ブロックチェーンの実証実験企画

参考資料

2019年1月25日

株式会社 bitFlyer

bitFlyer

ブロックチェーンで世界を簡単に。

本資料はブロックチェーンの活用における参考情報の提供を目的としており、当社の仮想通貨交換業の勧誘を目的としたものではありません。
当社は本資料の掲載情報に関し、最新かつ正確な情報を提供するよう努めておりますが、その完全性・正確性について保証するものではありません。
また、本資料における内容は個人的見解を含むことがあります。ブロックチェーン導入または使用等におけるリスク、その他ご質問については、当社までお問い合わせください。

本書の目的と構成

本書の目的

- ブロックチェーンの活用を企画する際に、企画書に盛り込む参考情報となる要素をまとめました。

構成要素	内容
取り組む必要性	■ ブロックチェーン市場動向 ■ 金融デジタライゼーション戦略への対応
何から取り組むか	■ 地域銀行の状況、及び企業が銀行に求める役割 ■ ブロックチェーン活用ステップ
どのように進めるか	■ 技術基盤の構築と、早いサイクルでのPDCAプロセス ■ 実証実験の想定スケジュール

取り組む必要性(1/2)

- グローバル及び国内のブロックチェーン関連支出は今後急速に拡大、金融セクターが主導すると見込まれ、銀行における急速な採用がその主な促進要因になると予測されております。
- https://www.idcjapan.co.jp/Press/Current/20180905Apr.html

グローバル市場動向

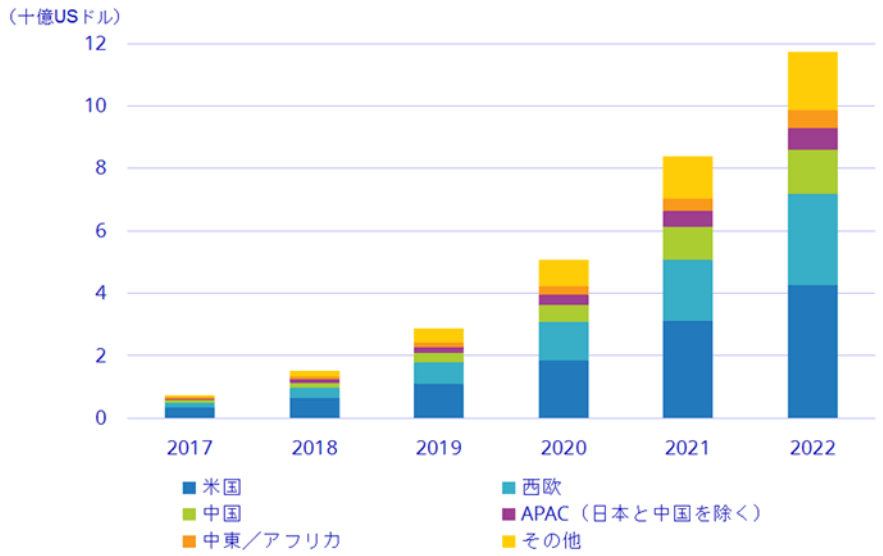
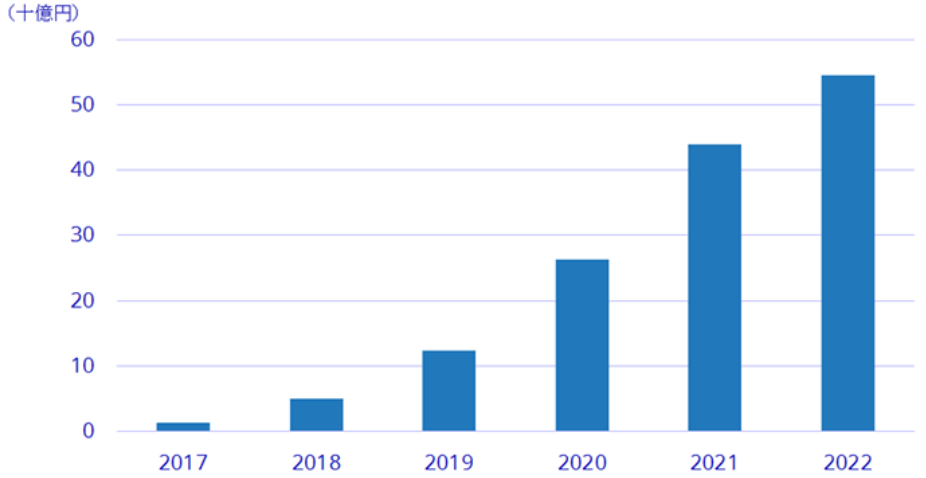


