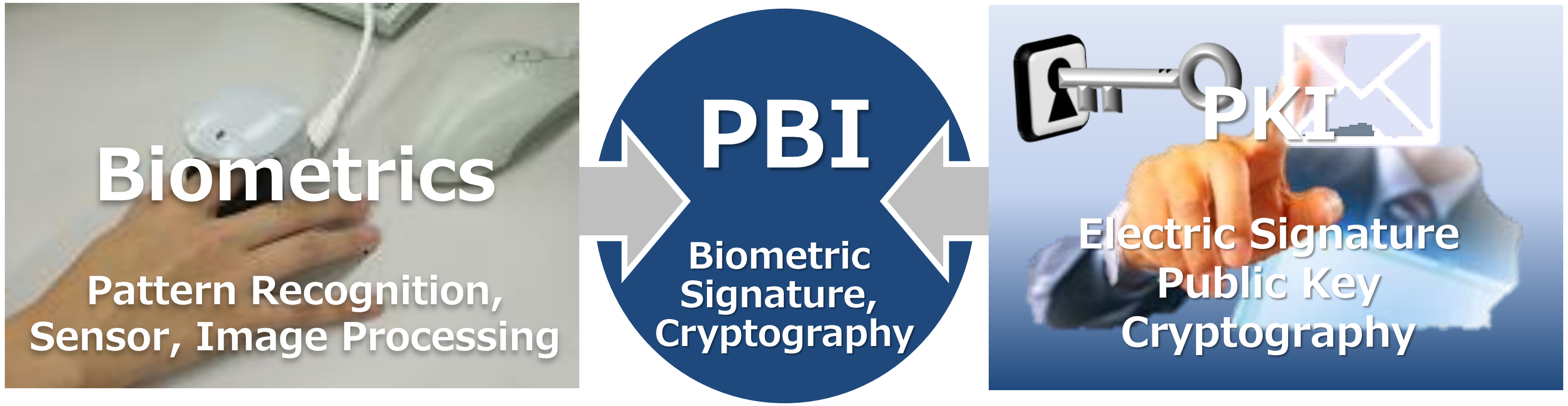
⇨ Who manages the server in the decentralized environment?

⇨ Is the server secure?



Applying Public Biometric Infrastructure (PBI) to Blockchain

PBI Is PKI Using Biometrics as a Private Key.



Biometrics

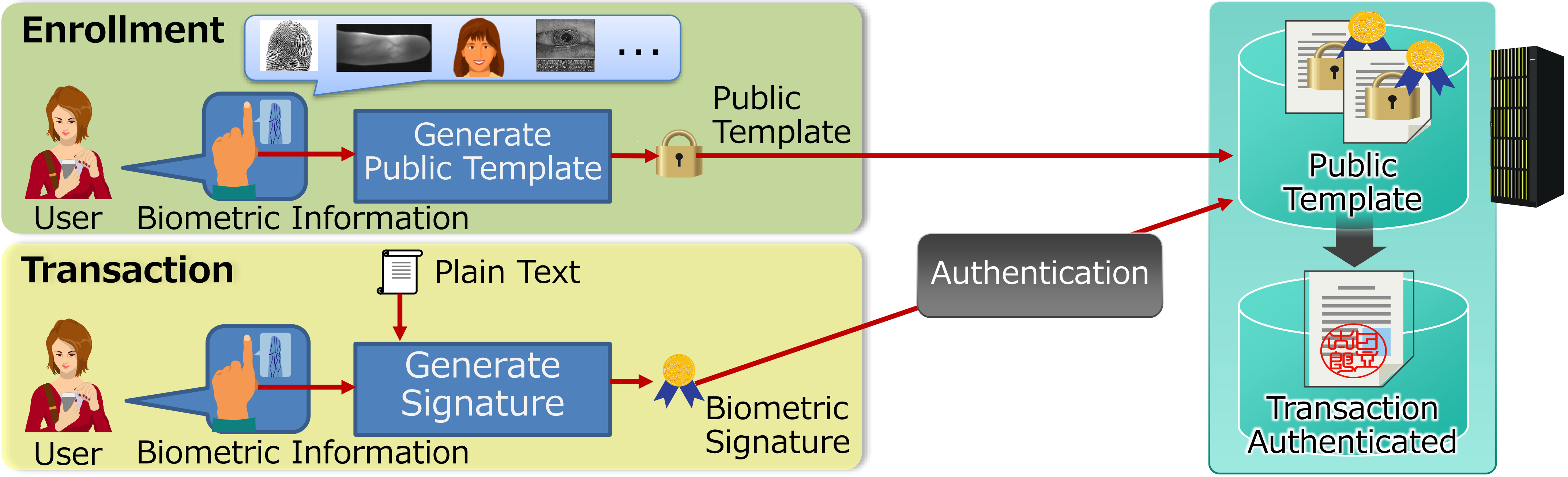
Pattern Recognition, Sensor, Image Processing

