ETHTerakoya x Blockchain EXE

FUJITSU
shaping tomorrow with you

プライバシーを考慮したブロックチェーン連携 による取引記録証明技術の提案

2021年6月10日

富士通株式会社 研究本部 データ&セキュリティ研究所 シニアリサーチャー
坂本拓也

自己紹介

FUJITSU

- 坂本拓也 (さかもとたくや)

- 所属
  - 富士通株式会社 研究本部
  - データ&セキュリティ研究所
  - ブロックチェーンエコノミーPJ

- 研究分野
  - 分散ネットワークセキュリティ
    - 現在は、ブロックチェーンとプライバシー保護
    - 過去には、ホームネットワーク/ホームゲートウェイ/PC (コンテンツ流通/保護、IPTV)、HTML5 (Webアプリプッシュ配信/保護)、IoT (W3C Web of Things) など

発表内容

FUJITSU

- 背景
  - 富士通のブロックチェーンへの取り組み
  - プライバシー強化技術、特にゼロ知識証明
- 分散型アイデンティティーとプライバシー強化技術
  - 分散型アイデンティティーとは
  - 課題: アイデンティティー開示証明時のプライバシー
  - 解決技術: ゼロ知識証明による秘匿開示証明技術
- ブロックチェーン連携とプライバシー強化技術
  - デジタルトラストとブロックチェーン連携
  - トークンエコノミーへの展開
  - 課題: トークンエコノミーでの取引記録活用とプライバシーの両立
  - 解決技術: 秘匿開示証明技術の取引記録活用への適用
- まとめ

ブロックチェーンの技術の進化と適用拡大

FUJITSU

連携、データ利活用、自律化

- 情報や価値を改ざんなくつなげる基盤
- 社会・組織の契約やプロセスを自動化

応用領域の拡大 ＋

機能拡張（セキュリティ、高速性）

- クロスボーダー取引
- 機密・パーソナルデータの活用

分散台帳

- 技術検証・実験
- PoC

暗号資産
(仮想通貨)

デジタルアセット管理
（土地台帳、電子政府、
KYCなど）

例 サプライチェーン

医療・保険
ワンストップサービス

ブロックチェーン技術の進化

仮想通貨を起点とし、ブロックチェーンを使った独自技術で複数事業者連携と、データ利活用などへ適用分野の拡大に取り組んでいる

富士通のブロックチェーンのアクティビティ

FUJITSU

- 基盤技術とその標準化から応用まで広く取り組み

応用	分散型 アイデンティティー	サプライチェーン / トークンエコノミ	クロスボーダー 取引	
	IDYX (IDentitY eXchange) (2019)	Rice Exchange (2019) 電力トレード	みずほ銀行実証 (2016) P2P送金(2017)	
基盤	ブロックチェーン 連携	ビジネスロジック セキュリティ 開発環境		
	ConnectionChain (2017)			
	標準化 (Blockchain OSS)			
	Hyperledger Cactus (2020)	Hyperledger Fabric Hyperledger URSA (Crypto library)		

INATBA
INATBA(Intl. Assoc. for Trusted Blockchain Applications)創設メンバー
データ共有、トレーサビリティ
Virtuora DX/VPX (2017) Chain Data Lineage (2018)
セキュリティ強化
スマートコントラクト検証 (2018) TaaS (Trust as a Service) (2020)
スケーラビリティ
トランザクション高速化(2017)
OSS 貢献
Hyperledger 創設・プレミアメンバー 技術ステアリング委員

分散型アイデンティティーとブロックチェーン連携について プライバシーの観点での研究について紹介

注目のプライバシー強化技術

FUJITSU

- データ利活用にはプライバシー強化が重要な課題

- 差分プライバシー(Differential Privacy)
  - データにノイズをかけて匿名化 (そのための指標)
- 統合分析(Federated Analysis)
  - 分散するデータを集約せずに、計算結果を受け取って分析
- 準同型暗号(Homomorphic Encryption)
  - データを暗号化したまま計算可能な暗号
- 秘密分散+MPC (Secure Multiparty Computation)
  - 秘密分散: 一定数以上の断片が揃わないと復号できない状態にデータ分割
  - MPC: 複数のサーバーで分割されたデータを計算(MPC)して結果を集約
- **ゼロ知識証明(Zero Knowledge Proof)**
  - 証明したい情報を明かすことなく、その情報に関することを証明する手法

アイデンティティーや取引記録など個々のデータのプライバシー強化に適した技術

世界経済フォーラム2019より
https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-next-generation-data-sharinging-financial-services.pdf

