ETHTerakoya x Blockchain EXE

FUJITSU

shaping tomorrow with you

Proposal of Transaction Record Verification Technology through Blockchain Interoperability Considering Privacy

Takuya Sakamoto
Senior Researcher,
Data & Security Research Laboratory, Research Division, Fujitsu Limited

June 10, 2021

Self-introduction

- Takuya Sakamoto

- Company and Division
  - Research Division, Fujitsu Limited
  - Research Division, Fujitsu Limited
  - Blockchain Economy PJ

- Areas of Research
  - Distributed network security
    - Currently working on blockchain and privacy protection
    - Past studies: home network/home gateway/PC (content distribution/protection, IPTV), HTML5 (web app push notification, app protection), IoT (W3C Web of Things), etc.

Today's Topics

- Background
  - Fujitsu's blockchain projects
  - Privacy-enhancing technologies, especially zero-knowledge proofs

- Decentralized Identity and Privacy-Enhancing Technologies
  - What is decentralized identity?
  - Challenges: Protecting privacy when disclosing identity at verification
  - Technological solution: Secure-sharing verification technology using zero-knowledge proofs

- Blockchain Interoperability and Privacy-Enhancing Technologies
  - Digital trust and blockchain interoperability
  - Develop into the token economy
  - Challenges: Balancing privacy and utilizing transaction records in the token economy
  - Technological solution: Applying secure-sharing verification technology in transaction records

- Summary

Evolution and widespread application of blockchain technology

Expansion of application areas

Interoperability, data utilization, and autonomy

- Infrastructure that connects information, values, etc. without falsification
- Automation of social and organizational contracts and processes

Extended functionality (security, high speed)

- Cross-border transactions
- Use of sensitive personal data

Distributed ledger

- Technical verification/ experiments
- PoC

Digital assets (Cryptocurrency)

Digital asset management (Land registry, e-government, KYC, etc.)

Examples

Supply chain

Healthcare/Insurance One-stop service

Development of blockchain technology

Based on cryptocurrency, we are working on unique technology of blockchain interoperability among multiple entities as well as expanding application areas such as making use of data

Blockchain Activities at Fujitsu

- Working extensively on core technology and its standardization to applications

Application	Decentralized identity	Supply Chain / Token Economy	Cross-border transactions
	IDYX (IDentitY Xchange) (2019)	Rice Exchange (2019) Power trading	Mizuho Bank demonstration (2016) P2P money transfer (2017)
Core	Blockchain interoperability	Business logic Security Development environment	
	ConnectionChain (2017)		
	Standardization (Blockchain OSS)		
	Hyperledger Cactus (2020)	Hyperledger Fabric Hyperledger URSA (Crypto library)	

INATBA	Founding member of INATBA (Intl. Assoc. for Trusted Blockchain Applications)
Data sharing, traceability	Virtuora DX/VPX (2017) Chain Data Lineage (2018)
Enhanced security	Smart contract verification (2018) TaaS (Trust as a Service) (2020)
Scalability	Higher transactions per second (2017)
Contribution to OSS	Founding/premier member of Hyperledger Technical Steering Committee

Introducing research on decentralized identity and blockchain interoperability from the privacy perspective

Privacy-Enhancing Technologies is Hot

- Enhancing privacy is an important issue for utilizing data

- Differential privacy
  - Anonymize data by adding noise (a benchmark for that)
- Federated analysis
  - Analyze received computation results without aggregating distributed data
- Homomorphic encryption
  - Cryptography that allows the user to compute on encrypted data
- Secret sharing & MPC (Secure multiparty computation)
  - Secret sharing: Data is split and cannot be reconstructed unless the sufficient number of shares are combined together
  - MPC: Divides the computation process across multiple servers (MPC) and aggregate the results
- **Zero-knowledge proof**
  - A technique that allows the user to prove specific information without revealing anything

A privacy-enhancing technology suitable for individual data such as identity and transaction records

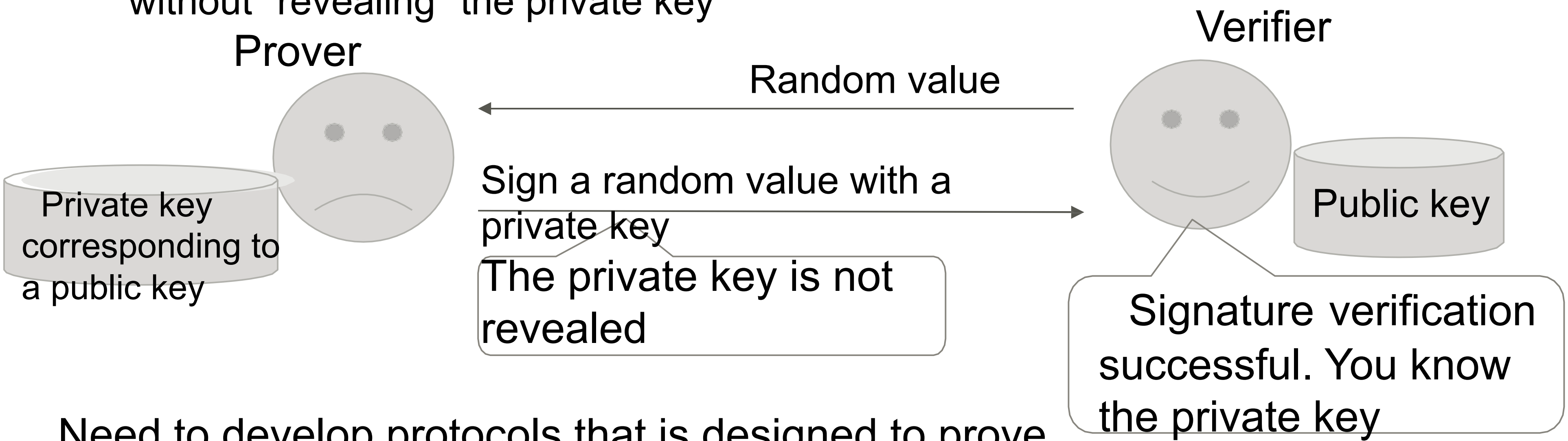
Reference: World Economic Forum 2019
https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-next-generation-data-sharinging-financial-services.pdf

Overview of zero-knowledge proof

- The technique that allows the party to prove the information without revealing it. How does it work?

