スマートコントラクト推進議員懇話会

スマートコントラクトの普及における ブロックチェーン活用の必要性について

2020年7月30日

FPTコンサルティングジャパン株式会社

本日の目的

- スマートコントラクト（先端技術を活用した次世代デジタル契約）を活用し、従来ビジネス枠組みを超えた、革新的なビジネスモデルの創造と社会全体への普及が求められています。
- しかし、従来の中央集権的なシステムを前提に、スマートコントラクトを官民含めた様々な業界や利害関係のある組織に普及していくことは極めて困難であると考えます。
- そこで我々は、ブロックチェーンによる自律分散社会を実現し、様々な異なる組織がアクセスできるオープンデータプラットフォームの構築が必要であると考えます。

ベトナムにおけるブロックチェーンの活用事例をご紹介

ブロックチェーンが目指す自律分散社会についてご説明

FPT開発したブロックチェーン“akaChain”をご紹介

ベトナムでのakaChain活用事例

FPTコーポレーションのご紹介

■ FPTコーポレーションはベトナム市場のリーディングカンパニーです。

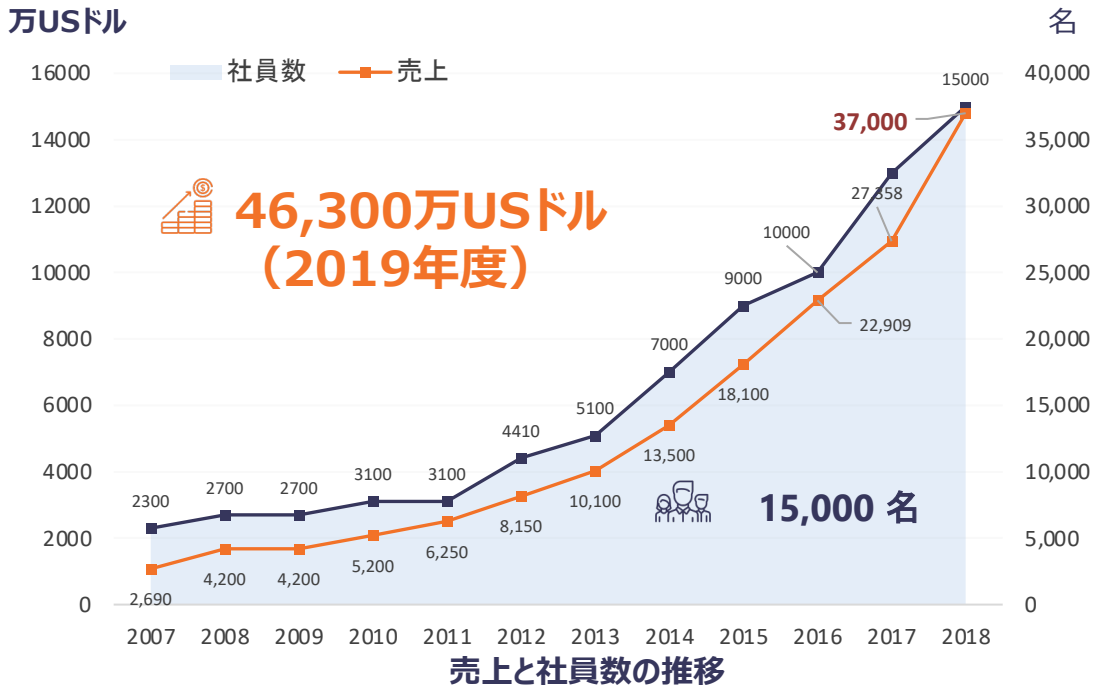
社名	FPT コーポレーション
資本	10.21億USドル（2018年度）
設立	1988年
本社所在地	ベトナム　ハノイ
ビジネス	• ソフトウェア • テレコミュニケーション • 教育
売上	10.21億USドル-流通・小売業への主要投資を含まない（2018年度）
研究開発投資	税引前利益の5%
社員数	34,000名（2018年度）
企業形態	上場企業　（2006年12月VNSEに上場）
役員	会長　Truong Gia Binh（チュオン・ザー・ビン） CEO　Bui Quang Ngoc（ブィー・クァン・ゴック）

FPTソフトウェアのご紹介

■ FPTソフトウェアはベトナム最大手でかつ最も成長しているソフトウェア企業です。

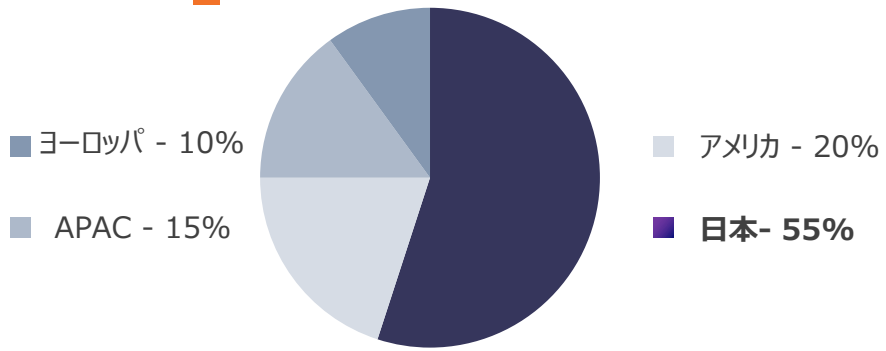
設立日	1999年1月13日
売上	4億6,300万USドル（2019年度）
本社	ハノイ　－　ベトナム
従業員数	16,000名 以上　（2020年1月現在）
成長率	33.4%（2013年～2017年）
国際基準認証	CMMI Level 5 v1.3 / ISO 9001:2015 ISO 27001:2013 (BS 7799 -2:2002) ISO/ TS 16949 / IEC20000-1:2011 ASPICE　LEVEL 3

FPTソフトウェアはFPTコーポレーション内の国外向けITベンダーです。
全世界16か国に拠点がありますが、FPTソフトウェアの売上の約60%が日本におけるビジネスです。



売上と社員数の推移

■ 市場別売上（2018年12月）



FPTソフトウェアのブロックチェーン事業体制

■ FPTソフトウェアは自社ブロックチェーン製品“akaChain”を開発、数多くの経験豊富なブロックチェーンエンジニアによって事業体制を構築しております。

Key Expertise ブロックチェーンのリソース

30
エキスパートエンジニア
ブロックチェーン研究開発ソリューション・チームで活用している

3
ブロックチェーン・マーケティング・チーム

70+
経験豊富なエンジニア
ブロックチェーン・プロジェクトで活用している

8
Corda資格

Partners

SBI Ripple Asia　aelf.　FACTOM

akachain

akaChainの日本での展開をミッションとしているのが
FPTコンサルティングジャパン(株)のakaChainチームです。

活用事例1 新型コロナウィルス拡大防止 (ベトナム)