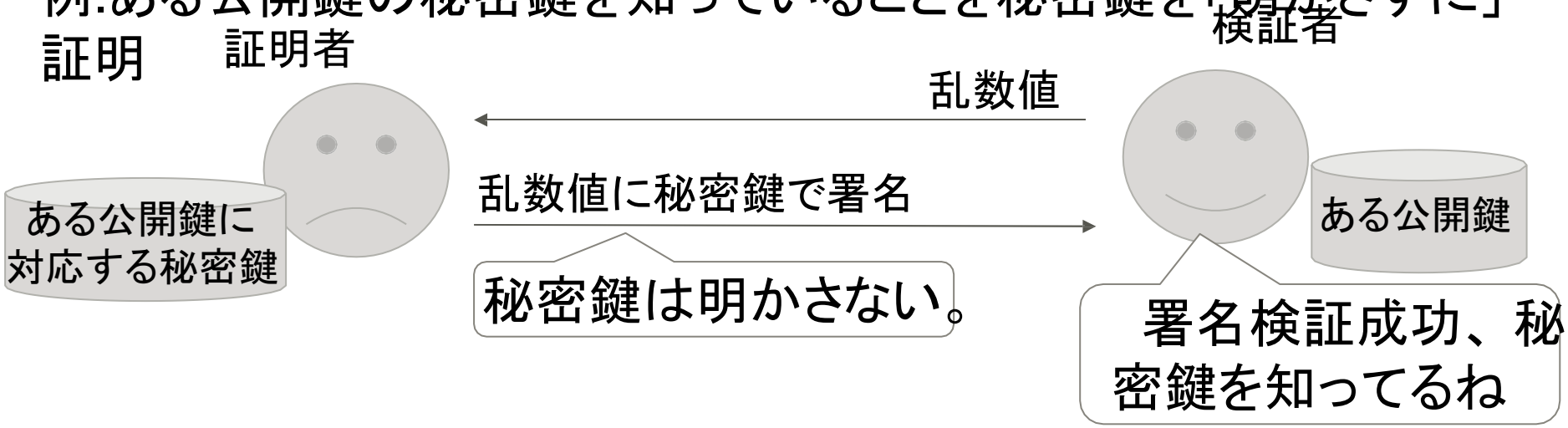
ゼロ知識証明の概要

FUJITSU

- 証明したい情報を明かすことなく、その情報に関することを証明す る手法とは?

  → その情報を知らないとできない計算をすることで証明

例.ある公開鍵の秘密鍵を知っていることを秘密鍵を「明かさずに」証明



証明内容に応じたプロトコル開発が必要

さまざまな証明が可能プロトコル: idemix, zkSNARKs,

分散型アイデンティティーとブロックチェーン連携において ゼロ知識証明でプライバシー強化する技術を研究開発

FUJITSU

分散型アイデンティティーとプライバシー強化技術

分散型アイデンティティーの必要性

FUJITSU

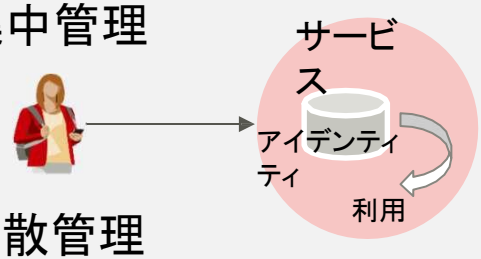
- 自己主権型アイデンティティー (Self-Sovereign Identity)
  - インターネットで、アイデンティティー(自分の属性)を個人が自ら制御