図1　ブロックチェーン市場 支出額予測 （主要地域別）、2017年～2022年
Note: 日本は「その他」に含まれる

国内市場動向

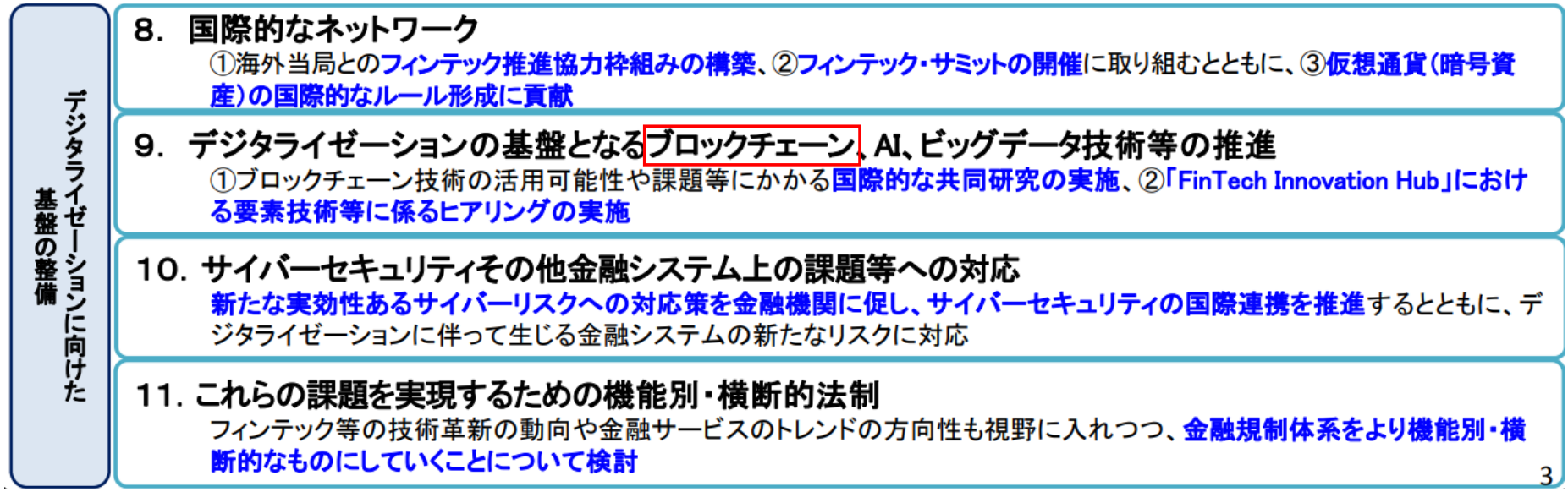


（参照）: IDC 「Worldwide Semiannual Blockchain Spending Guide」 2017H2, 9/2018

取り組む必要性(2/2)

- 金融庁の【金融デジタライゼーション戦略の11の施策】においてもデジタライゼーション基盤としてのブロックチェーン技術の活用推進が謳われております。
- https://www.fsa.go.jp/policy/Summary_of_For_Providing_Better_Financial_Services.pdf