PBI

Biometric Signature, Cryptography

PKI

Electric Signature Public Key Cryptography



Enrollment

User

Biometric Information

Generate Public Template

Public Template

Transaction

Plain Text

User

Biometric Information

Generate Signature

Biometric Signature

Authentication

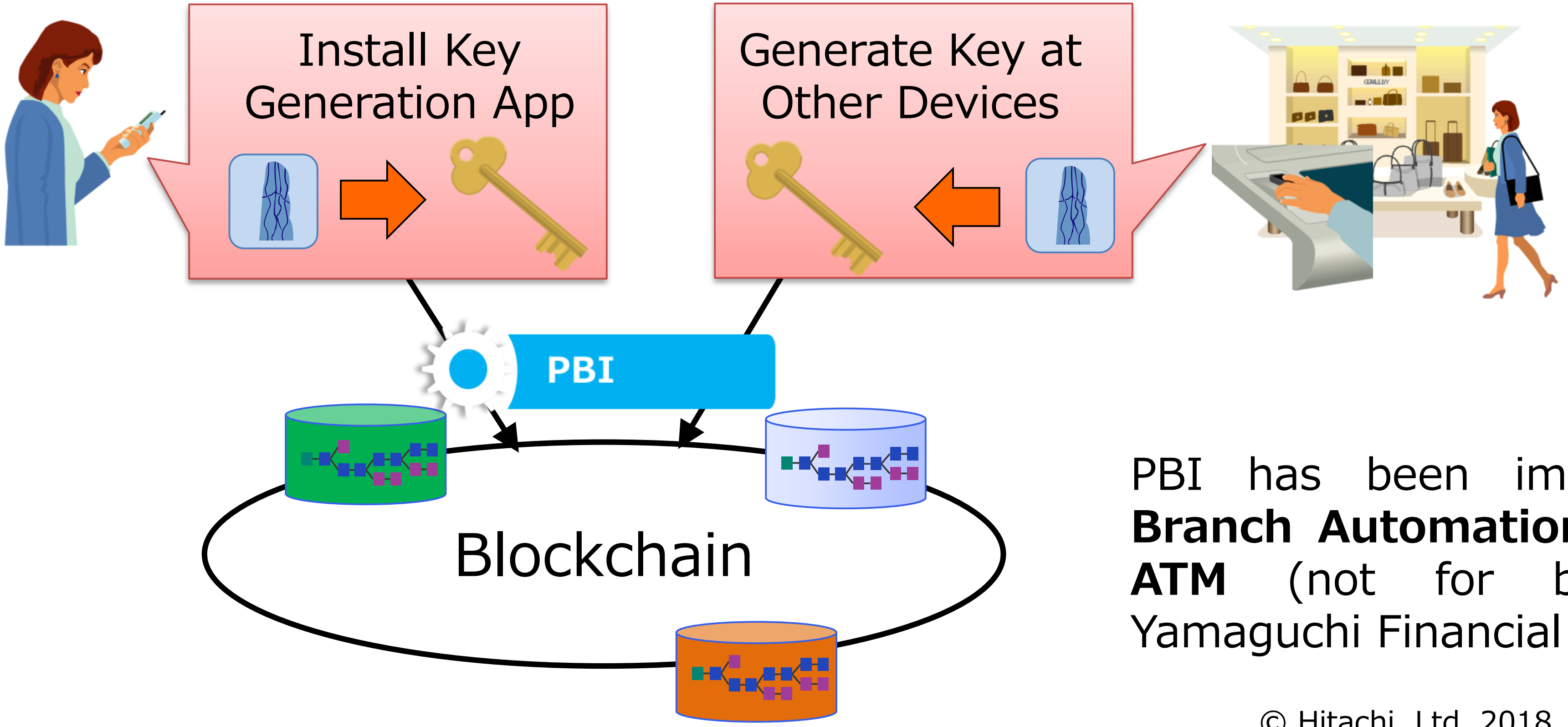
Public Template

Transaction Authenticated

Benefits of PBI for Blockchain

Applying PBI to Blockchain, we can expect:

- Key management server is not necessary.
- Key management itself is not necessary to be within a device. Reinstallation of the application would be OK even if you lose your device such as smartphone.
- Same methods can be applied to multiple applications and locations as the system is device-independent.

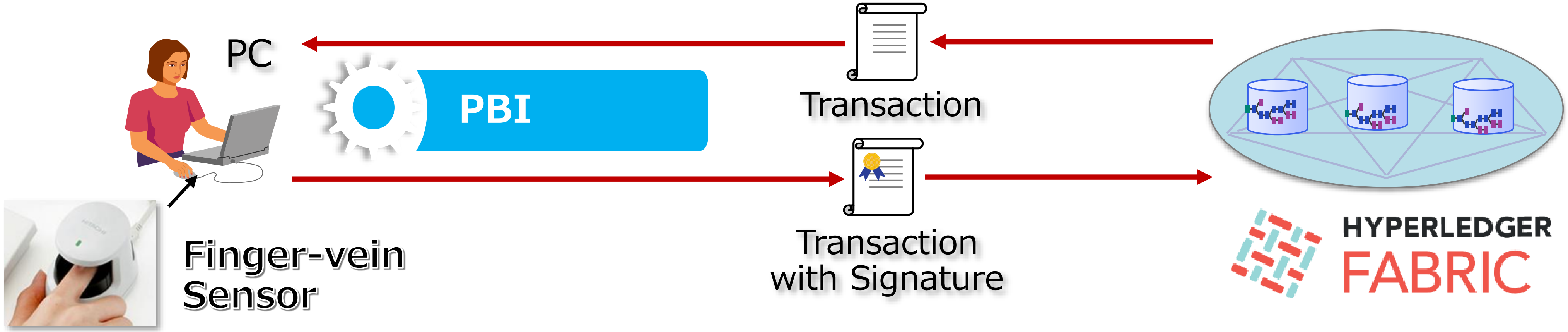


YMFG
Yamaguchi Financial Group

PBI has been implemented for **Branch Automation System and ATM** (not for blockchain) at Yamaguchi Financial Group.

Evaluation of PBI on HYPERLEDGER FABRIC

We have already had an experiment using PBI through Finger Vein authentication over Hyperledger Fabric to ensure the applicability of PBI.



	Data / Process	Public Key Based Signature	PBI Based Signature
File Size (For Primitive Data)	Public Template	-	10Kbyte
	Public Key Certificate	1Kbyte	-
	Signature	71byte	71byte
Process Time (For Primitive Function)	Public Template Generation	-	235 ms
	Signature Generation	19 ms	169 ms
	Signature Verification	14 ms	14 ms

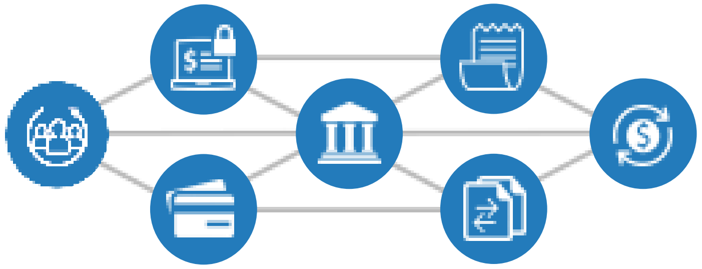
CPU: Intel Core™ i5-3470 3.2GHz, Memory: 4GB

3. For Wider Use of Blockchain: Use Case Aspect

Expansion of Blockchain Application

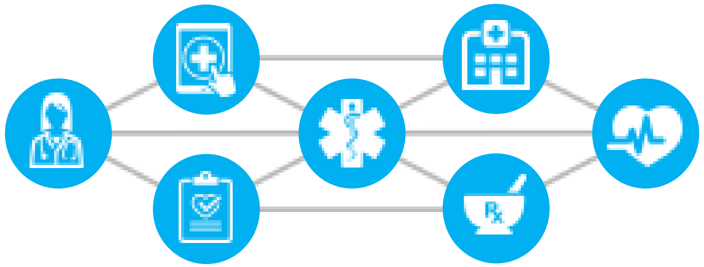
While blockchain technology has been conceived to realize bitcoin, applicability is blockchain is not limited to bitcoin and it can be used much wider range of purposes.