  → Prove by performing computation that cannot be done without knowing that information

  Example: Proving that you know a private key corresponding to a public key without "revealing" the private key


Prover
Verifier
Random value
Sign a random value with a private key
Private key corresponding to a public key
Public key
The private key is not revealed
Signature verification successful. You know the private key

Need to develop protocols that is designed to prove different content accordingly

Protocols that can prove various content idemix, zkSNARKs, Bulletproof, etc.

Research and development of privacy-enhancing technologies with zero-knowledge proofs in decentralized identity and blockchain interoperability

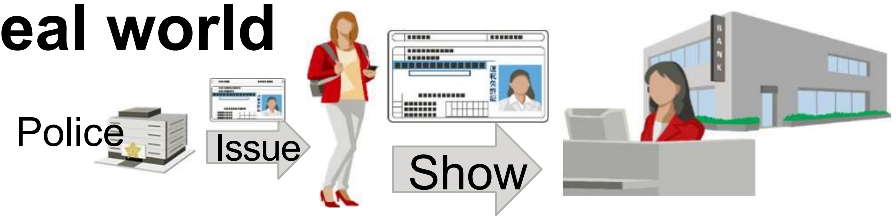
FUJITSU

Decentralized Identity and Privacy-Enhancing Technologies

The need for decentralized identity

- Self-sovereign identity
  - Each individuals control own identity (attributes) on the Internet

In real world

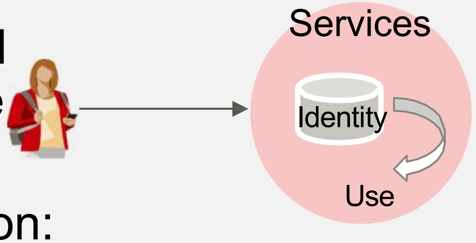


Identity = ID + attributes

Physical certificates are used freely
Attributes such as the name, age, and credit are verified