■ 情報通信省と協力し、病院や政府機関等の官民の信頼性の高いデータを収集し、誰でも簡単にアクセスできるオープンデータベースを開発しました。

サービス概要

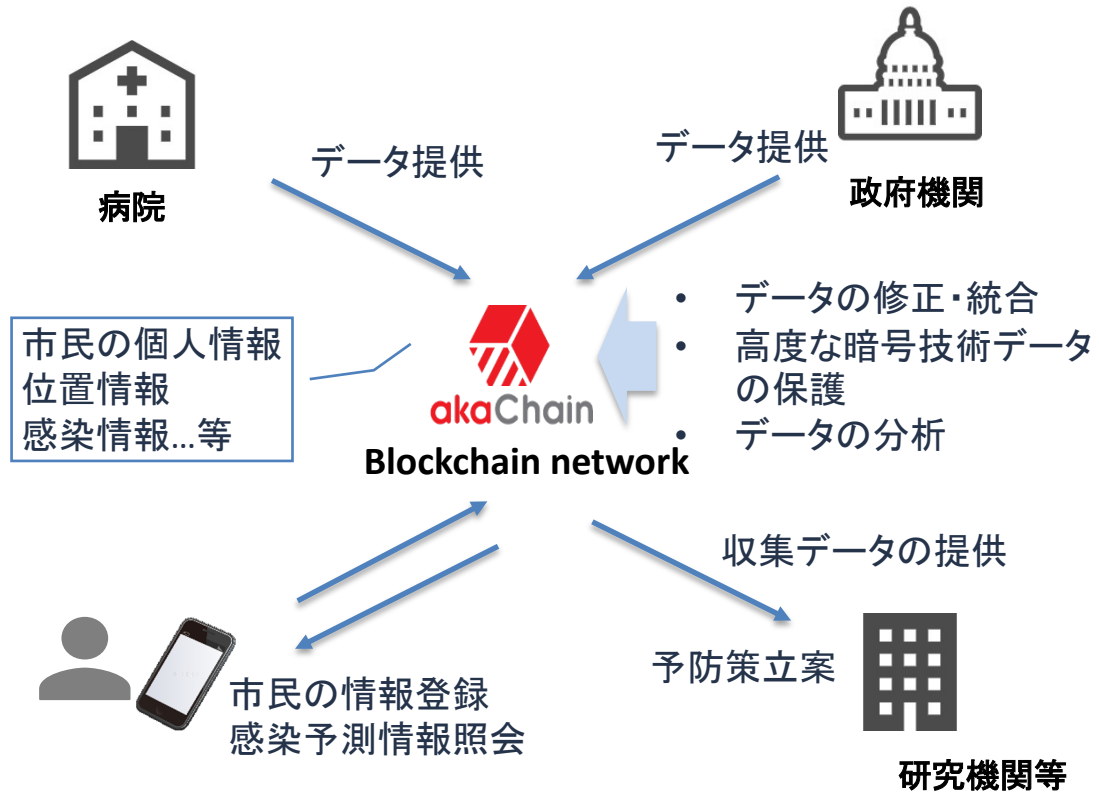
- 各種データを収集し矛盾やエラー及び誤りを修正して共有可能な形に統合
- 高度な暗号技術によりユーザーのプライバシー保護しながら、健康データと位置情報を管理
- 感染経路と発生に関するデータを組合せ、感染可能性のある場所を予測（無症状性キャリアの発生なども予測可能）

対象顧客と提供価値

- 医師や・科学者・研究者に対して信頼性の高いデータを提供することで感染予防の対策の立案に寄与
- 市民に対して感染の情報や、今後の感染可能性のリスクを示すことによる感染拡大を予防

サービスイメージ

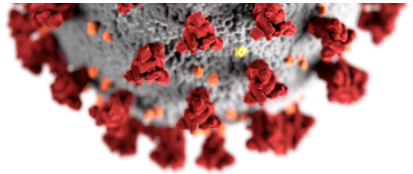
https://aicovidvietnam.info/#/home



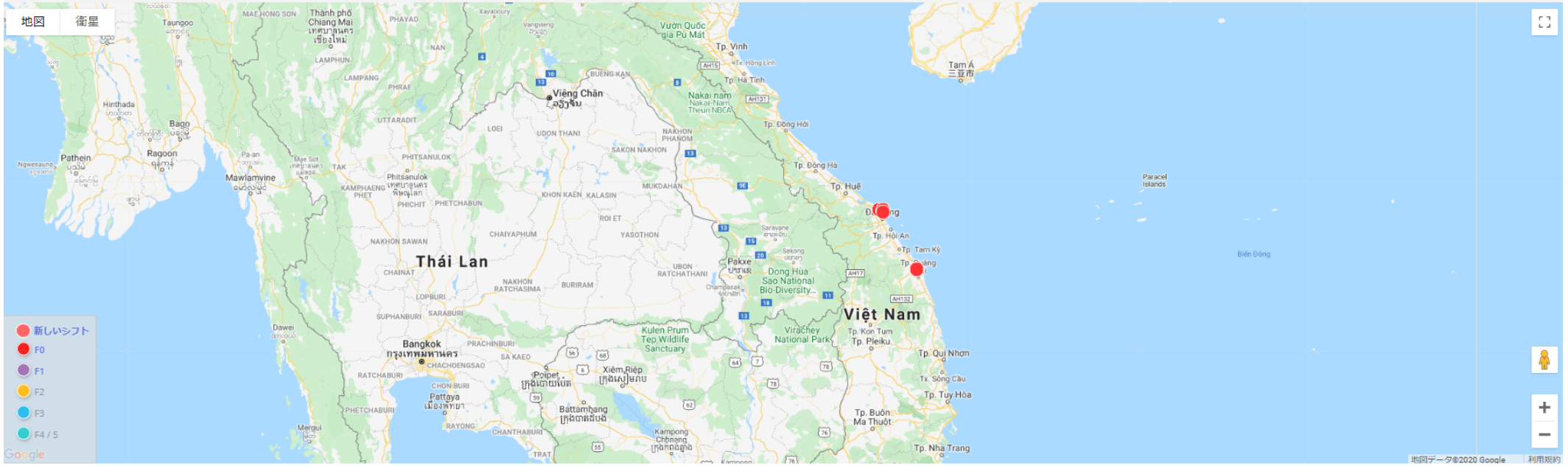
新型コロナウィルス拡大防止 (ベトナム)の画面

■ 地図上に、感染のレベルごとに位置情報がプロットされる。

コロナ感染の可能性を確認する



ベトナムのCovid-19マップ



Akachainによる電源

プライバシー　このプロジェクトは、情報通信省と協力しています

akaChain

活用事例2 医療保険金請求システム (香港)

■ 患者・病院・保険会社が共通利用できる医療保険金請求システムにより、患者の保険適用範囲やカルテを皆が認識し、取引がスムーズに実施されます。

サービス概要

- 保険契約を電子的に登録
- 病院は、患者の保険適用範囲を照会
- 病院から保険会社に補償を請求、補償範囲に応じて保険会社と患者が病院に支払

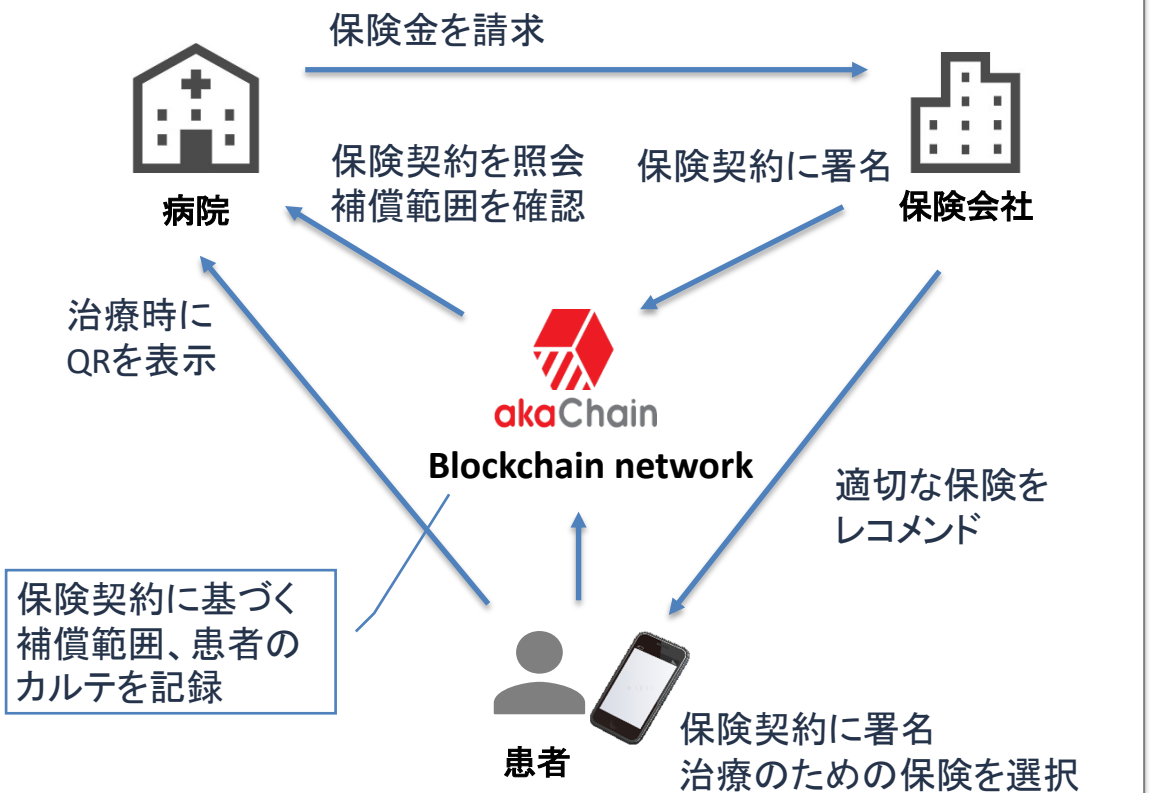
対象顧客と提供価値

- 患者は容易に病院のサービスを利用可能
- 病院は顧客と保険会社を同じプラットフォーム上で容易に管理可能
- 保険会社は保険の請求プロセスを容易に管理可能

マネタイズ方針

- 患者の治療計画を病院は保険会社に連携、保険会社の販売促進手数料を獲得

サービスイメージ



活用事例3 ロイヤリティポイント (ベトナム)