Blockchain allows multiple parties to securely interact with the same universal source of truth. Starting from financial industry, areas of application are expanding to other industries.



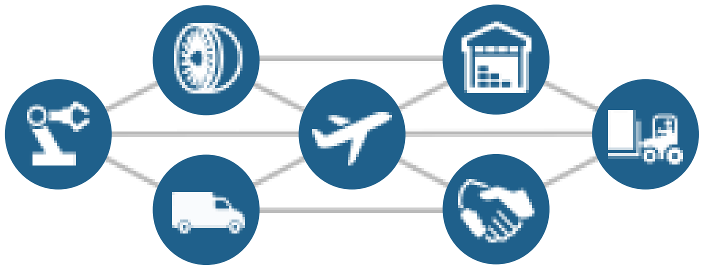
Finance

- Streamlined Settlement
- Improved Liquidity,
- Increased Transparency
- New Products/Markets



Healthcare

- Unite Disparate Processes
- Increase Data Flow And Liquidity
- Reduce Costs
- Improve Patient Experience And Outcomes



Supply Chain

- Track Parts And Service Provenance
- Ensure Authenticity Of Goods
- Block Counterfeits
- Reduce Conflicts

Source: Linux Foundation with additions and modifications by Hitachi.

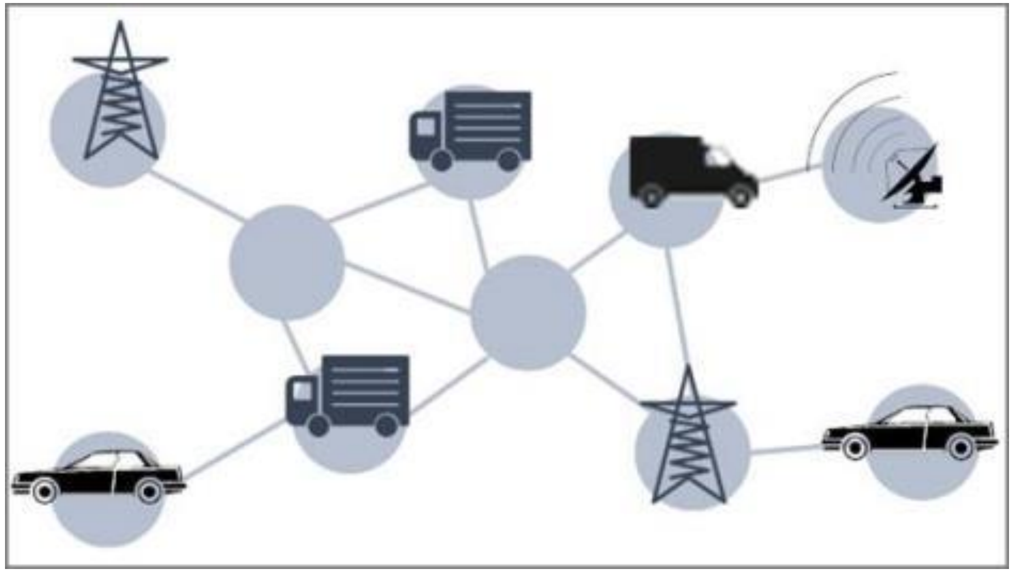
Example: Blockchain Initiatives by Toyota

Toyota Research Institute, which has been founded as an advanced R&D division in Silicon Valley, is examining Mobility Ecosystem jointly with MIT Media Lab using IoT and Blockchain in the following areas:

① **Data Sharing**: Using blockchain, enterprises and individuals share driving and test data ensuring the data ownership.

② **Car Sharing**: Using blockchain, car utilization data will be stored to effectively use the unused resources.

③ **Usage-based Insurance**: Storing driving data through sensor on automobile, insurance fee will be decided according to driving distance, driving characteristics, location, time and such.



Toyota seems to assume IoT and Blockchain are the essential part of future infrastructure for Mobility Ecosystem by:

✓ Connecting multiple sensors on automobile

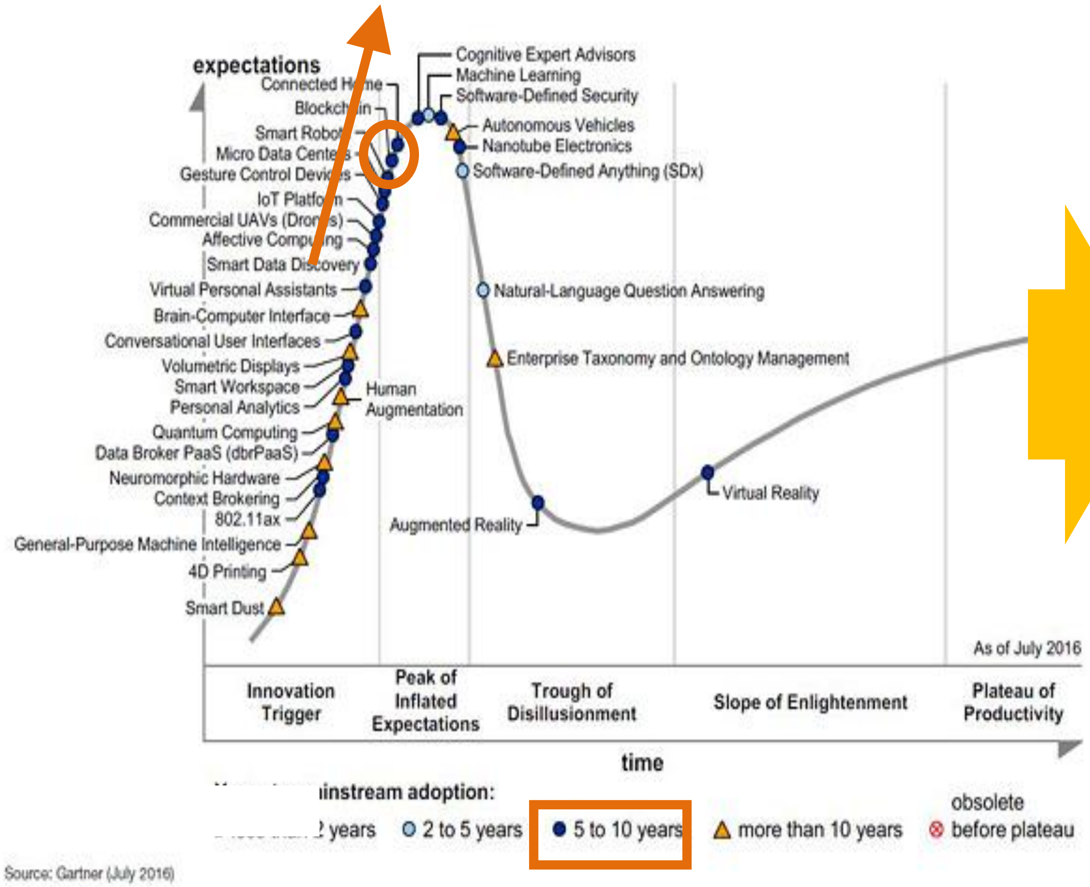
✓ Utilizing driving data securely to generate revenues