リアル

アイデンティティー= ID + 属性
物理的な証明書を自由に利用
名前や年齢、信用などの属性を証明

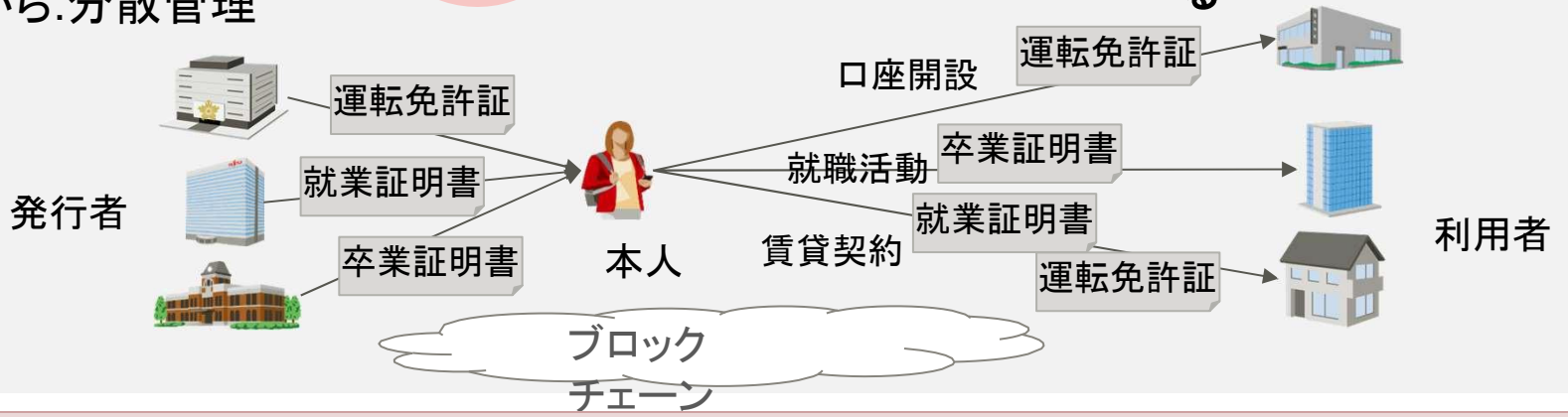
サイバー

これまで:集中管理



これから:分散管理

第三者によって発行された自身のアイデンティティーを、自身で所有・制御する



自分でアイデンティティーを制御することで、分散された信用(トラスト)を実現

アイデンティティー開示の課題

FUJITSU

- アイデンティティーを開示する目的は何か？

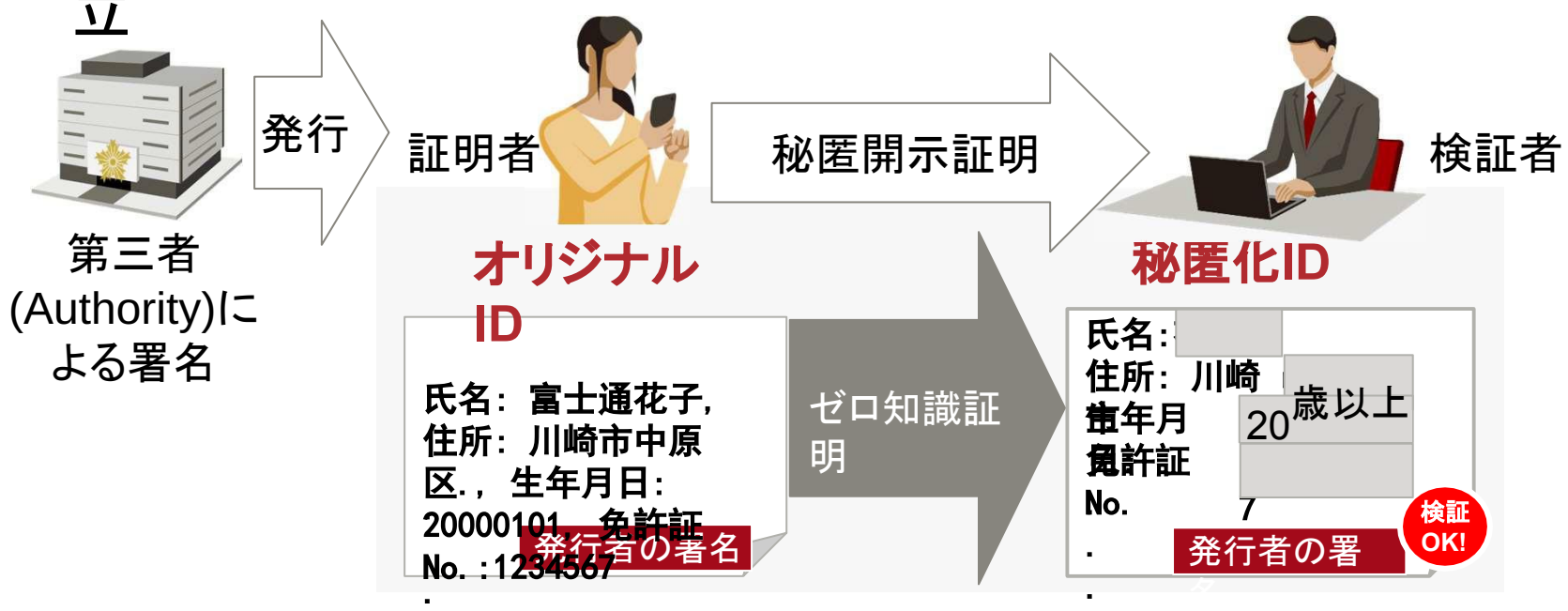
→ 開示先が必要とする項目を確認、トラストを得ること

プライバシーに考慮し必要な情報のみ開示したい
しかし、署名だと全項目を開示しないと検証できない

アイデンティティーの秘匿開示証明技術