■ FPTリテール、FPTテレコムの他に、Redsun、TPBank、Hoayeuthuongなどの1,000万のエンドユーザーを有するポイントサービスを運営しています。

サービス概要

- Utopポイントの発行
- 他社の独自ポイントをUtopポイントに交換
- Utopポイントの加盟店での決済

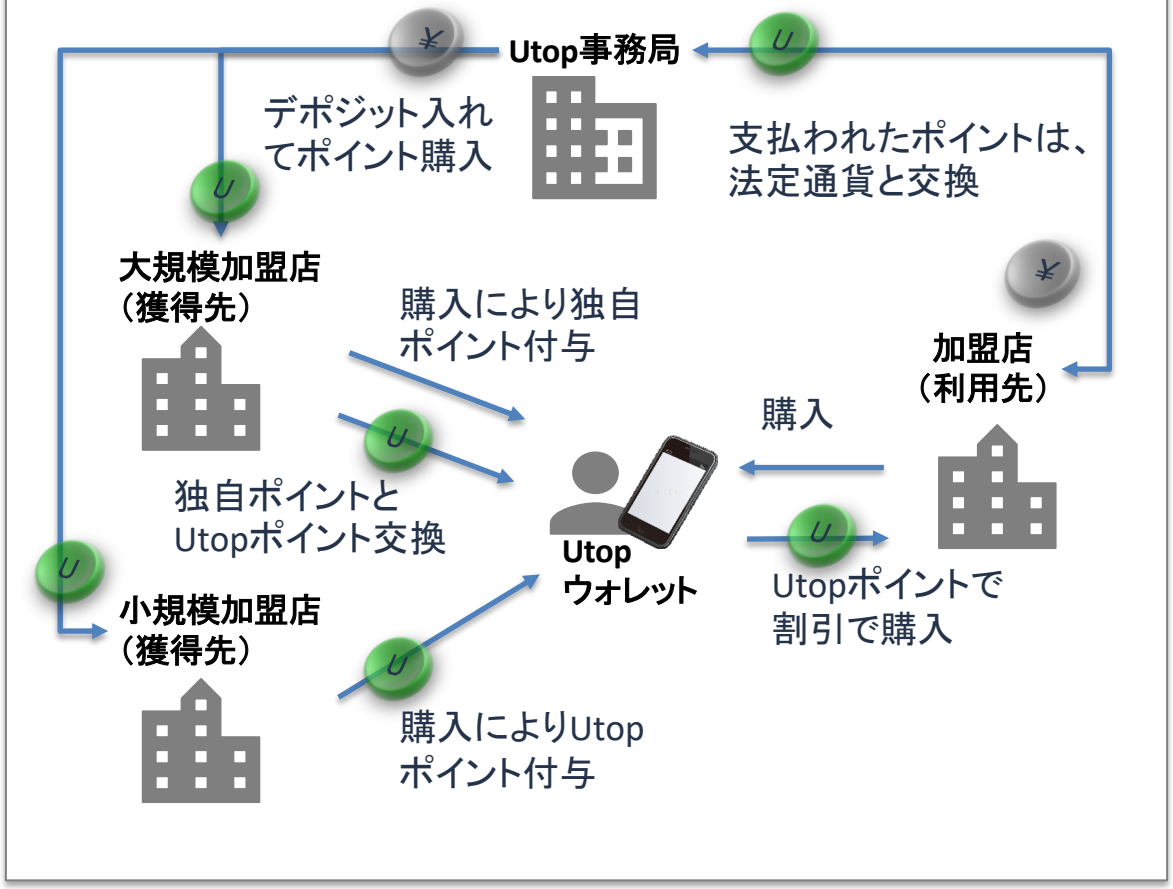
対象顧客と提供価値

- 購入頻度や価格の異なる様々な加盟店で共通のポイントを獲得・利用可能
- 購入頻度は少ないが、高額な商品にポイントを使った販売を促進

マネタイズ方針

- ユーザー情報に基づく商品・サービスをレコメンドし、販売促進・広告の手数料を獲得

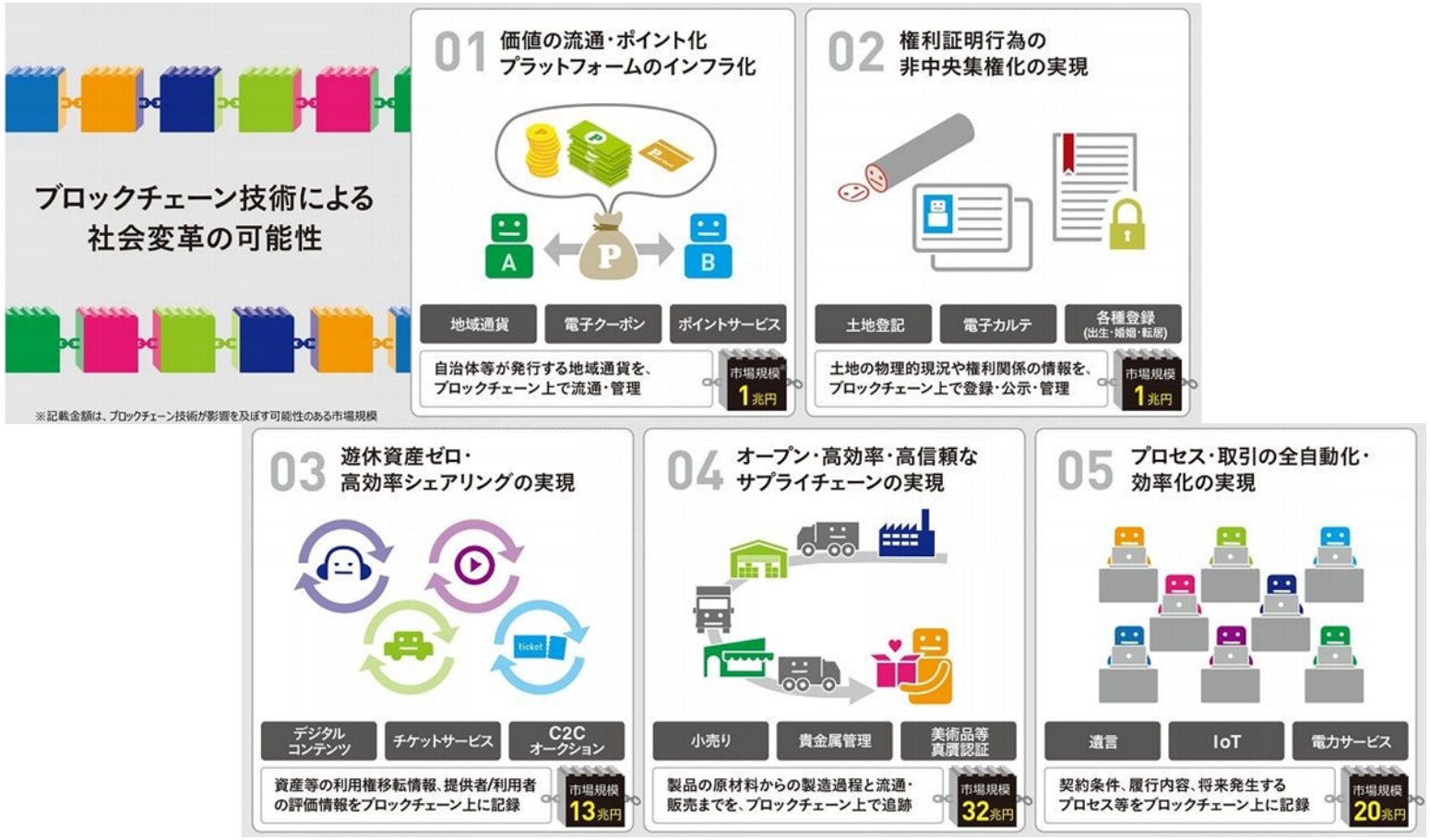
サービスイメージ



ブロックチェーンが目指す自律分散社会

ブロックチェーンの市場動向

■ 資産流通や権利証明等の小規模な活用から始まり、将来的にサプライチェーンや、重要な社会基盤の領域で活用される可能性があります。