Virtual

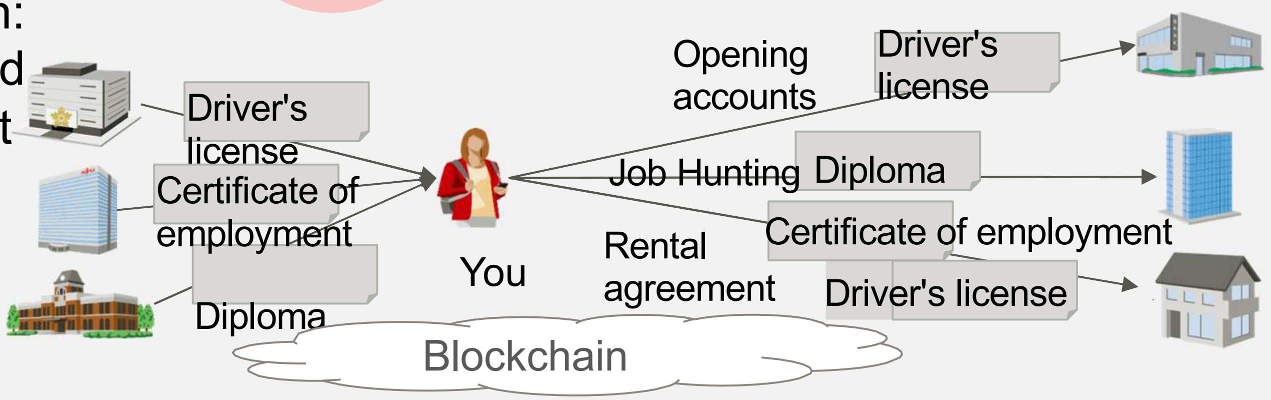
Traditional:
Centralized manageme



The user owns and controls his/her own identity issued by third parties

From now on:
Decentralized management

Issuer



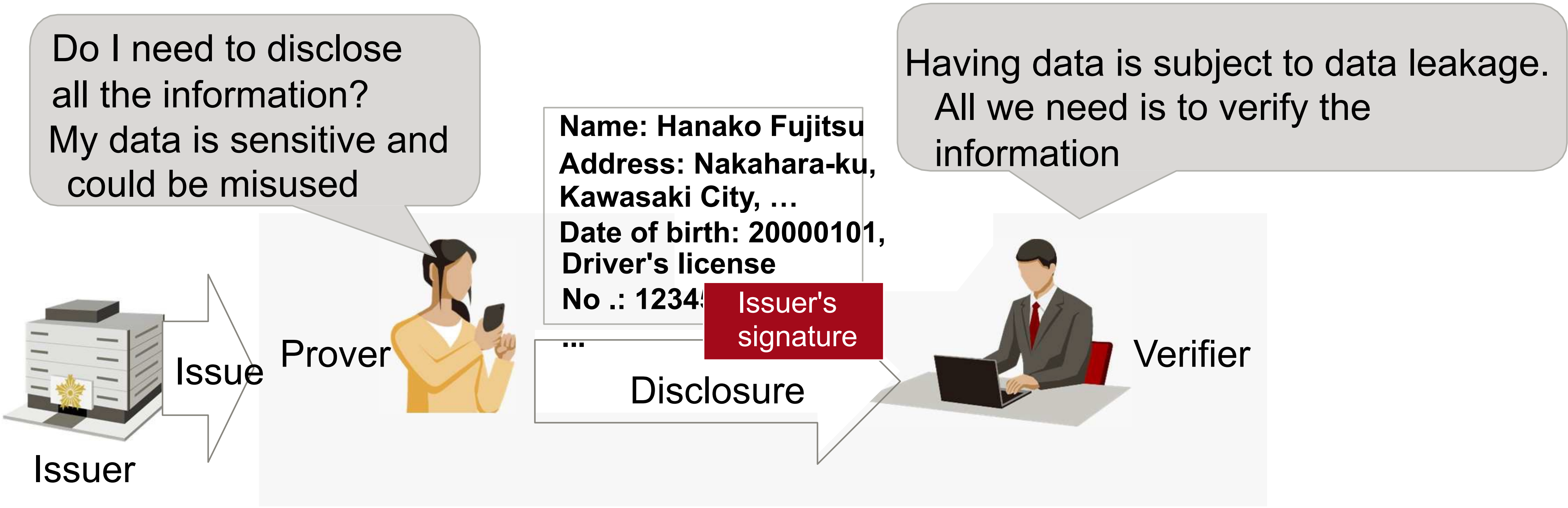
User

Controlling the user's own identity results in gaining distributed trust

Challenges in Identity Disclosure

- What is the purpose of disclosing the identity?

→The other party needs to verify required information to gain the trust



Do I need to disclose all the information?
My data is sensitive and could be misused

Having data is subject to data leakage.
All we need is to verify the information

Name: Hanako Fujitsu
Address: Nakahara-ku, Kawasaki City, …
Date of birth: 20000101,
Driver's license
No .: 1234
…

Issuer's signature

Issuer

Issue

Prover

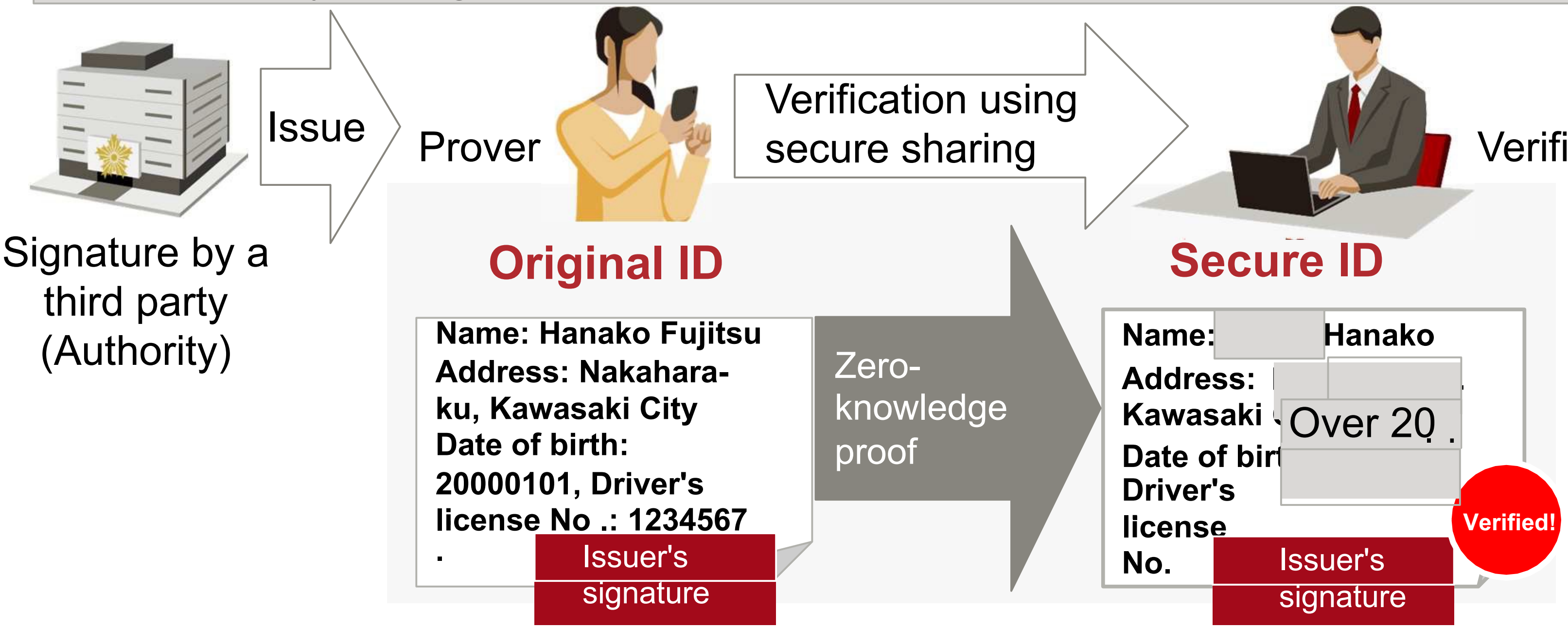
Disclosure

Verifier

Considering privacy, the prover wants to share only the necessary information
However, the signature method requires disclosing all the information to be verified

Proving the identity using secure-sharing verification technology

Enhance zero-knowledge proof technology to achieve both privacy and authenticity of digital IDs



Signature by a third party (Authority)

Issue

Prover

Verification using secure sharing

Verifier

Original ID

Name: Hanako Fujitsu
Address: Nakahara-ku, Kawasaki City
Date of birth: 20000101, Driver's license No .: 1234567 .