✓ Accessing available data at secure market place

Expectation on Blockchain Technology

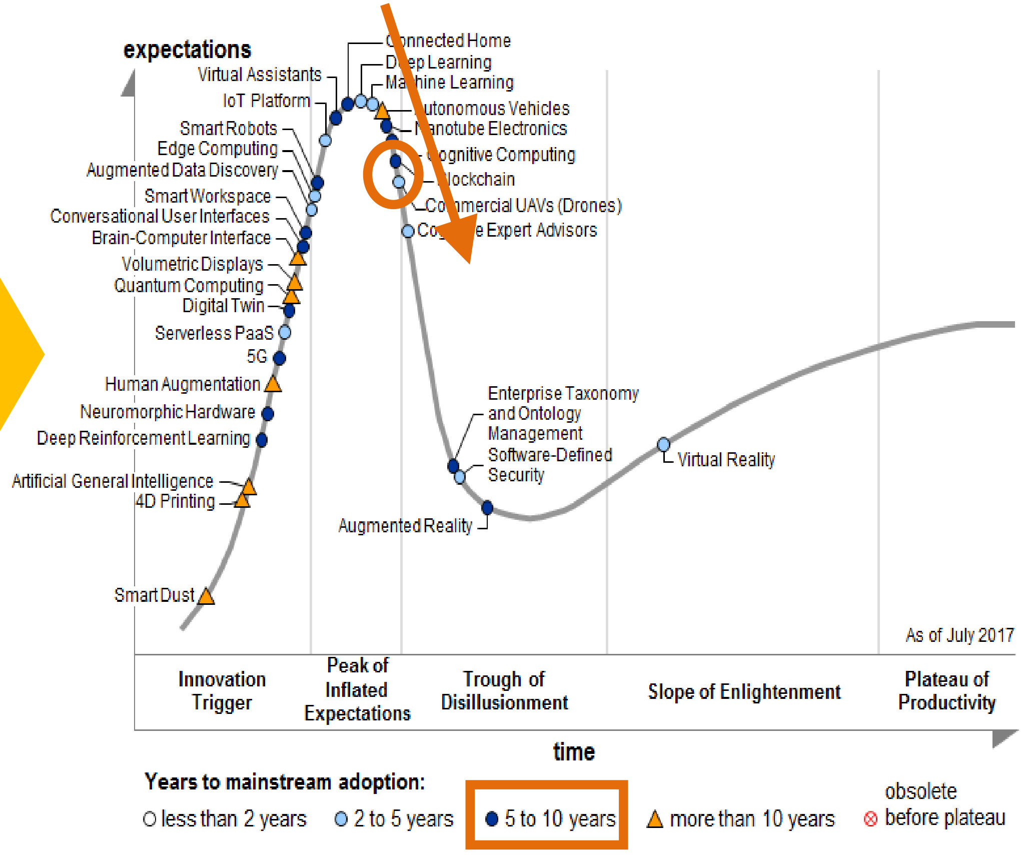
Gartner’s Hype Cycle for Emerging Technologies evaluates Blockchain technology as in a peak period of inflated expectations. However, the position changed between 2016 and 2017. In the hype cycle of 2017, blockchain is getting into downslope to the “Trough of Disillusionment.”

2016



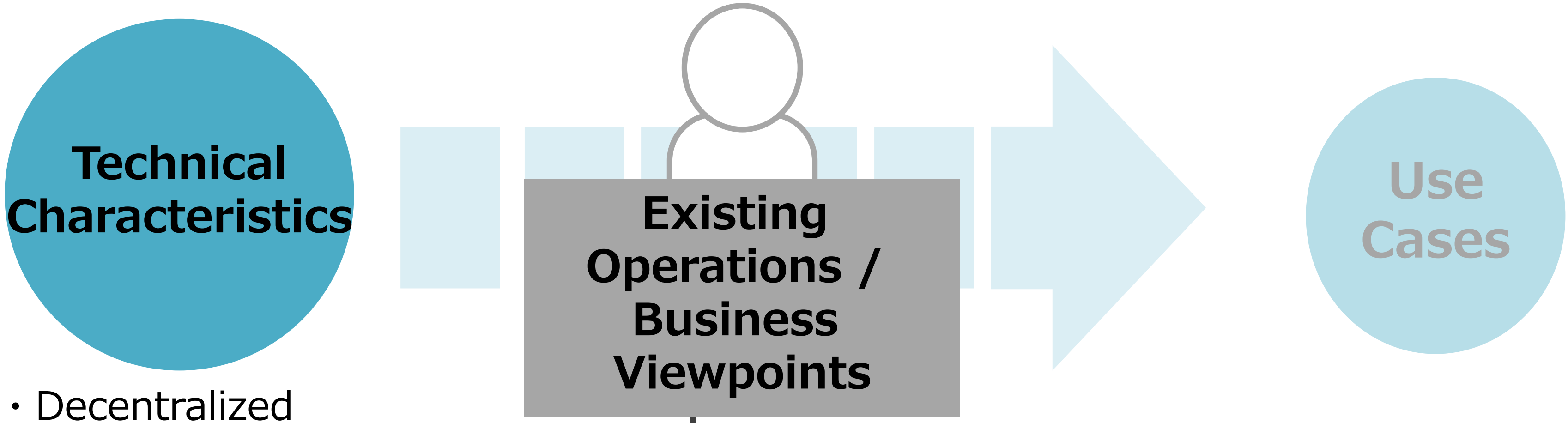
Source: Gartner (July 2016)

2017



Source: Gartner

Use Case Issues around Blockchain


Technical Characteristics
Existing Operations / Business Viewpoints
Use Cases

- Decentralized
- Tamper-Resistant
- Transparent

⋮

Concepts within Current Business

- Tend to focus on short-term ROI while low reality with long-term stories

“What is expected cost reduction?”