グローバル市場

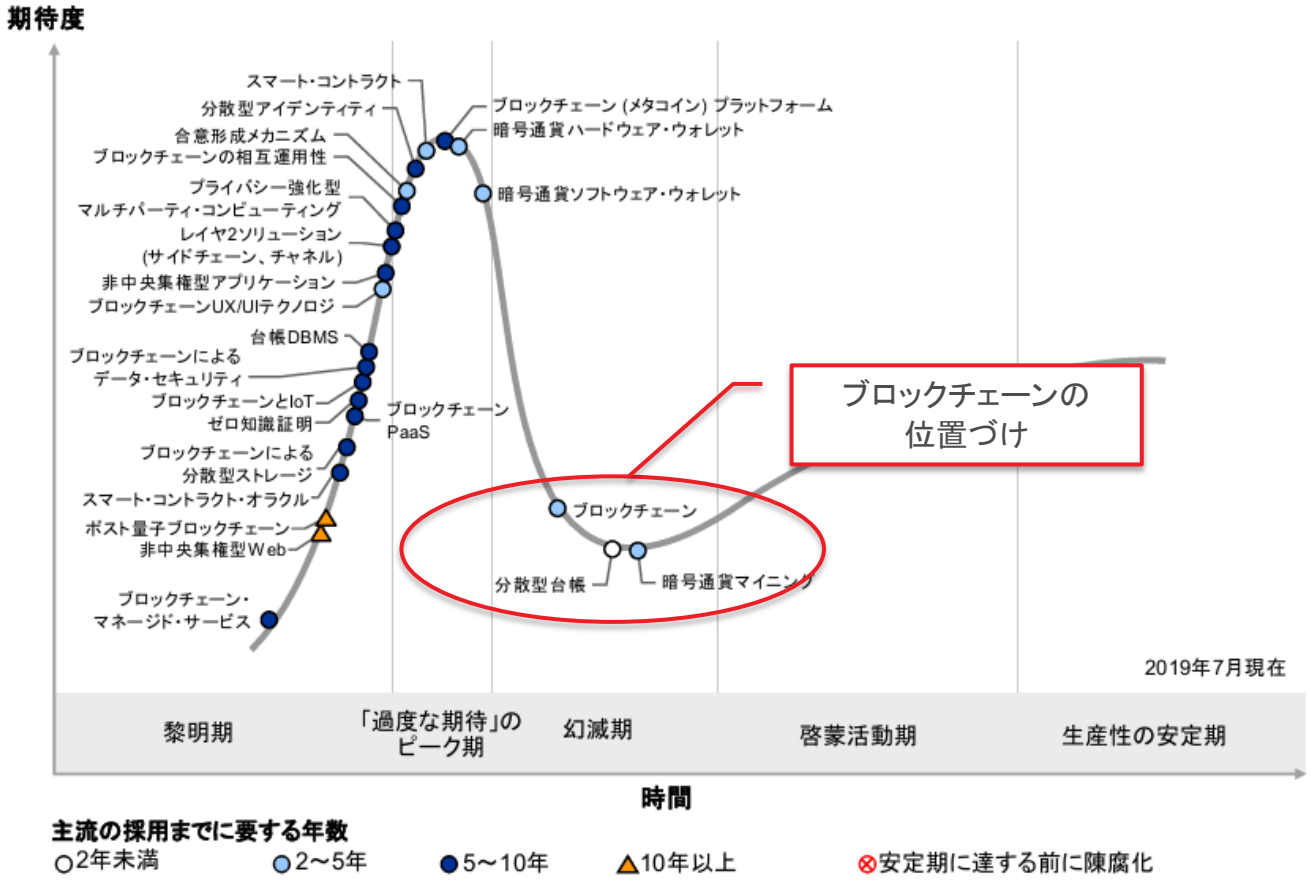
300兆円規模*1

*1：3.1兆ドル(2030年時点の予想値)「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備(平成28年4月28日 経産省)」(GARTNER)より抜粋
ブロックチェーン技術の展開が有望な事例とその市場規模（出典：経済産業省「平成27年度 我が国経済社会の情報化・サービス化に係る基盤整備」）

ブロックチェーンの技術トレンド

■ しかし、ブロックチェーンは幻滅期に入っており、良い面だけでなく、問題点にも向き合い、実用化に向け導入の領域やタイミングを見極める必要があります。

先進テクノロジのハイプサイクル：2019年*1



出典）ブロックチェーン・テクノロジのハイプ・サイクル：2019年
https://www.gartner.com/jp/newsroom/press-releases/pr-20191018