Issuer's signature

Zero-knowledge proof

Secure ID

Name: Hanako
Address:
Kawasaki
Over 20
Date of birt
Driver's license No.

Issuer's signature

Verified!

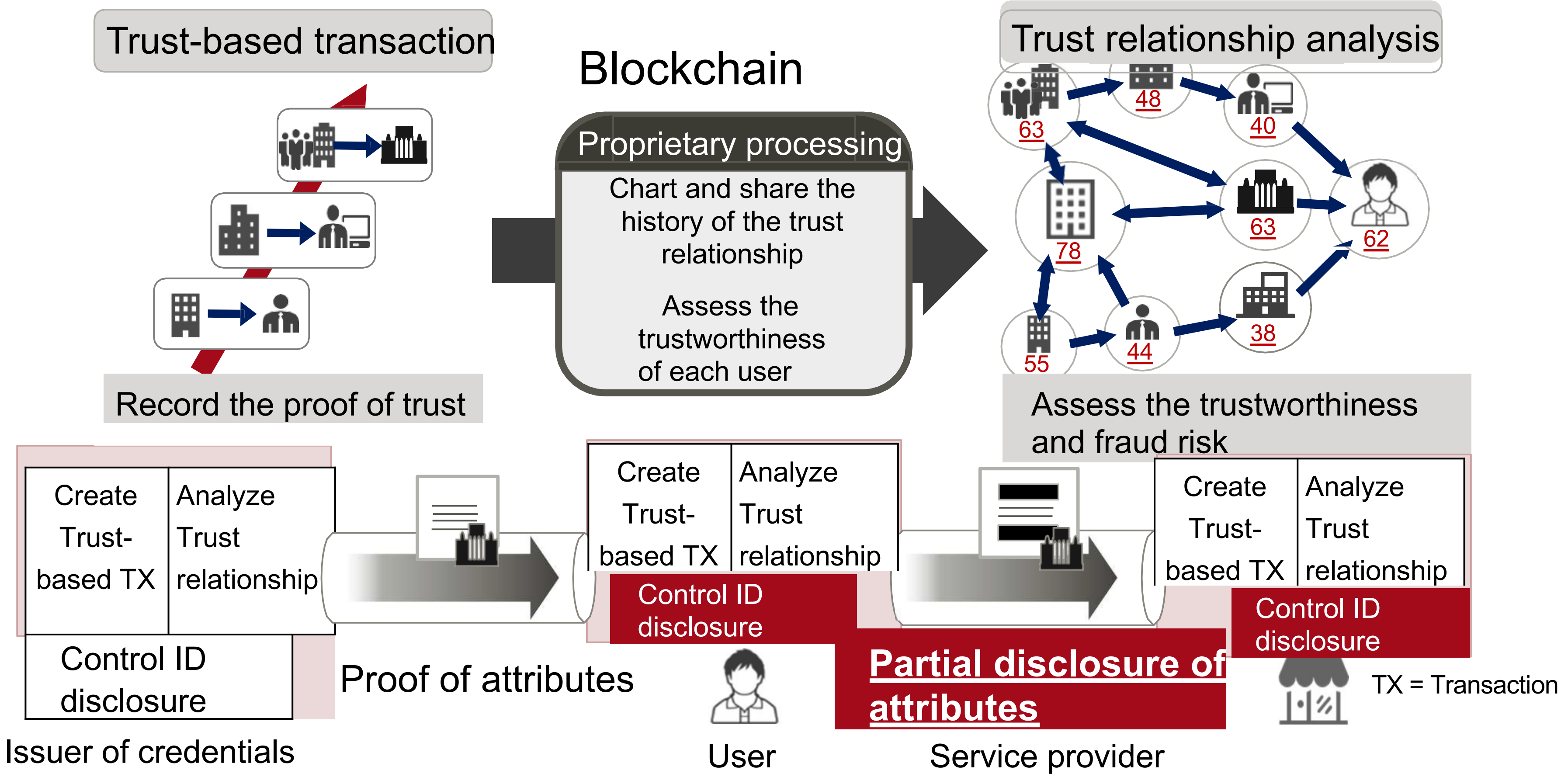
Key technology: The same signature can be used to prove the veracity of the partially disclosed information even if the part of attribute values remains concealed (Existing technology allows concealing by attribute)

* Using the CL signature scheme, which allows proving without disclosing the signature itself

Developing the protocol to prove the veracity of the partially disclosed information without disclosing precise attribute values

Digital identity exchange technology, IDYX

- Allows a party to assess the trustworthiness of the other party online and exchange identities
  - Each user is assessed for each transaction, which is recorded in the blockchain; the trust score is calculated based on the reputation among users
  - Users only disclose the part of personal information to prove the trustworthiness and can make transactions