FUJITSU

ゼロ知識証明技術を拡張し、デジタルIDの秘匿性と真正性を両立



技術ポイント: 属性値内の一部を秘匿しても、同一の署名で開示部 の正しさを証明することが可能 (既存技術: 属性ごとでの秘

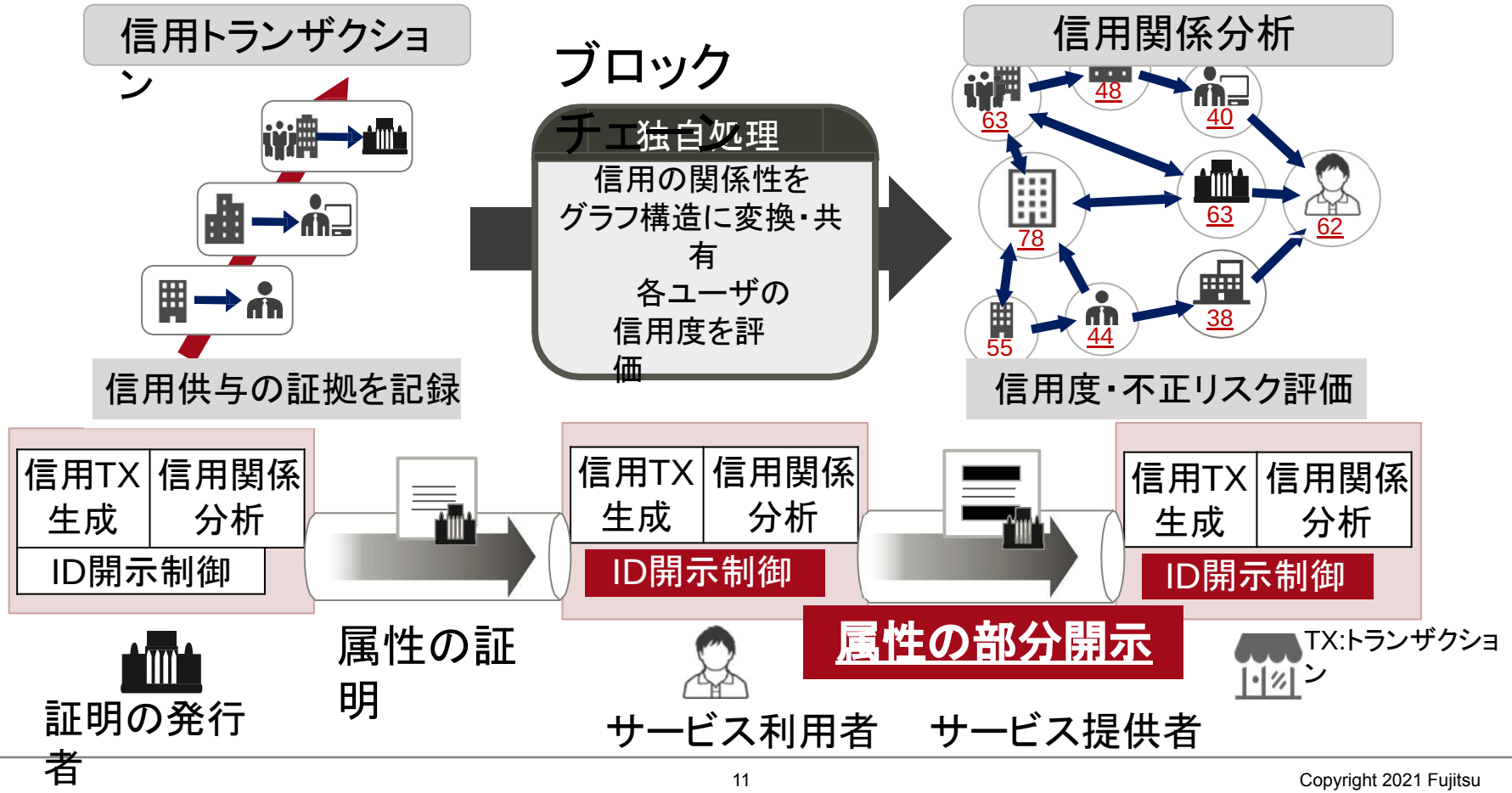
※ 署名方式はCL署名、署名自身も開示せずに証明

自身の正確な属性値を伝えることなしに、
情報の一部を伝えて正当性を証明するプロトコルを開発

アイデンティティー流通技術IDYX

FUJITSU

- オンラインの取引相手の信用を判断可能にし、アイデンティティーを流通
  - 取引によって発生するユーザー毎の評価をブロックチェーンに登録し、ユーザー間の 関係性から信用スコアを算出
  - ユーザーは一部の本人情報の開示だけで、それらの真偽を証明し、取引が可能