■「過度な期待のピーク期」から「幻滅期」の特徴

➢実証実験などの取り組みを通し、単に期待を抱いていたところから現実に直面

■実用化に向けてとるべき姿勢

➢基本に立ち返ってテクノロジーの本質を把握すると共に、問題点に向き合う

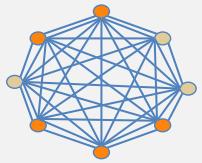
➢新技術の導入領域やタイミングを見極める

ブロックチェーンの特徴と活用テーマ

■ 従来システムでは実現が難しかった仲介者・管理者がいない環境で、異なる企業や組織及びユーザー同士の直接取引の安全性を保証します。

ブロックチェーンの特徴

① 参加者が仲介者なしに直接取引できる



- 自律分散ネットワーク

② 取引データの改ざんができない

- 取引履歴をブロック化して連鎖

③ 条件に応じた自動処理ができる

- スマートコントラクト

スマートコントラクトにおける活用テーマ

契約に基づく価値の移転

- 契約に基づいた、金銭や不動産の取引に活用

契約者の本人性確認

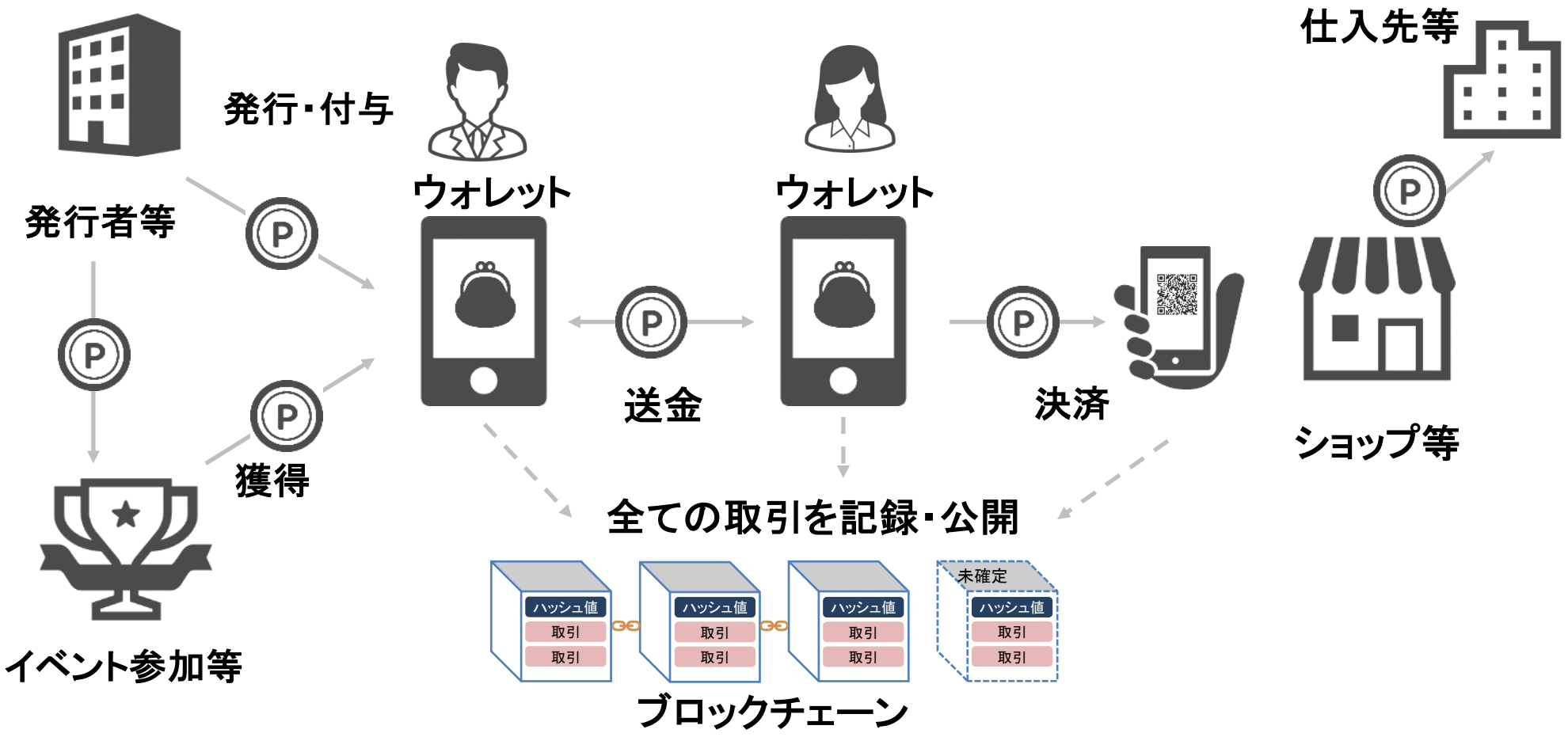
- 契約者同士が本当に本人であるかを検証するために活用

エスクロー取引の自動化