Trust-based transaction

Record the proof of trust

Blockchain

Proprietary processing

Chart and share the history of the trust relationship

Assess the trustworthiness of each user

Trust relationship analysis

Assess the trustworthiness and fraud risk

Create Trust-based TX	Analyze Trust relationship
Control ID disclosure	

Issuer of credentials

Proof of attributes

Create Trust-based TX	Analyze Trust relationship
Control ID disclosure	

User

Partial disclosure of attributes

Create Trust-based TX	Analyze Trust relationship
Control ID disclosure	

Service provider

TX = Transaction

Blockchain Interoperability and Privacy-Enhancing Technologies

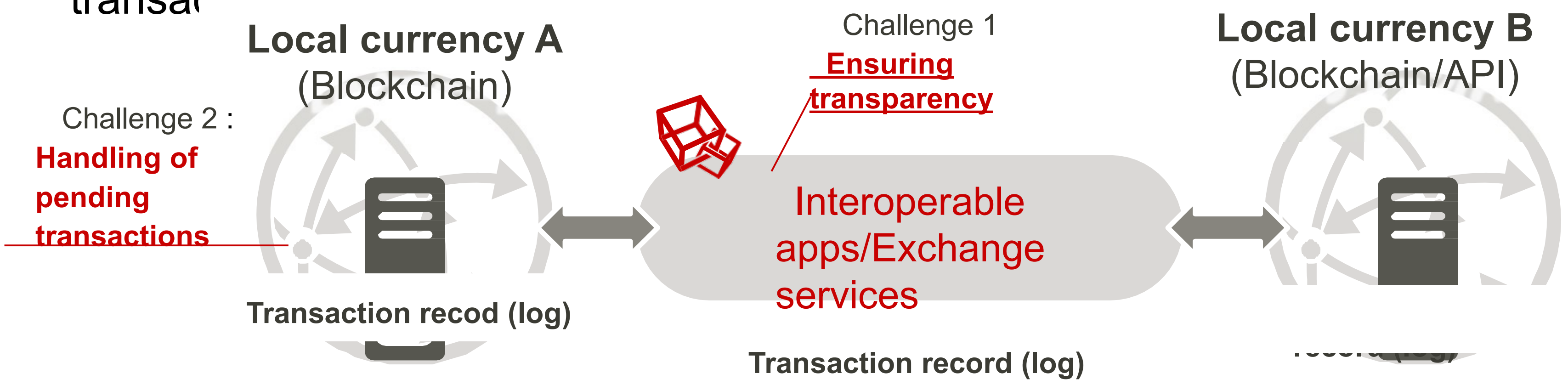
Aiming to Achieve Digital Trust

New demand for blockchain

- Past: Bitcoin only -> Current: Altcoins; the existence of many cryptocurrencies (digital assets)
- Growing demand for "connecting the value of data" such as exchange between different cryptocurrencies, inter-chain transactions, and data communication between blockchains and existing systems

Challenges in blockchain interoperability

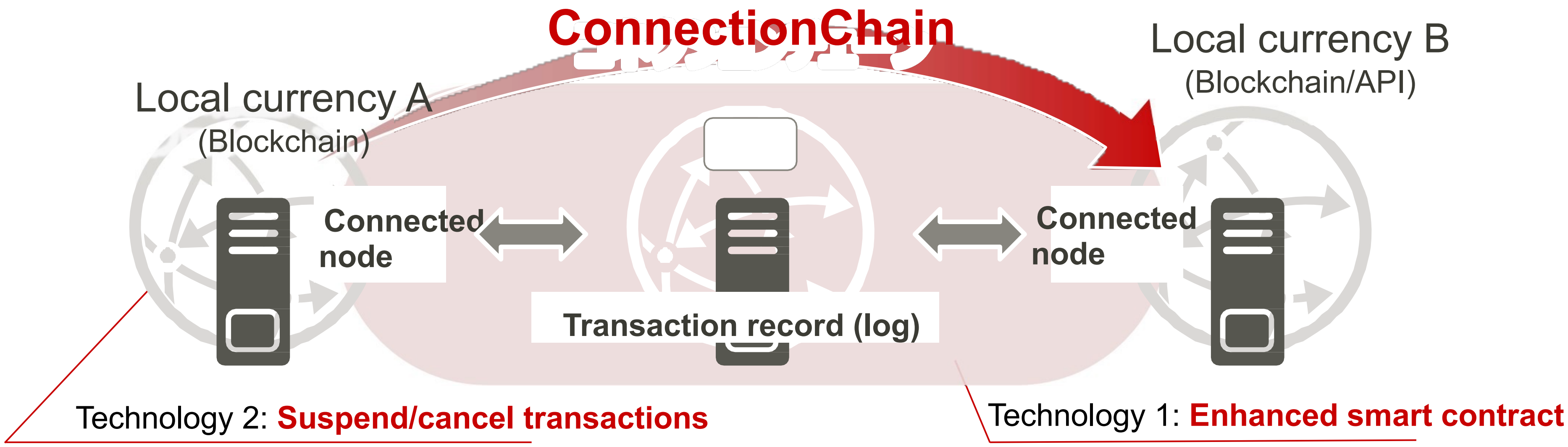
- Transparency: There were cases where fraudulent cryptocurrency exchanges caused damage of tens of billions of yen
- Integrity of transactions among blockchains (blockchain cannot reverse transa



In the era of digital trust, transparency is essential in connecting diverse systems

ConnectionChain

- ConnectionChain = Connecting "with" blockchains
- Allows uses to exchange values between different blockchains
- Enhancing smart contract to ensure transparency of transactions of currency exchange, etc. in various blockchains and APIs