金融デジタライゼーション戦略の11の施策におけるブロックチェーンの位置づけ



（参照）:金融庁「変革期における 金融サービスの 向上にむけて」, 9/2018

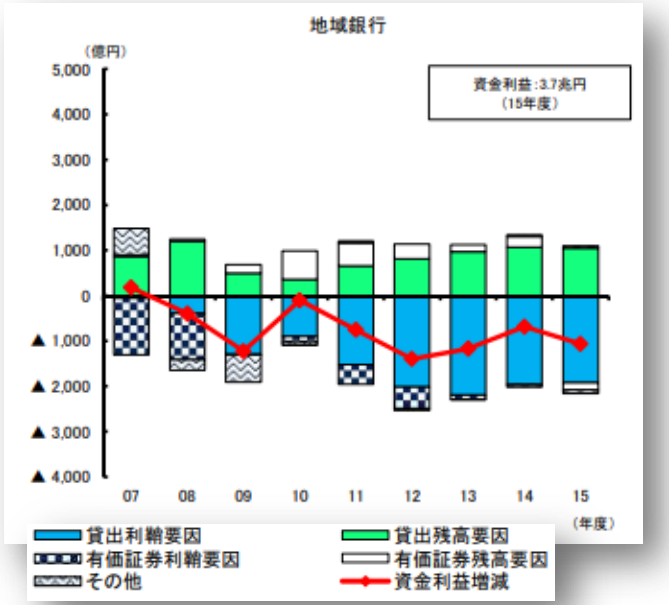
■ １１の施策の中では、「顧客情報の信頼性担保」や、「金融・非金融の情報伝達を可能にする金融インフラのデジタル化」へのブロックチェーン活用にも言及。こういった環境整備の必要性に加え、「既存の金融機関も、新しいプレイヤーとの協働・連携や競争を通じて、ビジネスモデル変革による利用者利便の向上が求められている」と述べている。

何から取り組むか (1/4)

- 金融庁のレポートでは、今後の地域銀行の役割として、顧客本位の良質な金融サービス提供による企業価値向上によって安定的な収益確保を目指す「共通価値の想像」を掲げています。
- 企業側も、銀行には金利の低さより企業の事業理解といった事業性評価に基づいた経営支援を求める傾向にあります。
- https://www.fsa.go.jp/news/28/20161021-3/01.pdf

金利低下による資金利益の低下

既存ビジネスモデルの限界
「貸出が緩やかに増加しているものの、国内の金利水準の低下を受けた貸出利鞘の縮小によって、資金利益は減少が続いている」※注

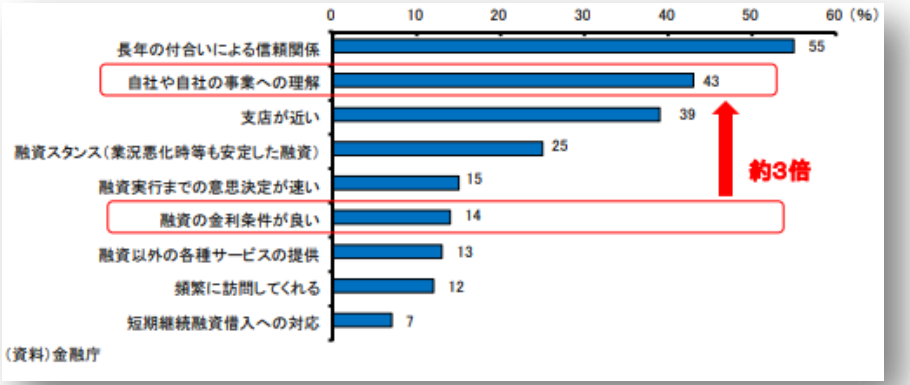


※注 (参照):金融庁「金融レポート」, 9/2016

企業の銀行に対するニーズ

金利の低さより事業理解を求める
企業は「融資の金利条件」以上に、「自社や自社の事業への理解」等、企業に寄り添う姿勢を重視する傾向にある

企業がメインバンクに求めるもの



(参照):金融庁「金融レポート」, 9/2016

何から取り組むか (2/4)

ブロックチェーンは将来的に、革新的な社会インフラ創造の可能性を秘めています。一方で、新しい技術の為、Harverd Business Reviewでは『ほとんどの企業にとっては、まず「単体での利用」から始めてみるのが一番簡単』と述べています。