- 契約の履歴や、契約に基づく取引の履歴記録して追跡可能とする

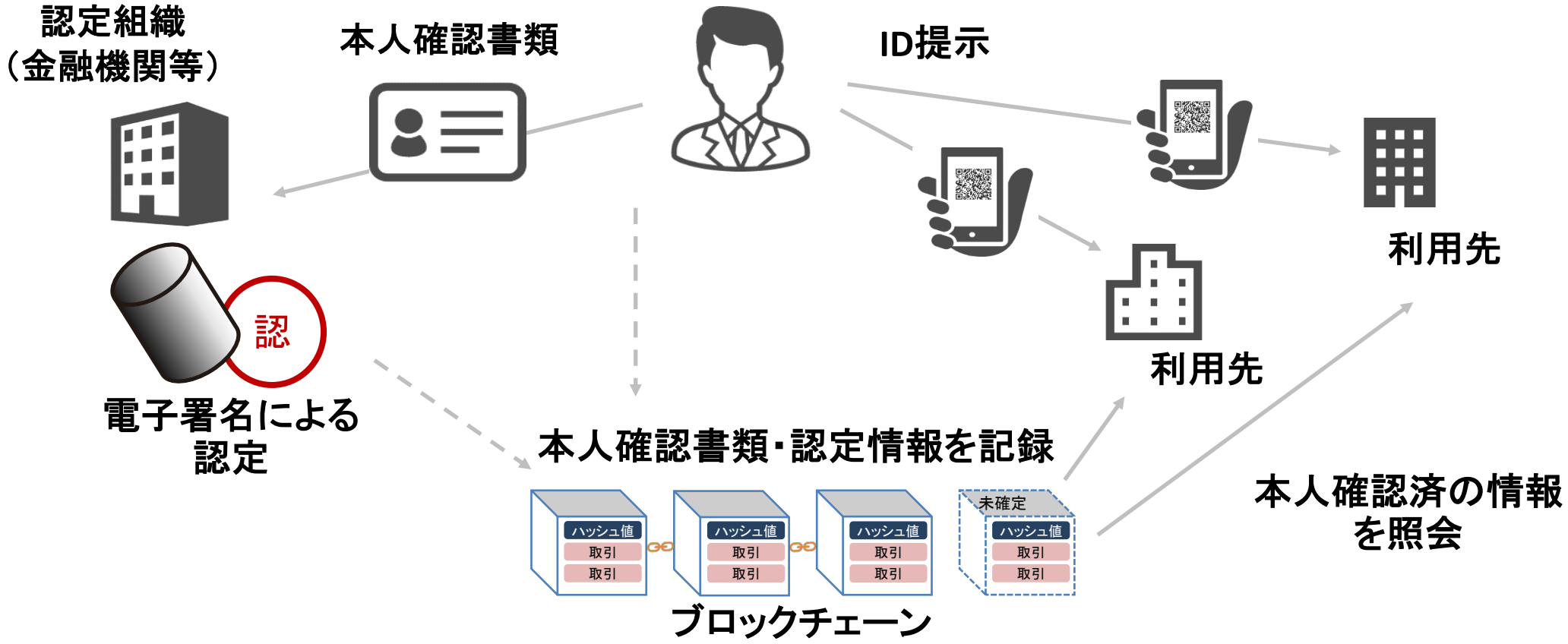
活用ユースケース①　契約に基づく価値の移転

■ ブロックチェーンで管理するトークンを流通、ユーザーがウォレットに残高を管理し、発行元を介さず直接取引を行うことができます。



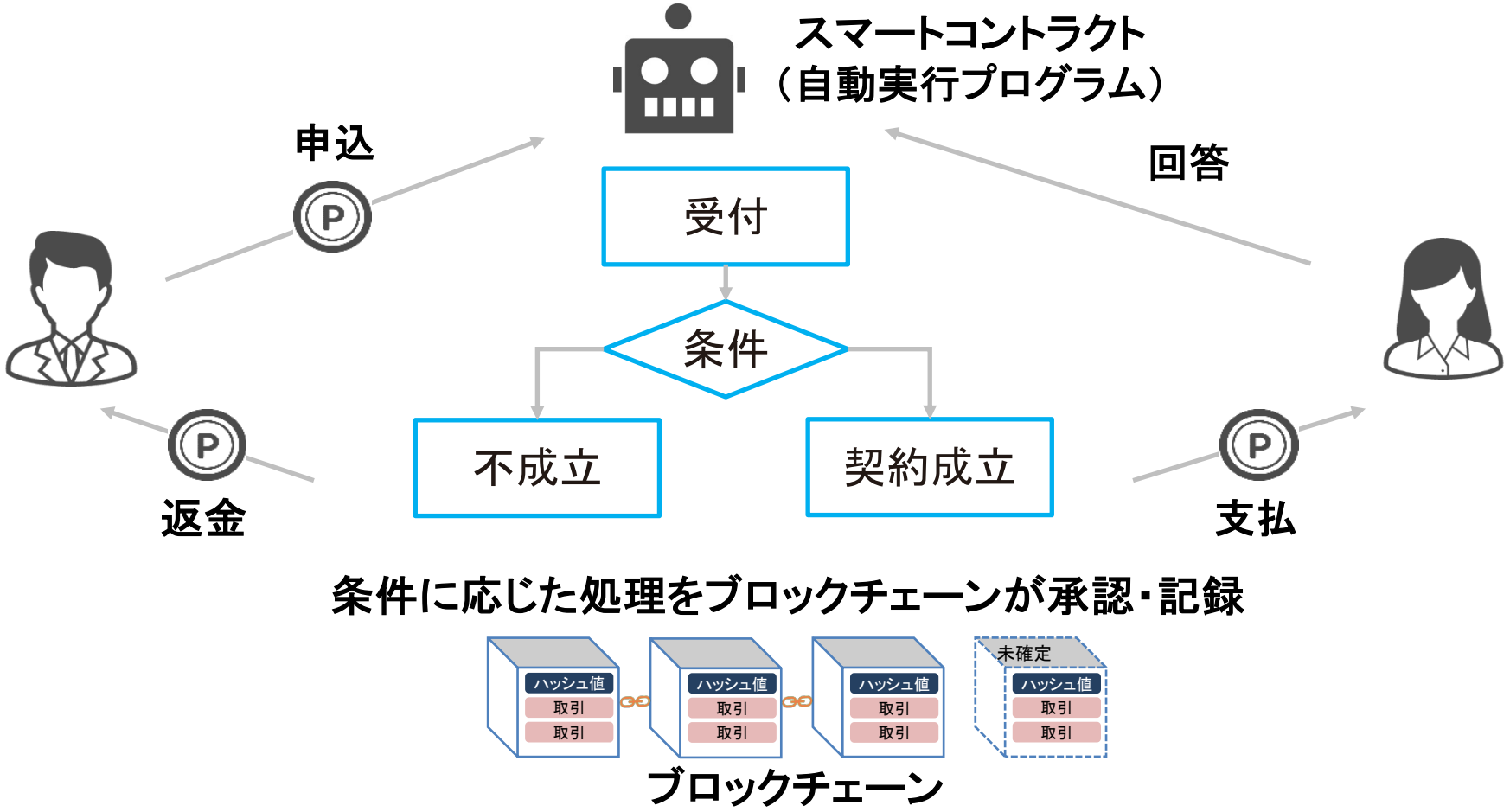
活用ユースケース②　契約者の本人性確認

■ ユーザーは、一度本人確認を行えば、その後、本人確認が必要な際にIDを提示するだけで、本人確認と同等の確認を容易に行うことができます。



活用ユースケース③　エスクロー取引の自動化

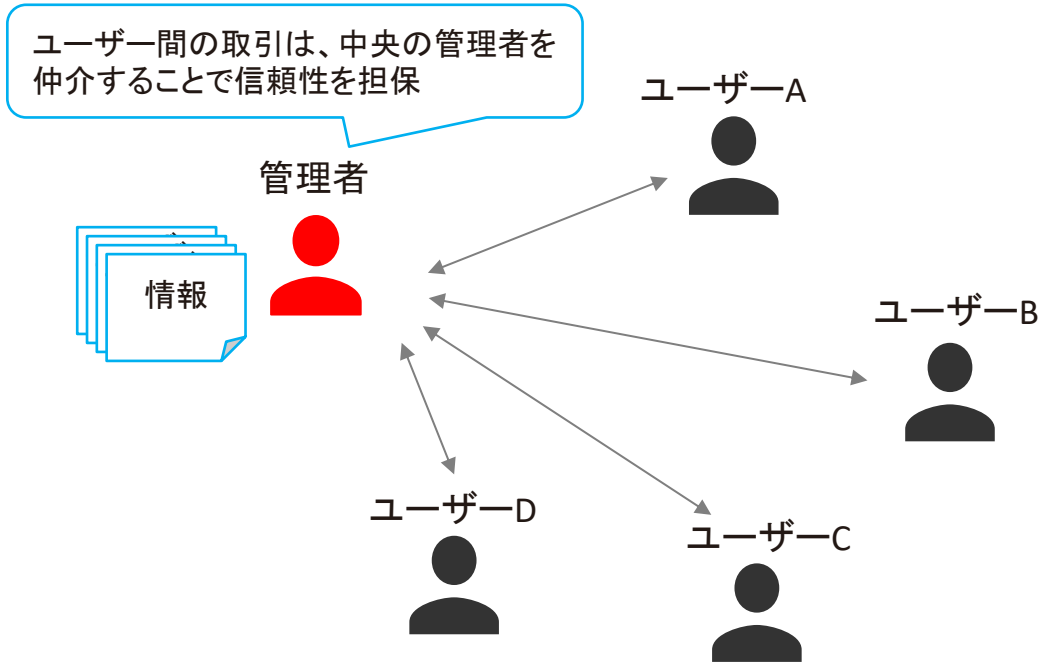
■ 自動実行プログラムである“スマートコントラクト”が仲介者を代替、相手の対応に応じて契約成立／返金を行うエスクロー取引が自動で実行できます。



ブロックチェーンが目指す自律分散社会

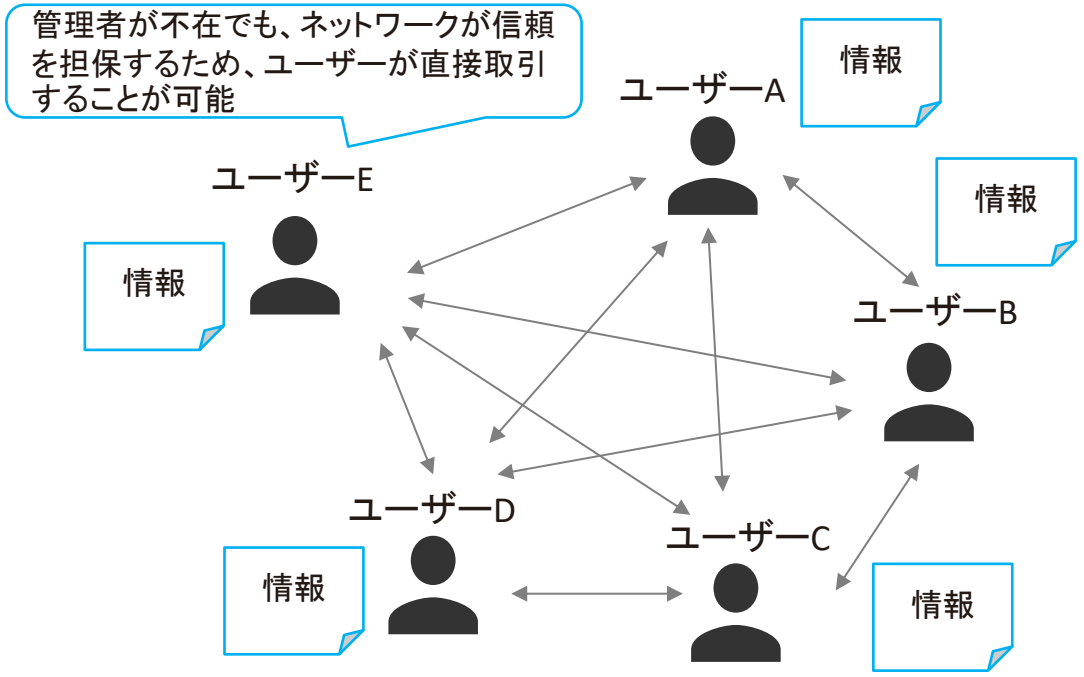
■ 複数の参加者が情報の正しさを確認することで、特定の管理機関に依存しない“ユーザー主権”の自律分散社会をブロックチェーンは目指します。