Technology 2: **Suspend/cancel transactions**

Manage escrow accounts and roll back if the transaction failed halfway through

Technology 1: **Enhanced smart contract**

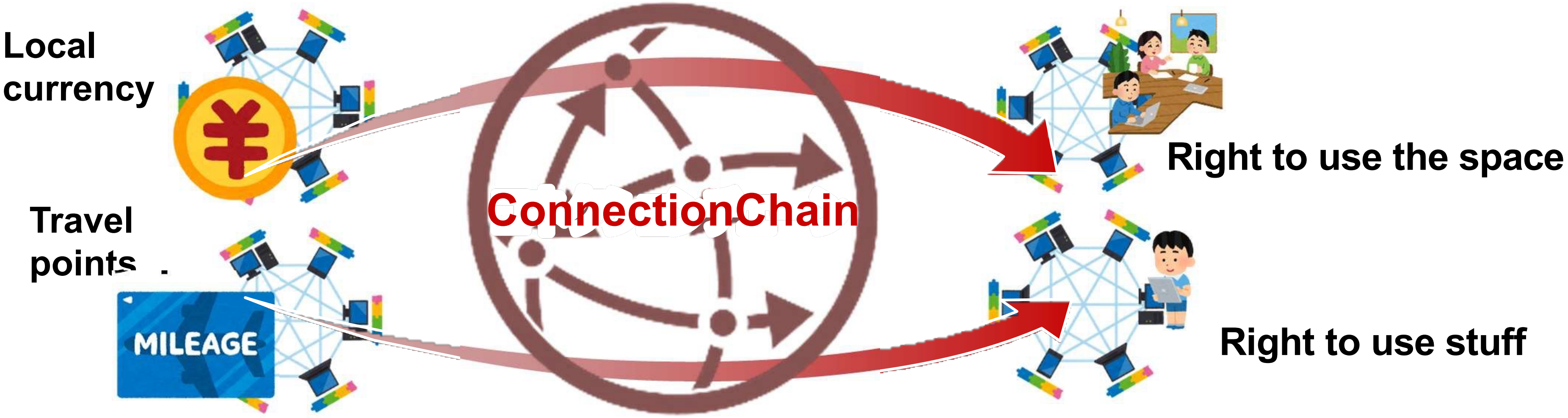
Ensure transparency of inter-chain transaction history

Replacing transactions handled by human with blockchain and ensuring transparency across the systems

Token Economy and Privacy

- According to Gartner, the token economy will be commercialized around 2023
- The tokenization market is estimated to grow to US$ 4.8 billion by 2025*1
- Existing services in the token economy for customer reviews of products and restaurants
- New sharing business models: e.g., remote working at a karaoke room, carrying goods (masks, etc.) in airplanes seats

* 1: https://www.marketsandmarkets.com/PressReleases/tokenization.asp

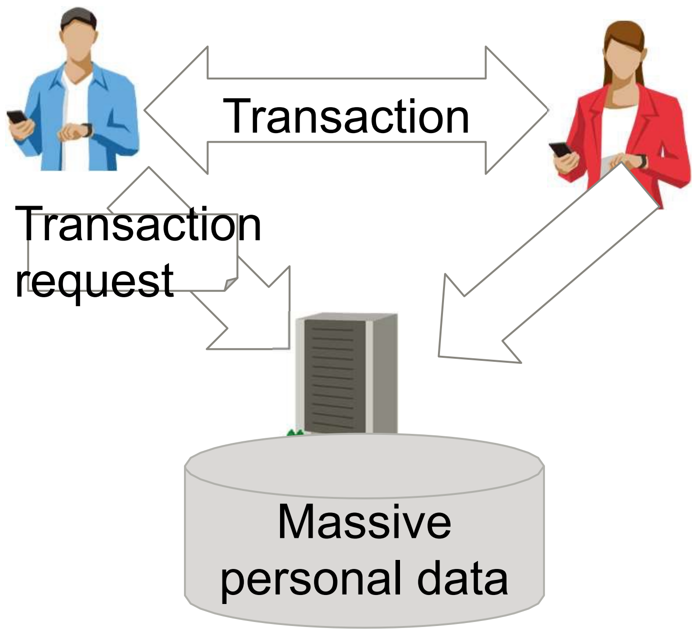


ConnectionChain aims to connect token economies

Personal data such as time and stuff used will be stored as transaction records

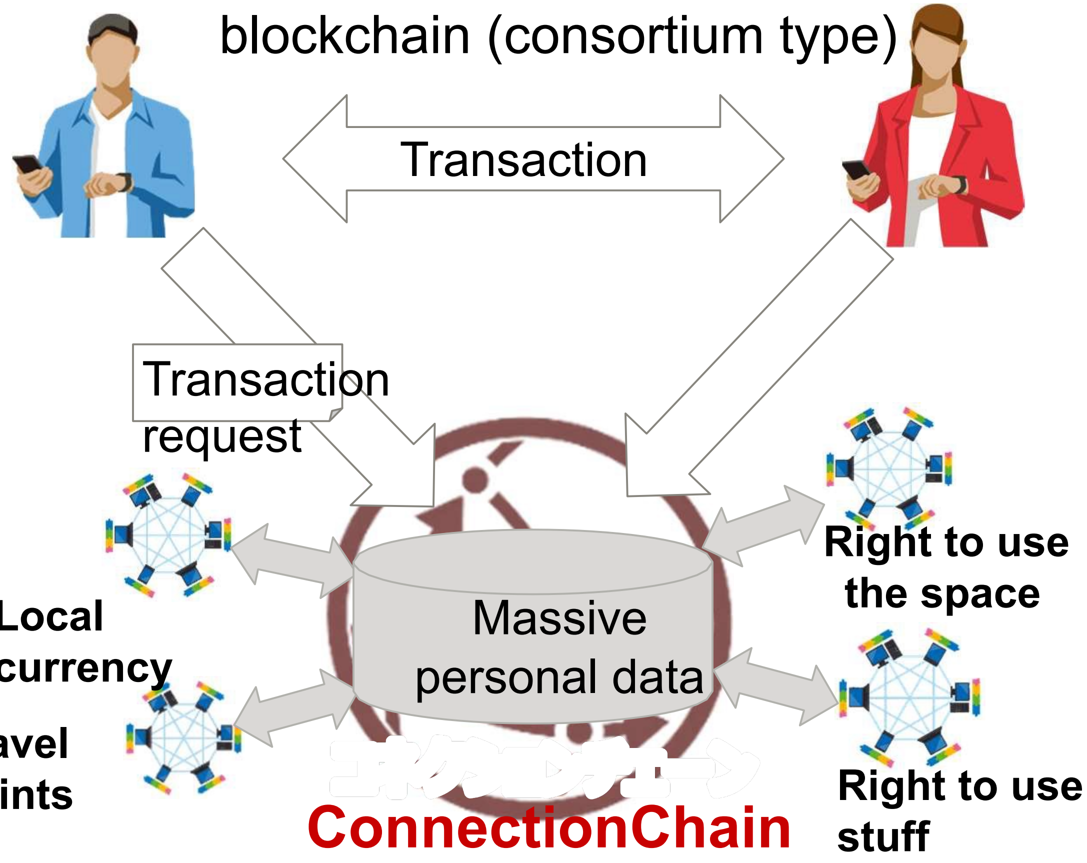
Utilizing ConnectionChain and transaction data