“What is the difference from ongoing plan?”

Concepts from Technical Elements

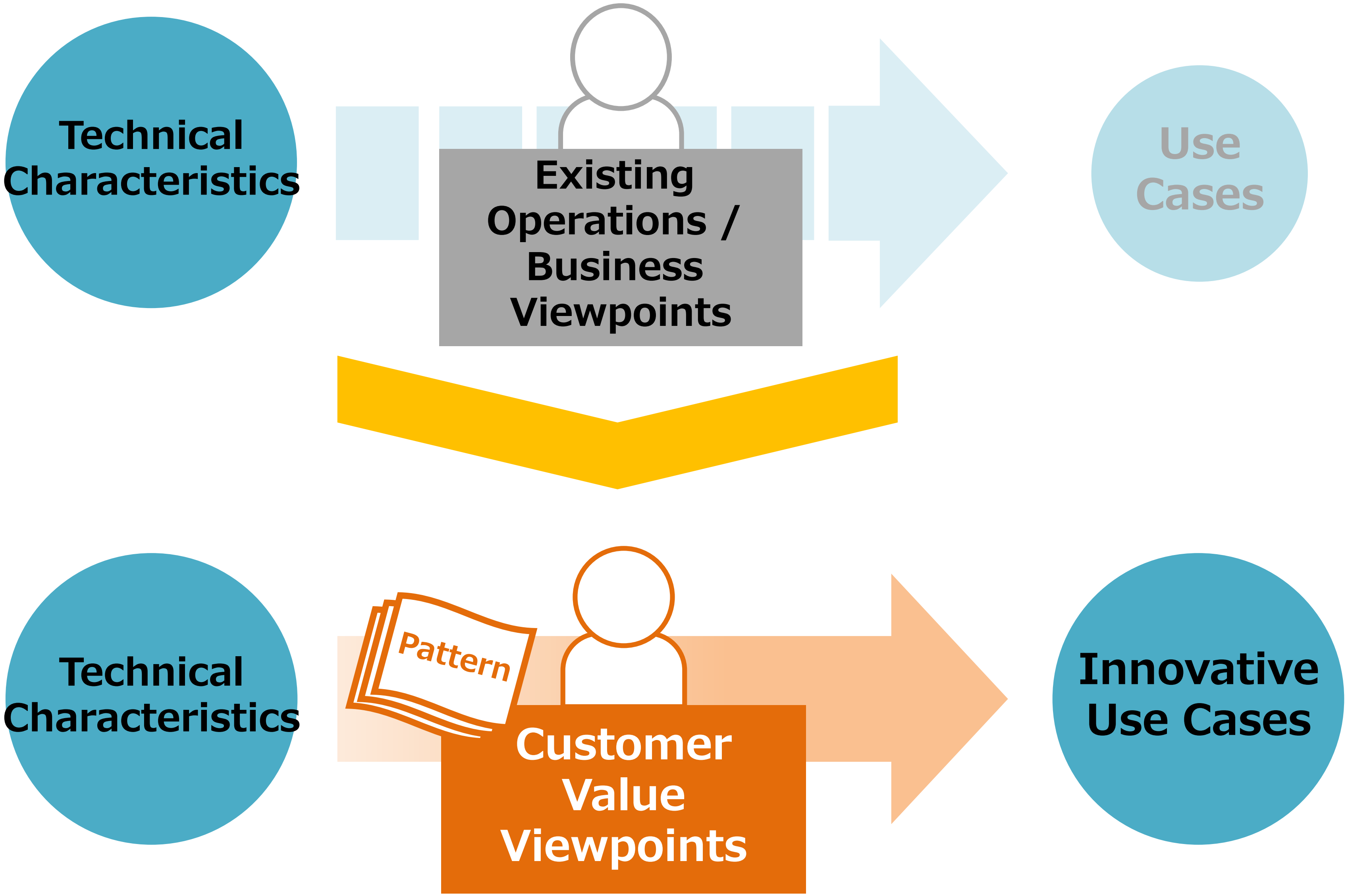
- Difficulty to conceive use cases fitting to blockchain and unsatisfactory outcome is waiting

“Is there any meaning to use blockchain?”

“What is the benefit compared with existing technology?”

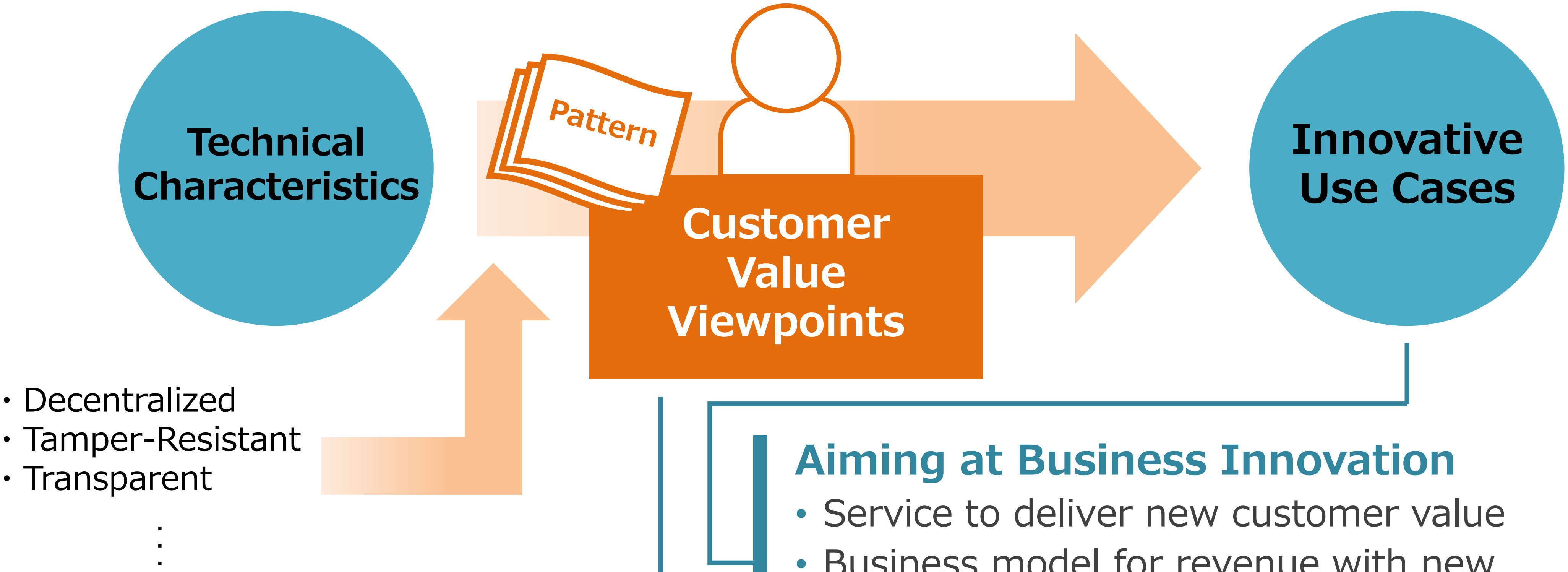
Change the Mindset: Use Cases to Utilize Blockchain