中央集権型社会



- ✓ 管理者が情報を一元管理
- ✓ 管理者がルールを策定し管理
- ✓ ユーザーを認証し、取引の正当性をチェック

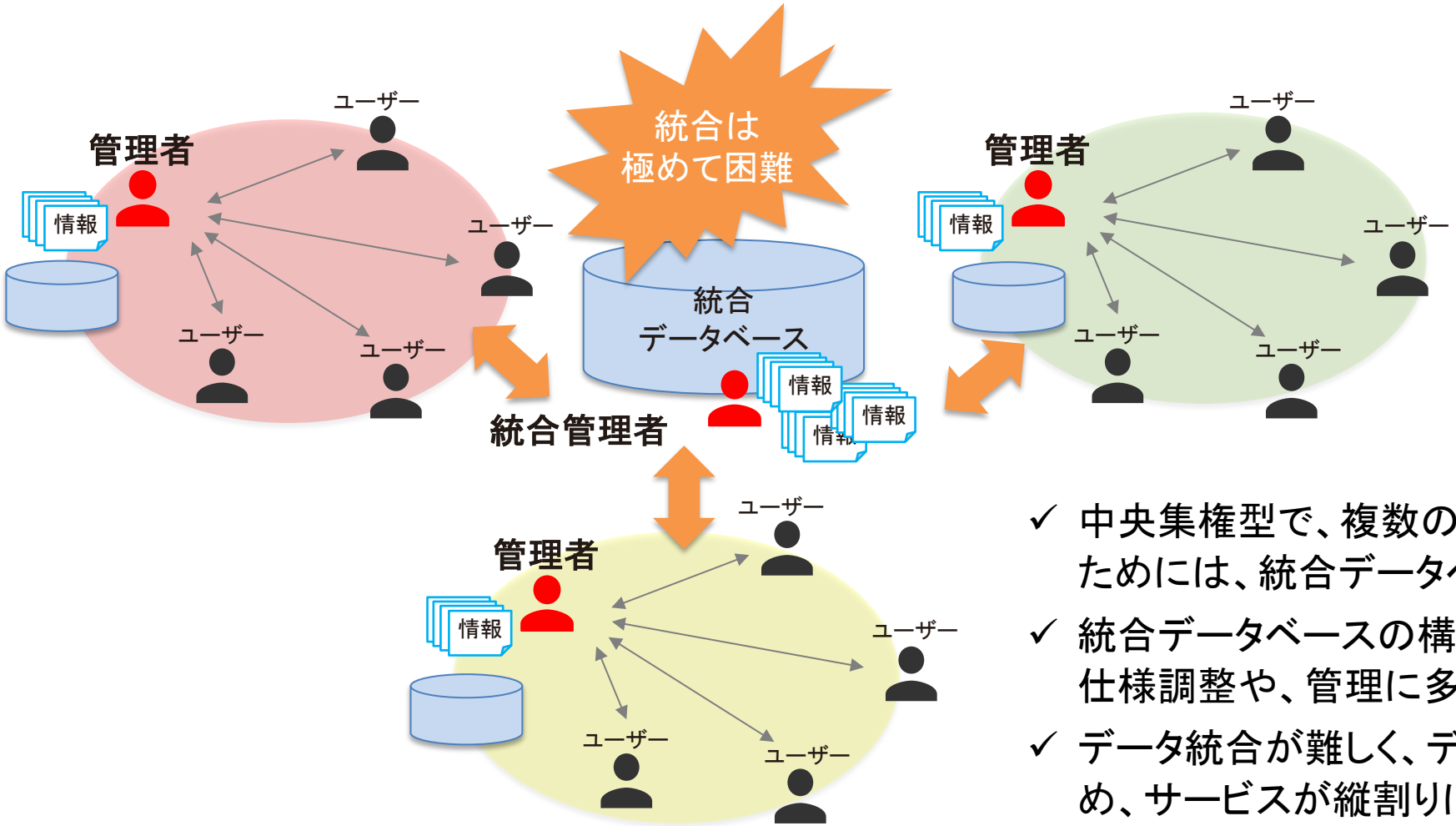
自律分散社会



- ✓ ユーザーが情報を共有
- ✓ ルールをネットワークのユーザーが策定・管理
- ✓ ネットワークがユーザーを認証し、取引の正当性をチェック

中央集権型におけるサービス統合の難しさ

■ 中央集権型社会ではデータが縦割りになっており、サービスを統合には、さらに上位に統合管理者と統合データベースが必要となるため実現は極めて困難です。

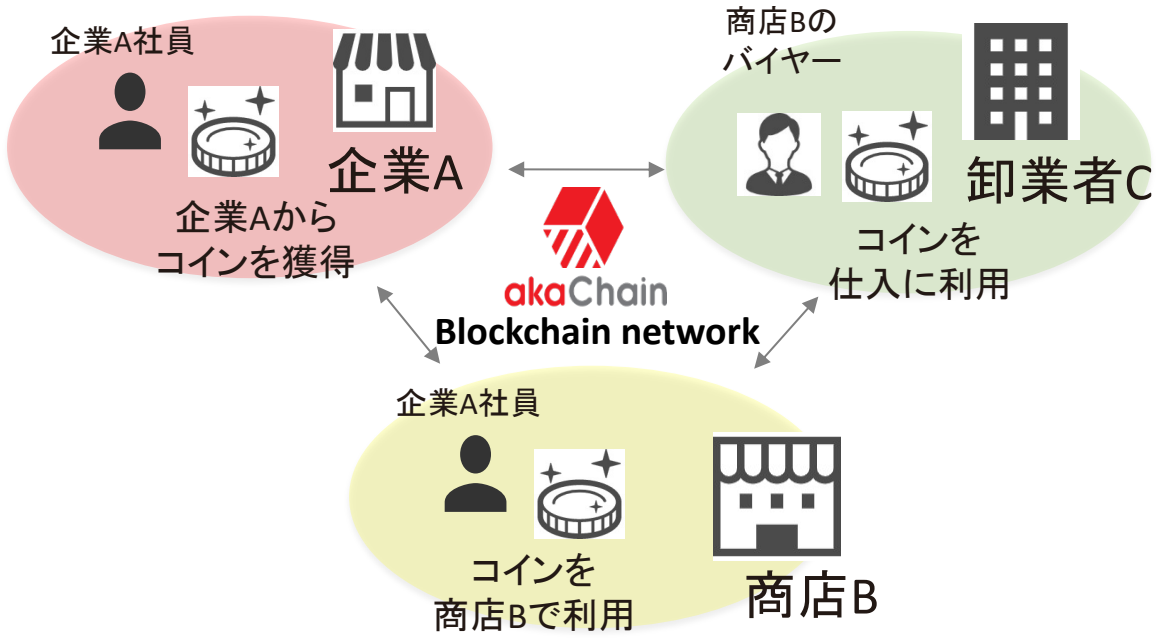


- ✓ 中央集権型で、複数のサービス間で取引を行うためには、統合データベースが不可欠
- ✓ 統合データベースの構築や維持には、組織間の仕様調整や、管理に多大なコストを要する
- ✓ データ統合が難しく、データが縦割りのままのため、サービスが縦割りになる傾向

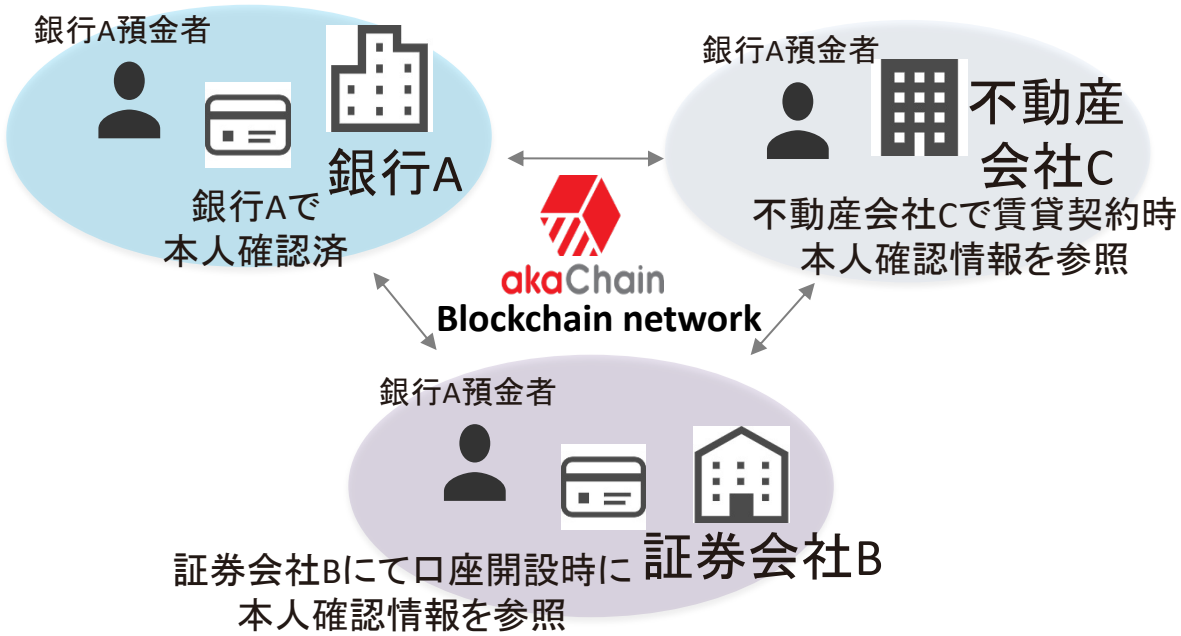
オープンデータプラットフォームの必要性

■ スマートコントラクトを官民含めた様々な業界や利害関係のある組織に普及するためには、ブロックチェーンによるオープンデータプラットフォームが有効です。

異なる業界での決済の統合



異なる企業間での信用情報の連携



✓ ネットワークに参加している異なる事業主体間で信頼して利用可能

✓ ネットワークに参加している異なる事業主体間でユーザーの信用情報を相互に共有

✓ ユーザーは毎回本人確認する手間が省け、事業者は、より精度の高い審査・与信が可能

akaChainのご紹介

ブロックチェーンの種類

■ ブロックチェーンは、承認者を限定し処理時間を短縮する方向性で進化し、様々な種類が存在します。

	ブロックチェーンの種類		特徴や代表的なサービス	
パブリック・ブロックチェーン	**PoW** (Proof of Work)	■ 膨大な計算処理を行い、最初に計算を終えたノードがブロックを生成	■ 改ざんが事実上不可能だが、取引に時間を要す（10分）誰もがブロック生成可能であり可用性は極めて高い	bitcoin
	PoS (Proof of Stake)	■ コイン保有量・期間が大きいノードは計算処理を容易にすることでブロック生成時間を短縮	■ PoWよりは取引時間が短い（12秒）、コイン長者による不正リスク有	ethereum
	DPoS (Delegated Proof of Stake)	■ コイン保有量により投票権を獲得、投票で選ばれたノードのみがブロックを生成することでブロック生成時間を短縮	■ PoSよりさらに取引時間が短い（数秒）、候補者による不正リスク有	LISK EOS
	PoI (Proof of Importance)	■ コイン保有量・期間に加え、直近のコイン使用頻度を加味し計算処理を容易にすることでブロック生成時間を短縮	■ PoSよりさらに取引時間が短い（数秒）、コイン長者によるによる不正リスク有	nem
プライベート・ブロックチェーン	**PBFT** (Practical Byzantine Fault Tolerance)	■ ブロックの生成権限のあるノードの2/3以上の合意を経てブロックを生成	■ 権限を特定ノードに集中させ、承認時間を短縮（数秒）、信頼できる機関による運営が必要	HYPERLEDGER
	PoC (Proof of Consensus)	■ 発行主体が選定した承認機関のうち80%以上が有効と認めた取引のみを承認	■ 権限を特定ノードに集中させ、承認時間を短縮（数秒）、信頼できる機関による運営が必要	ripple