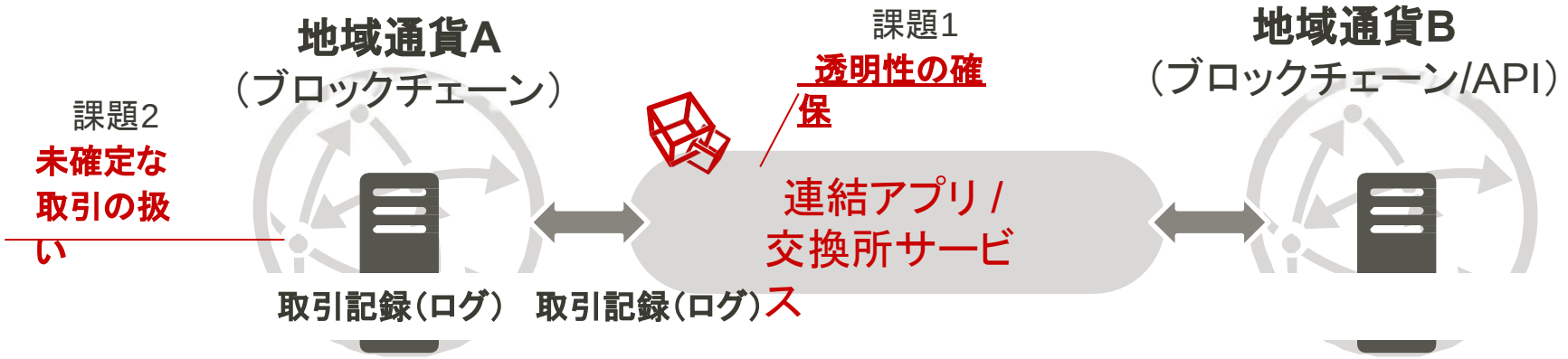
FUJITSU

ブロックチェーン連携とプライバシー強化技術

デジタル・トラスト実現に向けて

FUJITSU

- **ブロックチェーンの新たなニーズ**
  - ビットコインのみ→ アルトコイン、多くの仮想通貨(暗号資産)の存在
  - 異なる仮想通貨の交換や、ブロックチェーンどうし、ブロックチェーンと既 存システムなど「データの価値をつなげる」ニーズが高まる
- **ブロックチェーン連携の課題**
  - 透明性: 仮想通貨の交換所の不正により数百億円もの被害が出たケースも
  - 複数のブロックチェーンでの処理の整合性(ブロックチェーンは処理を戻せ ない)



デジタル・トラストの時代では、多様なシステムをつなげる際の透明性が最も重要

コネクションチェーン

- コネクションチェーン= ブロックチェーン「で」つなげる
- 異なるブロックチェーン間での、価値の交換を実現
- スマートコントラクトを拡張し、個々のブロックチェーンや APIで実装された異なる通貨の交換などの取引の透明性を確保

技術2:**取引の保留・キャンセル**

エスクロー口座を管理し、途中で取引失敗の場合にはロールバック

技術1:**拡張スマートコントラクト**

チェーンをまたがる取引履歴の透明性を確保

人手の処理をブロックチェーンで置換し、システム全体での透明性を確保

トークンエコノミーとプライバシー

- Gartnerによると2023年頃にトークンエコノミーがビジネス化
- トークンエコノミーの市場規模は2025年に48億米ドルになるとの予測も*1
- 既に商品や飲食店のレビューなどを対象にしたトークンエコノミーサービス
- 新たなシェアリングに - カラオケ個室でテレワーク、飛行機の座席でマスクを運搬