HITACHI
Inspire the Next



Technical Characteristics
Existing Operations / Business Viewpoints
Use Cases
Technical Characteristics
Pattern
Customer Value Viewpoints
Innovative Use Cases

Use Cases to Utilize Blockchain



- Decentralized
- Tamper-Resistant
- Transparent

⋮

Aiming at Business Innovation

- Service to deliver new customer value
- Business model for revenue with new stakeholders
- Business process to realize these.

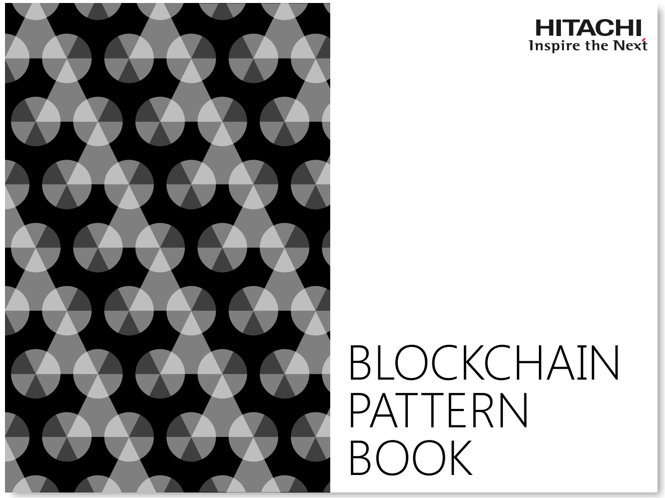
Concepts from Value Proposition Pattern

- Not from technical characteristics, but from typical pattern of value creation through blockchain

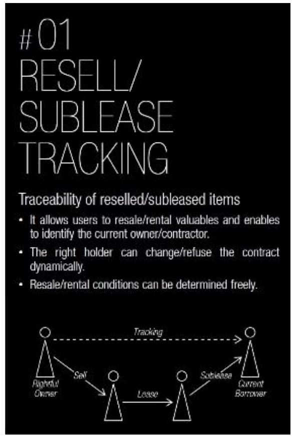
Blockchain Pattern Book

HITACHI
Inspire the Next

In order to deliver appropriate concepts using blockchain technology, Hitachi has published “Blockchain Pattern Book” to identify 11 patterns for benefits that are made possible by blockchain. We are trying to speed up the development of use cases in which societal challenges are resolved through cross-industry coordination.


HITACHI
Inspire the Next

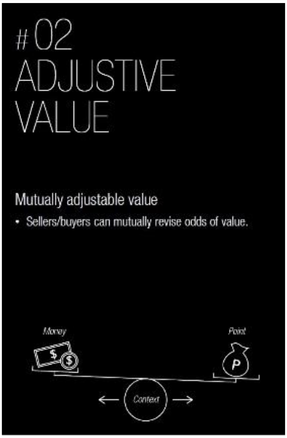
BLOCKCHAIN
PATTERN
BOOK


#01 RESELL/ SUBLEASE TRACKING

Traceability of reselled/subleased items

- It allows users to resale/rental valuables and enables to identify the current owner/contractor.
- The right holder can change/refuse the contract dynamically.
- Resale/rental conditions can be determined freely.

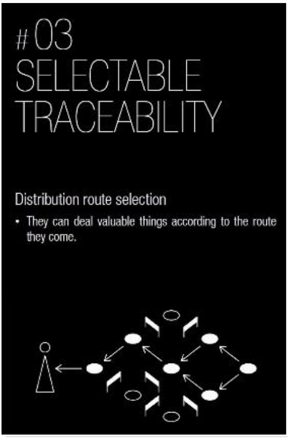
Tracking
Sell
Lease
Sublease
Rightful Owner
Current Borrower


#02 ADJUSTIVE VALUE

Mutually adjustable value

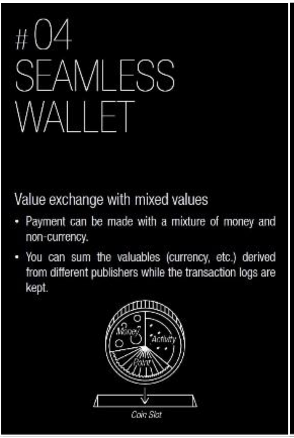
- Sellers/buyers can mutually revise odds of value.

Money
Point
Context


#03 SELECTABLE TRACEABILITY

Distribution route selection

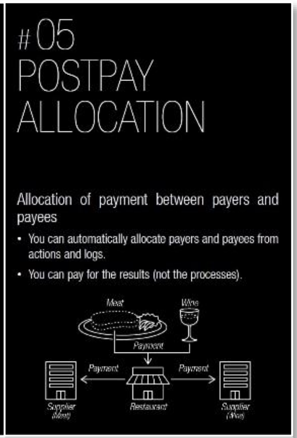
- They can deal valuable things according to the route they come.


#04 SEAMLESS WALLET

Value exchange with mixed values

- Payment can be made with a mixture of money and non-currency.
- You can sum the valuables (currency, etc.) derived from different publishers while the transaction logs are kept.

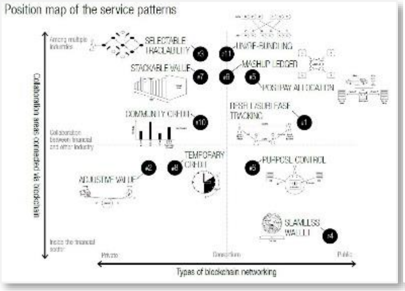
Money
Activity
Point
Coin Slot

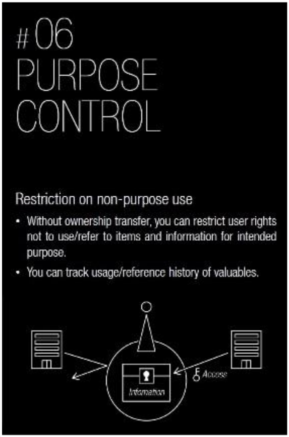

#05 POSTPAY ALLOCATION

Allocation of payment between payers and payees

- You can automatically allocate payers and payees from actions and logs.
- You can pay for the results (not the processes).