Controlled by a centralized platformer



Transparency: Low
Use of data:
Platformer acceptable, others depend on the platformer

Decentralized platform with blockchain (consortium type)

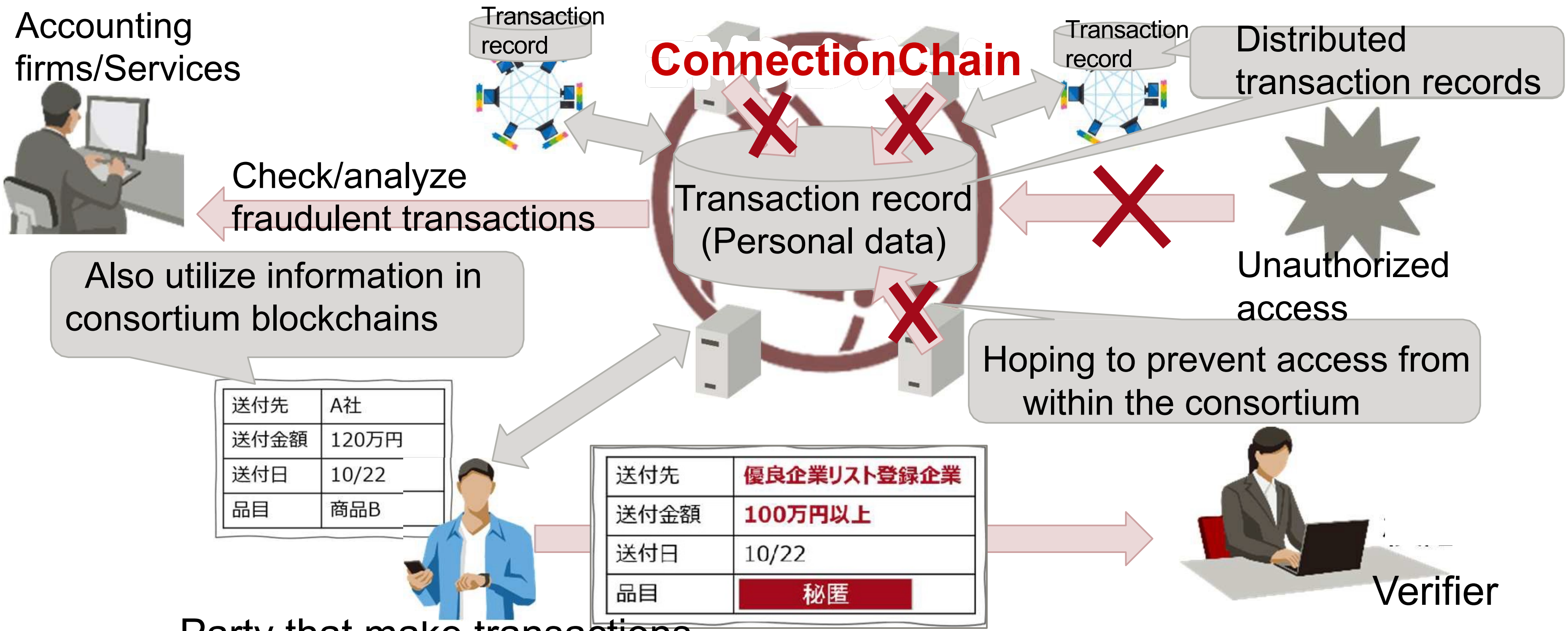


Transparency: High
Use of data:

When handling personal data in the decentralized platform, we need to consider how to utilize data and address leakage risk

Utilizing data and its challenges

- Accounting firms: Investigation of fraudulent transactions such as money laundering
(Services: Recommendations based on transaction history, etc.)
- **Parties that make transactions** Keeping proof of transaction history and the details



Accounting firms/Services

Transaction record

ConnectionChain

Transaction record

Distributed transaction records

Check/analyze fraudulent transactions

Transaction record (Personal data)