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

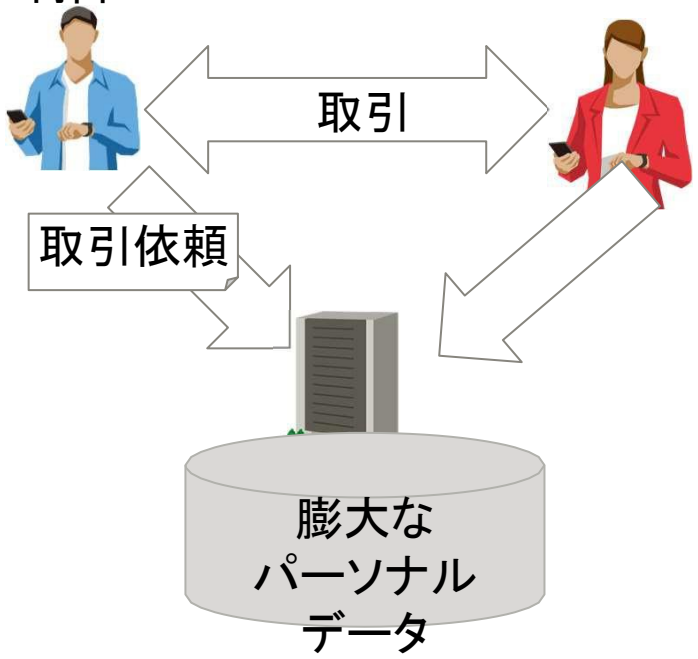
コネクションチェーンでトークンエコノミーをつなぐことを目指す

何をいつ使ったかなどのパーソナルデータが取引記録として残ることに

コネクションチェーンと取引データの活用

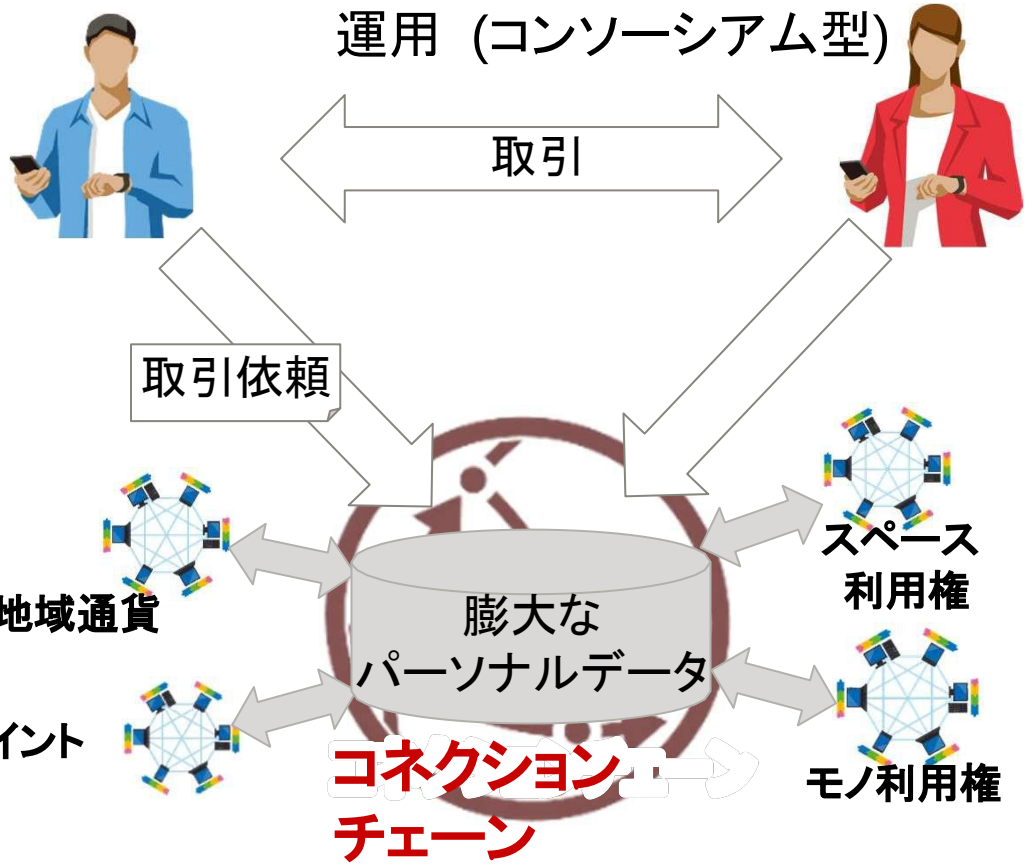
FUJITSU

中央集権プラットフォーマーが制御



透明性: 低
データ活用: プラットフォーマー可、他はプラットフォーマー次第

ブロックチェーンにより**分散型**で運用 (コンソーシアム型)



透明性: 高
データ活用:

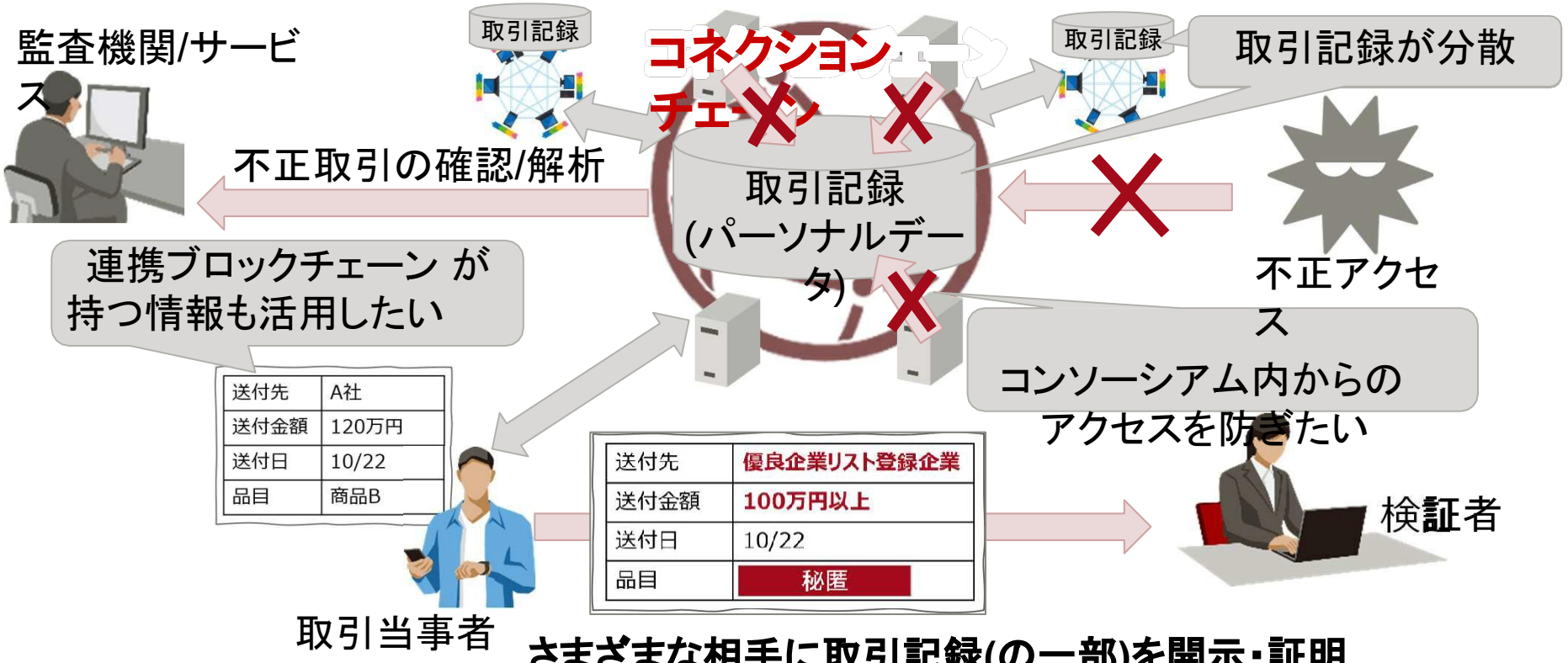
分散型でパーソナルデータを扱う場合の、
データ活用方法と漏洩リスク対象の検討が必要