Meat
Wine
Payment
Payment
Payment
Supplier (Meat)
Restaurant
Supplier (Wine)

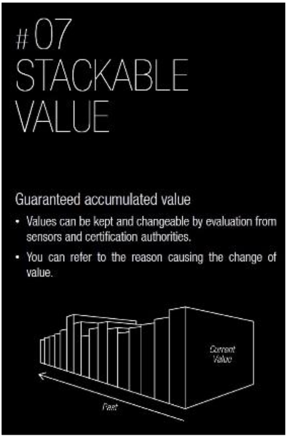

Position map of the service patterns


#06 PURPOSE CONTROL

Restriction on non-purpose use

- Without ownership transfer, you can restrict user rights not to use/refer to items and information for intended purpose.
- You can track usage/reference history of valuables.

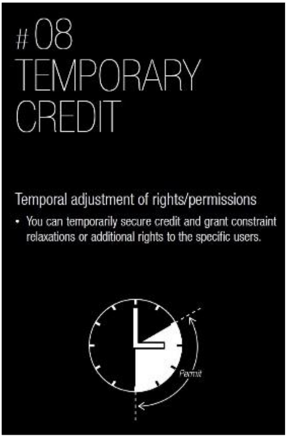
Information
Access


#07 STACKABLE VALUE

Guaranteed accumulated value

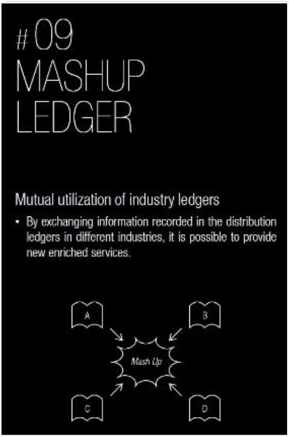
- Values can be kept and changeable by evaluation from sensors and certification authorities.
- You can refer to the reason causing the change of value.

Current Value
Past


#08 TEMPORARY CREDIT

Temporal adjustment of rights/permissions

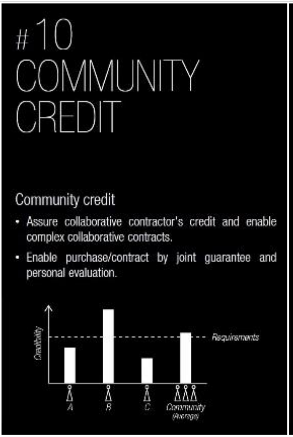
- You can temporarily secure credit and grant constraint relaxations or additional rights to the specific users.


#09 MASHUP LEDGER

Mutual utilization of industry ledgers

- By exchanging information recorded in the distribution ledgers in different industries, it is possible to provide new enriched services.

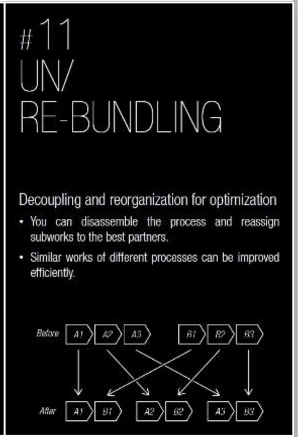
A
B
Mash Up
C
D


#10 COMMUNITY CREDIT

Community credit

- Assure collaborative contractor's credit and enable complex collaborative contracts.
- Enable purchase/contract by joint guarantee and personal evaluation.

Creditability
Requirements
A
B
C
Community (Average)


#11 UN/ RE-BUNDLING

Decoupling and reorganization for optimization

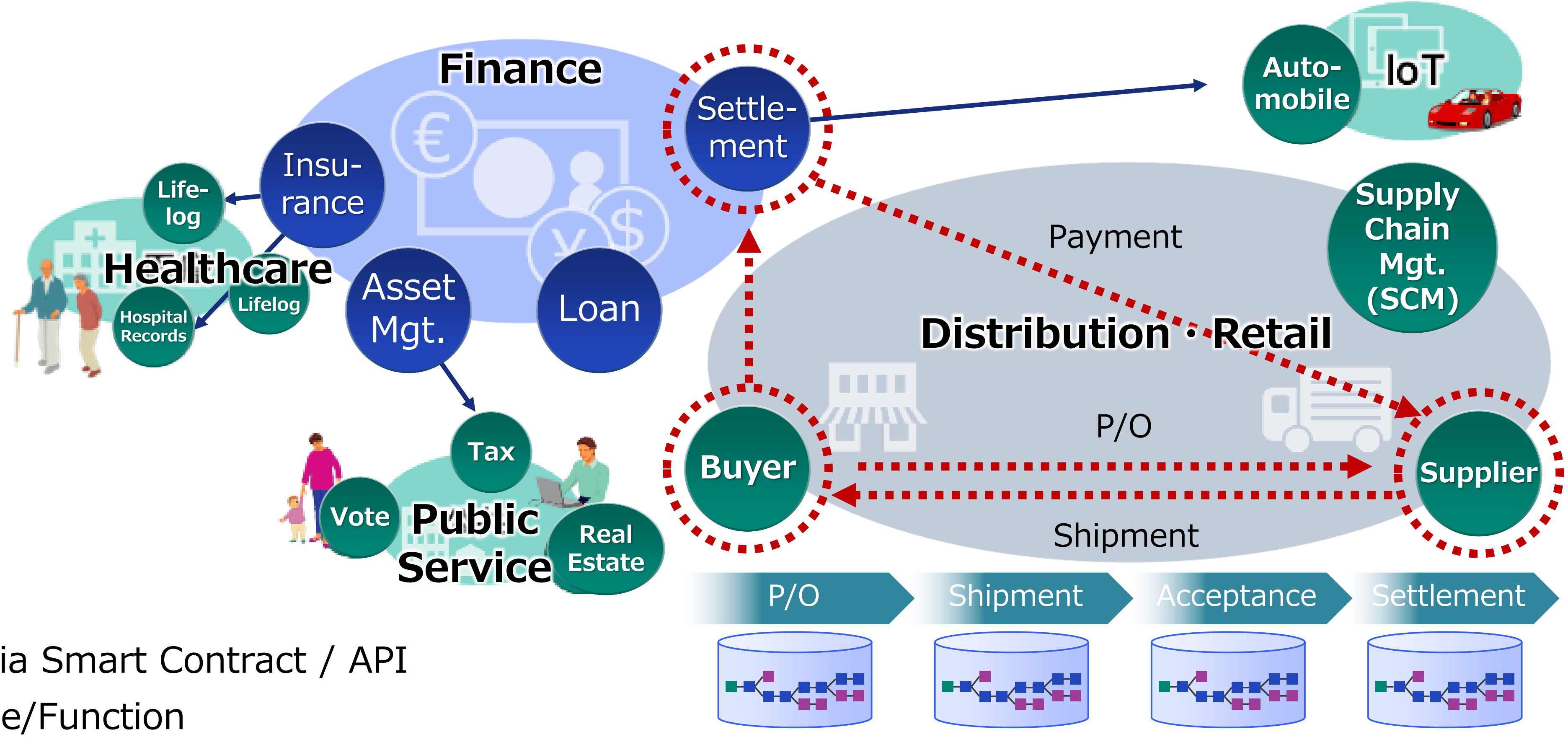
- You can disassemble the process and reassign subworks to the best partners.
- Similar works of different processes can be improved efficiently.