ブロックチェーンの実用化に向けた問題点

■ パブリックチェーンは全参加者が平等でオープンである一方、性能や秘匿性に問題があり、プライベートチェーンは中央集権的になるという問題があります。

ブロックチェーンの商用利用を想定する際に直面する問題点

パブリック・ブロックチェーン	処理速度が遅い	■ 取引が承認（ブロックが生成）されるまでに時間を要す	■ で改ざん耐性を確保するために、ブロックの生成に一定程度の難易度を設ける必要があり、取引の承認（ブロック生成）に時間が必要 ➢ ビットコイン：約10分、イーサリアム：約12秒 等 ＊上記時間でハッシュ値が計算できるよう難易度が自動調整される
		■ 取引が承認され、ブロックが生成されても取引が覆る可能性がある	■ 複数ノードが同タイミングでブロック生成した場合、ブロックチェーンが分岐 ➢ ブロックが複数繋がって確率論的に取引が確定（ビットコインで6ブロック） ブロック ブロック ブロック ブロック ブロック ブロック 短い方の取引は無効 長い方を正当なブロックチェーンと認識
		■ 単位時間当たりに処理可能な取引件数(スループット)が制限される	■ 仕様上、ブロックサイズが決められており、これを超過するトランザクションはブロックに格納できない ➢ ブロックサイズの仕様変更はハードフォークを伴い、対応難易度が高い ➢ ＊ビットコイン(1MB)はビットコインキャッシュ(8MB)にハードフォーク
	秘匿性が無い	■ 全参加者が全ての取引履歴を参照可能であり、プライバシーに懸念あり	■ 全参加者がブロック生成(過去の取引履歴を参照して残高や二重払いのチェックを行う)権限を持つため、取引履歴はオープンにしておく必要あり
プライベートブロックチェーン	中央集権傾向	■ 取引の承認（ブロック生成）の権限を限定することによる中央集権化の懸念	■ 取引の処理時間を短縮するために、取引の承認（ブロック生成）の権限を特定のノードに限定するため、特定のノードの結託やハッキングによる不正が発生するリスクがある

商用利用に特化したakaChain

■ FPTのブロックチェーンであるakaChainは商用利用目的に特化したプライベートブロックチェーンをベースとしています。

	種類・特徴	ルール・方針の決定	システム・データ
パブリックブロックチェーン	■ オープンなネットワークであり、参加は自由、全てのユーザーが情報を参照・更新できる ■ Bitcoin, Ethereum 等	■ ブロックチェーン上のプログラムに従う	■ データの原簿は、複数システムに分散し、改ざんが不可能 ■ 参加者全員が同じ情報を参照
プライベートブロックチェーン	■ ネットワークに参加するためには運営者の許可が必要、情報の更新は承認されたユーザーのみが可能 ■ Ripple, Corda, Hyper Ledger Fabric 等	■ ネットワークを運営する企業（複数企業によるコンソーシアム）が担う	

akaChainはHyper Ledger Fabricをベースとしている

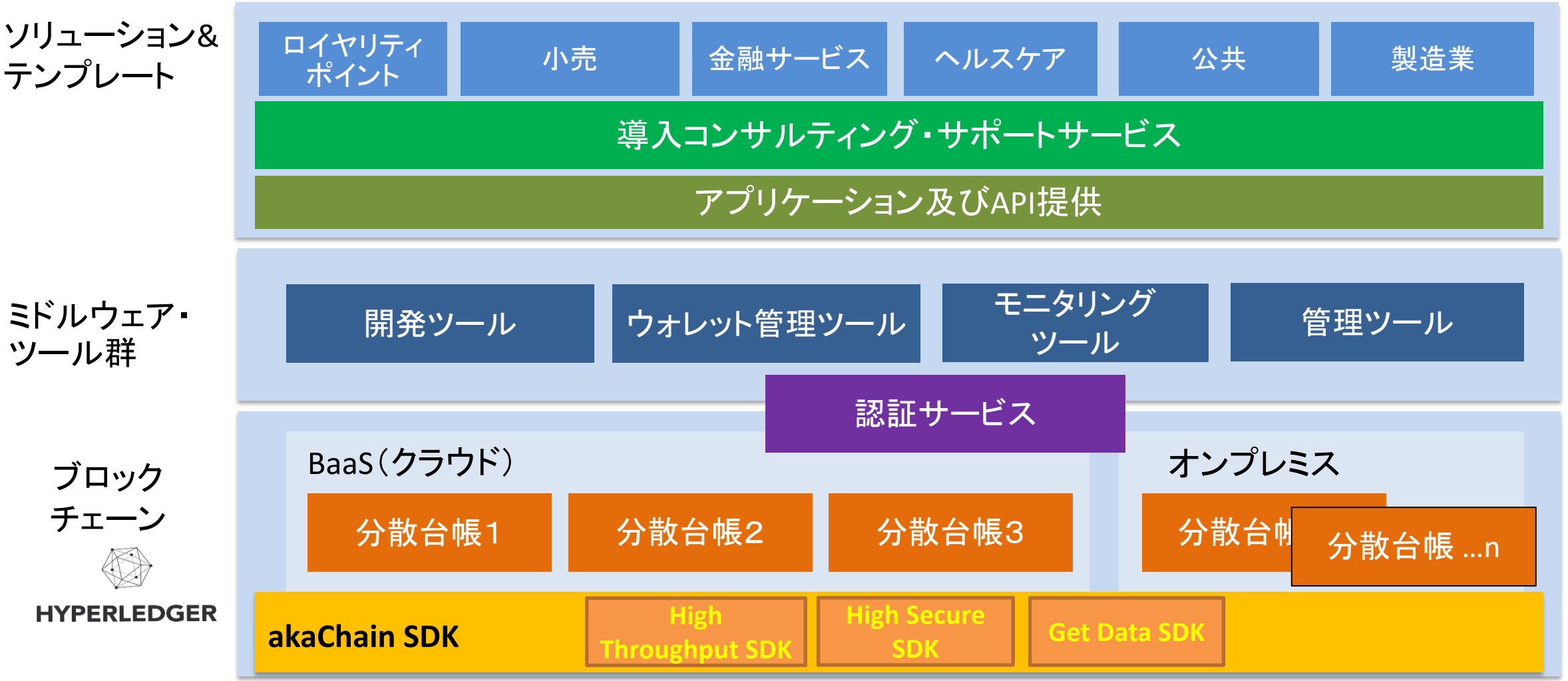
ブロックチェーン商用化に向けた課題

■ ブロックチェーンの商用利用に向けて、ビジネス面及び技術・運用面で乗り越えるべき課題をakaChainは解決します。

ブロックチェーンの商用化に向けた課題認識		akaChainによる解決方向性
Why ブロックチェーン	■ 現行システムの代替で、なぜブロックチェーンを使うのか？明確な回答が無い	• ブロックチェーンの特徴を活かすユースケースから検討し、段階的に活用領域を拡大する導入コンサルを提案
コストメリット	■ コスト削減効果の明確な説明が難しい	• 導入コンサルの中で、コスト増減ドライバーを明確化し、ビジネスケースを策定
選定基準	■ 最適なプロダクトの選定基準が無い	• 導入コンサルの中で、機能面・非機能面からの選定基準の明確化し、最適な解決策を提案
処理性能	■ 決済等の即時処理への対応が難しい ■ データの検索に制約がある	• 処理性能改善、検索性向上のアーキテクチャを提供
データの秘匿	■ データが共有され、個人情報や機密情報を秘匿できない	• データの特性に応じた、セキュリティ確保機能を提供
サポート体制	■ 商用利用を想定したサポート体制に不安がある	• 充実した技術支援及びカスタマーサポートを提供

akaChainの全体構成

■ コアブロックチェーン上に、ユースケースに応じてアプリケーションの開発・運用を支援するツールやテンプレートによって構成されています。



akaChainの特徴

■ 商用での利用を想定した機能やサポートを充実し、開発スピードの実現がakaChainの強みです。

エンタープライズソリューション

- 企業固有の複雑なビジネスに、柔軟に対応し、データプライバシーを確保するアーキテクチャを提供（ブリッジプロトコルやマルチチェーン等）
- 高いスループット（200tps～）
- 監視ツールとガバナンスの提供

迅速な開発スピードの実現

- サービスのソリューション＆テンプレートを活用した短期開発の実現
- クラウドサービスとしてブロックチェーンサービスを提供（BaaS）
- 自動実行プログラム（スマートコントラクト）を提供

グローバルでのサポート体制

- 24時間年中無休のグローバルプラットフォームサポート
- 現地国でのタスクフォースの組成
- ベトナムでの製品の継続的な研究開発とメンテナンス/アップグレード

エコシステムの拡張性

- 外部のブロックチェーン（ビットコイン・イーサリアム等）との接続するクロスチェーンプロトコル

Thank you !!!

Contact:
Nguyen Huu Long（ロン）: longnh1@fsoft.com.vn
鈴木　理：suzuki-osamu@akachain.io