データ活用と課題

- 監査機関による利用: マネーロンダリングなど不正な取引の調査など

（サービスによる利用: 取引履歴に基づいたリコメンドなど）

- **取引当事者による利用**: 領収書としての取引の存在・内容証明など



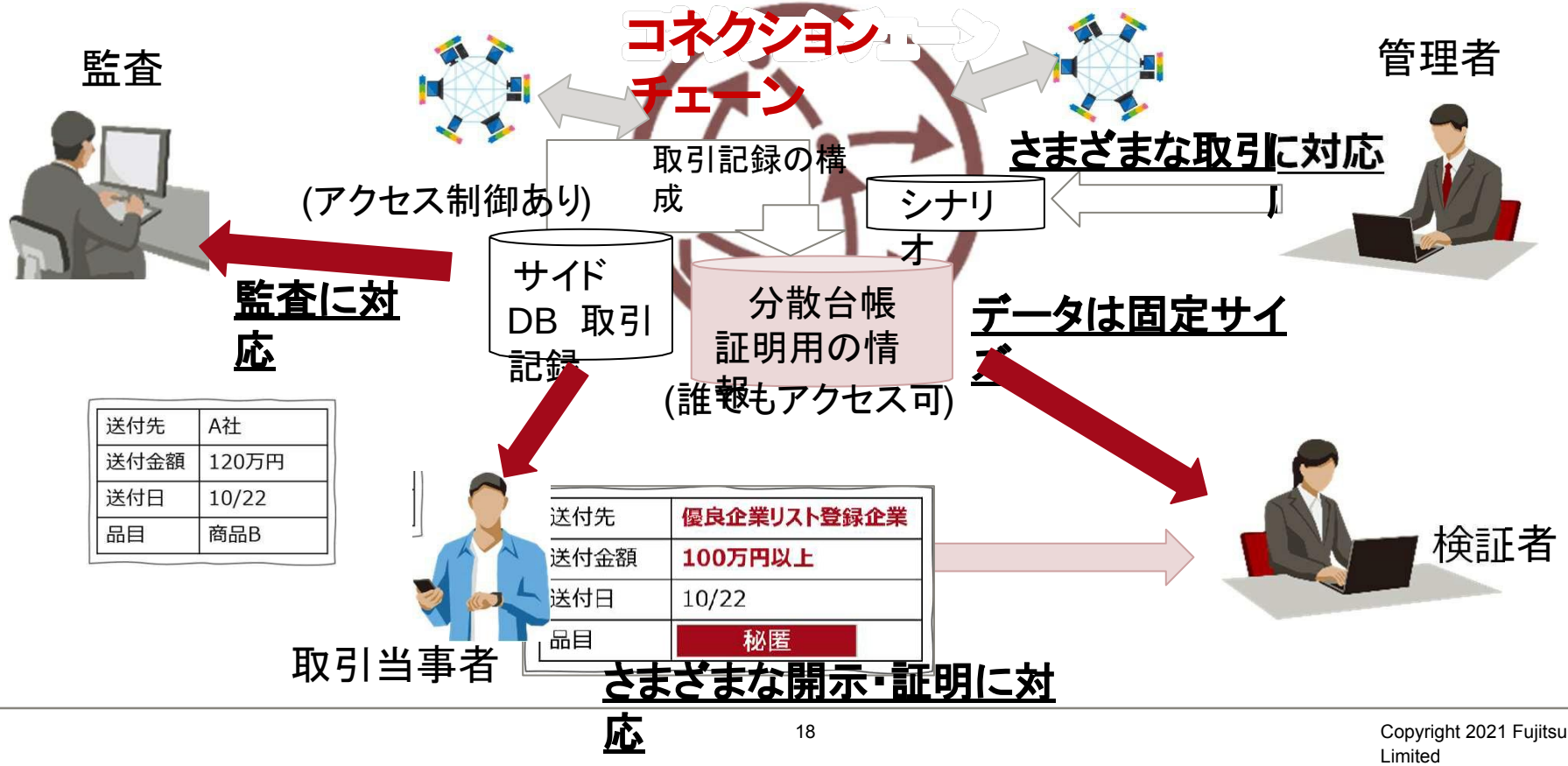
さまざまな相手に取引記録(の一部)を開示・証明

連携ブロックチェーンの取引記録の開示 → プライバシー保護は連携ブロックチェーンに依存 コンソーシアム参加者がアクセス可能 → 漏洩リスク、(ビジネス取引で)競合他社に渡る

取引データの秘匿開示証明技術を開発

FUJITSU

- 取引記録の構成: 取引シナリオ
  - シナリオに基づき連携ブロックチェーンから情報を収集して構成→ 取引記録の項目数増
- 取引記録の証明: ゼロ知識証明
  - 証明用の情報を分散台帳に保存し、取引記録の項目ごとに秘匿/開示を選択して証明可能
  - 技術のポイント: 分散台帳の証明用の情報は、項目数に依存しないデータ量を実現
- 取引データのアクセス制御
  ※ Hyperledger FabricのPrivate Data Collectionと同
  - 取引記録をサイドDBに保存(台帳に載せない)し、監査および取引当事者はアクセス可能



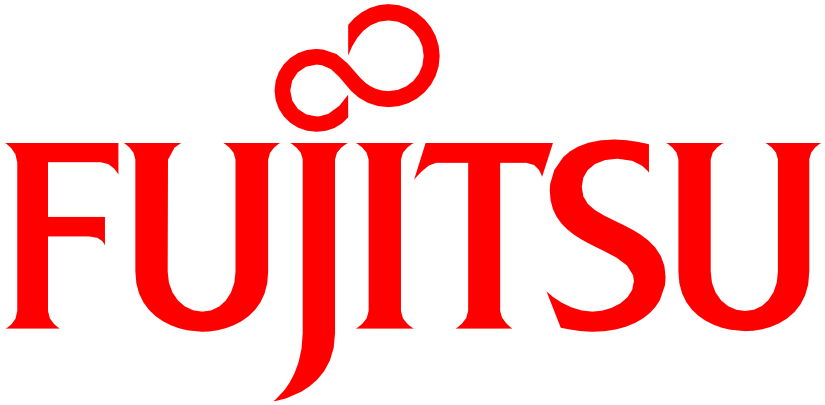
まとめ

FUJITSU

- 富士通ではブロックチェーン技術の進化を進めて応用領域を拡大してきた。その中から2つの事例をプライバシーの観点で紹介。

- 分散型アイデンティティー
  - アイデンティティー開示には、プライバシーに考慮して、内容を証明することが重要
  - 課題: 開示先により変わる必要とされる情報に合わせた柔軟な開示・証明
  - 解決: さまざまな秘匿・開示方法を選択して証明できるゼロ知識証明を開発
  - ポイント: 属性値内の一部を秘匿しても、同一の署名で開示部の正しさを証明可能

- ブロックチェーン連携
  - トークンエコノミーの実現には、取引記録の透明性とプライバシー保護の両立が重要
  - 課題: 分散台帳による透明性を確保した上で、開示先に必要な取引記録を開示・証明
  - 解決: 証明用の情報を台帳管理し、取引記録の項目毎に証明するゼロ知識証明を開発
  - ポイント: 連携により項目が増えた取引記録を固定□の証明用の情報で証明可能



shaping tomorrow with you