Before
A1
A2
A3
B1
B2
B3
After
A1
B1
A2
B2
A3
B3

How Industries Are Interconnected

Open API and **Blockchain**, especially its **Smart Contract** functionality, are supposed to bring new business opportunities by streamlining business processes and information sharing among industries with higher transparency.

Cross Industrial Services by Open API / Blockchain



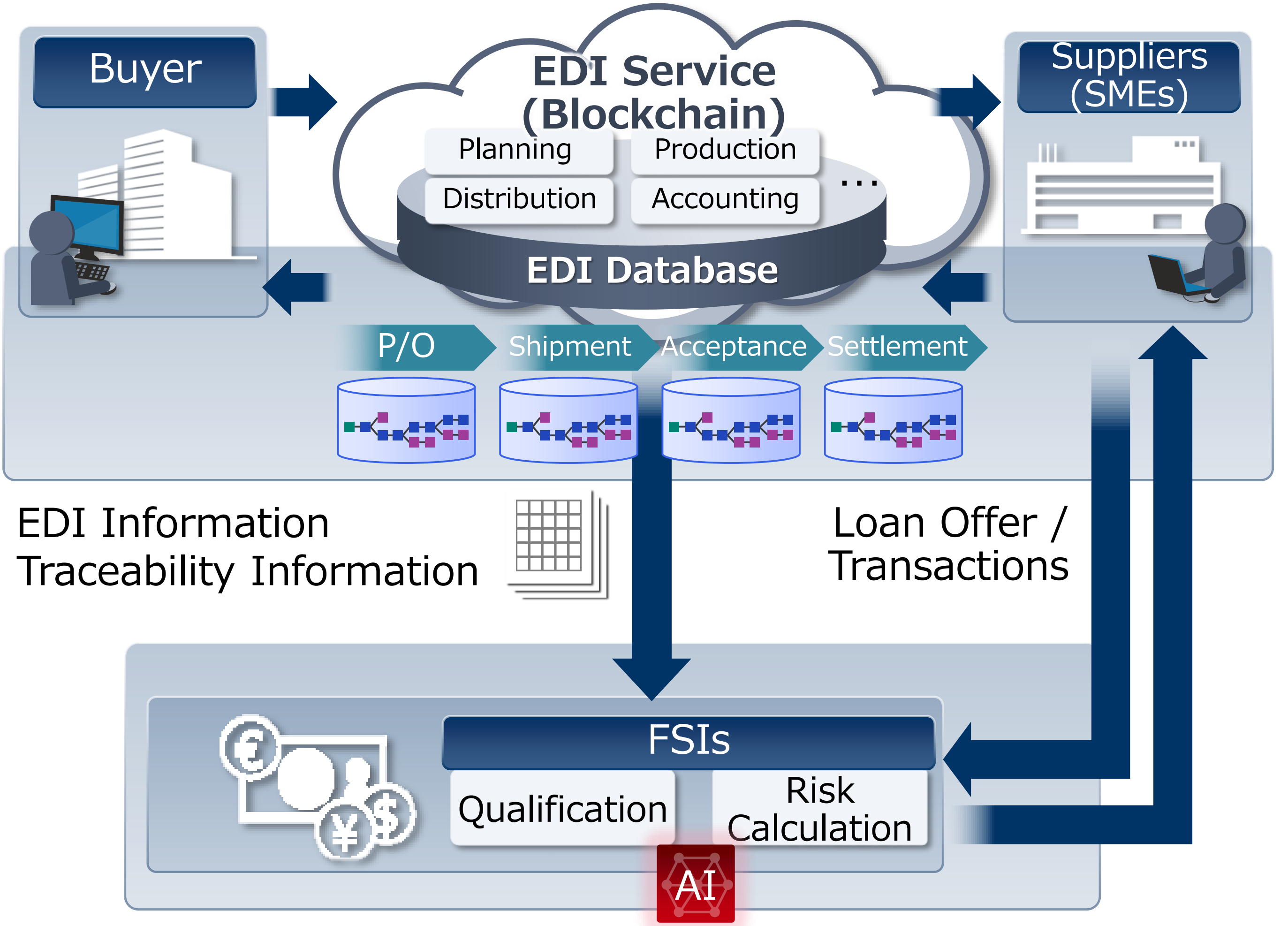
→ Link via Smart Contract / API

● Service/Function

New Services Using Blockchain and AI (Illustrative)

For instance, combining existing EDI(*) service with blockchain and AI, new service opportunities and functionality will be expanded.

Existing System + AI + Blockchain = New Services



Traceability Management

Transaction linked with EDI can be monitored with the latest status in the business stream using blockchain.

Transaction Lending

Based on the information on the supply chain, banks can offer loan along with AI based qualification in a flexible and dynamic manner.

EDI : Electronic Data Interchange

END

How We Can Expand the Utilization of Blockchain Technology: Security and Use Case Perspective

June 22, 2018

Toshiya Cho
Senior Evangelist / Managing Director
Financial Information Systems Sales Management Division
Hitachi, Ltd.

HITACHI

Inspire the Next

THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN

AUTOMOTIVE
LINUX SUMMIT

THE LINUX FOUNDATION