Also utilize information in consortium blockchains

Unauthorized access

Hoping to prevent access from within the consortium

送付先	A社
送付金額	120万円
送付日	10/22
品目	商品B

送付先	優良企業リスト登録企業
送付金額	100万円以上
送付日	10/22
品目	秘匿

Verifier

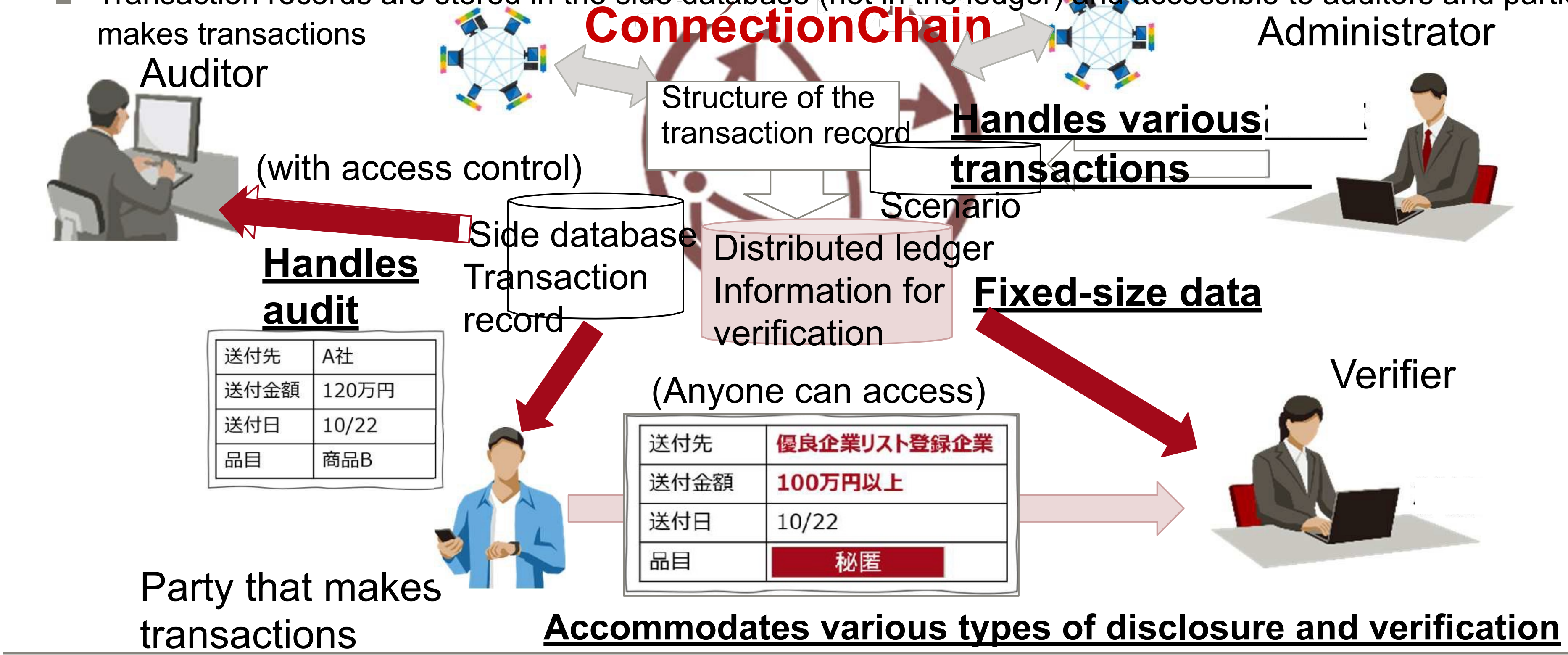
Party that make transactions

Disclose and prove (part of) transaction records to various parties

Disclosure of transaction records of consortium blockchains -> Privacy protection depends on the consortium blockchain -> Accessible to consortium members -> Exposure to risk of data leakage to competitors (in business transactions)

Developing secure-sharing verification technology of transaction data

- Forming transaction records Transaction scenario
  - Collect information from consortium blockchains based on the scenario and form records Increased number of items in the transaction record
- Proof of transaction records: Zero-knowledge proofs
  - Information for verification is stored in the distributed ledger, and the proving items in the transaction record can be concealed or disclosed
  - Key technology The amount of data for verification in the distributed ledger is independent of the number of items.
- Access control of transaction data * Same as private data collection in Hyperledger Fabric
  - Transaction records are stored in the side database (not in the ledger) and accessible to auditors and parties that makes transactions


ConnectionChain
Administrator
Auditor
Structure of the transaction record
Handles various transactions
(with access control)
Scenario
Side database Transaction record
Distributed ledger Information for verification
Handles audit
Fixed-size data
(Anyone can access)
Verifier
Party that makes transactions
Accommodates various types of disclosure and verification

送付先	A社
送付金額	120万円
送付日	10/22
品目	商品B

送付先	優良企業リスト登録企業
送付金額	100万円以上
送付日	10/22
品目	秘匿

Summary

- Fujitsu has developed blockchain technology to expand its application areas. Today, I have introduced two of these cases with privacy in mind.

- Decentralized identity
  - When disclosing the identity, it is important to consider privacy when proving the information
  - Challenges: Disclosing and proving the information according to need of the other party
  - Solution: Developed a zero-knowledge proof that allows the prover to choose various ways to conceal and disclose information
  - Key point Even if some of attribute values remain concealed, the same signature can be used to prove the veracity of disclosed information

- Blockchain interoperability
  - In order to implement a token economy, it is important to balance the transparency of transaction records and the protection of privacy
  - Challenges: Disclosing and proving necessary transaction records to the other party while ensuring transparency through the distributed ledger
  - Solution: Developed a zero-knowledge proof in which the information for verification is managed in the ledger and used to verify each item in the transaction record
  - Key point Fixed-length data can be used to verify transaction records that have an increased number of items due to consortium blockchains

FUJITSU

shaping tomorrow with you