ブロックチェーン活用のステップ例

比較的取り組みやすい領域

ブロックチェーン活用領域の分類

既存の枠組み改革へのチャレンジ

	変革的な活用
代替的な活用 • 決済インフラ • 銀行勘定系等	• 業界間連動 • 取引の自動化 等
単体での活用 • 社内情報管理 • 事務サービス • 決裁手続き等	**局地的な活用** • 社内コイン • 地域限定通貨 • シェアエコ等

縦軸：高 ↑ 複雑さ・調整作業量 ↓ 低
横軸：斬新さ → 高

技術応用可能性へのチャレンジ

STEP1 限定的な業務領域での実験的な活用

- 主に非IT化の社内業務へ活用して実現性や有用性を実感

STEP2 技術を応用して、特定領域における新サービスへ活用

- スマートコントラクト等を用いて更なる可能性を追求
- 主に既存業務が存在しない領域(社内コイン 等)での活用

事業性評価への活用領域

STEP3 既存の基幹システムや社会インフラへの代替的な活用

- 既存業務を踏襲しつつ、基幹業務・インフラを代替して更なる堅牢化・効率化に寄与
- 証券・資金決済基盤や主要産業の基幹業務等、成熟した規制・業務の改革を伴う活用

STEP4 社会のあり方を大きく変える革新的サービスへの活用

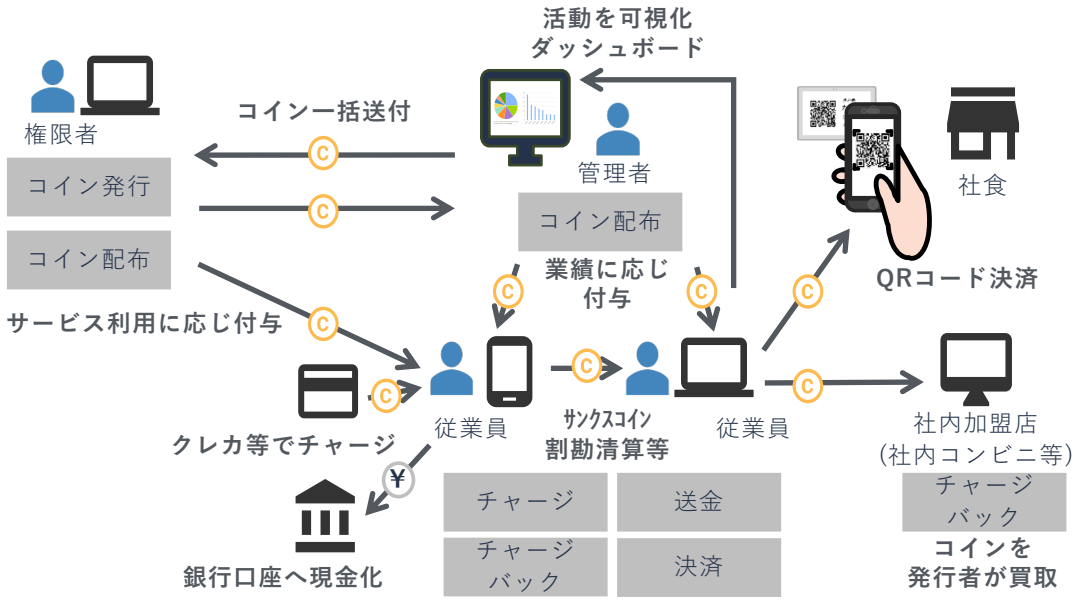
- 技術の更なる応用を前提とし、全く新しいサービスやインフラを創造
- 製造・販売・決済の各基盤が自動連動してサービスが自動化される社会の実現
- スマートコントラクト等により人の介在なく自律的に運営される企業・インフラの創造

(参照) :Harverd Business Review「ブロックチェーンと企業戦略」,7/2017を基にbitFlyerが作成

何から取り組むか（3/4）：1st ステップ

- 将来の事業の卵となる技術基盤として「コインによる価値流通基盤」は、あらゆるサービスを提供する上で必要となるため、1stステップの有力な候補の１つとなり得ます。
- 例えば、貴社内での社内コイン活用の実証実験が取り組みやすいと考えます。

事業の卵となる技術基盤の例（法人向け社内コイン）



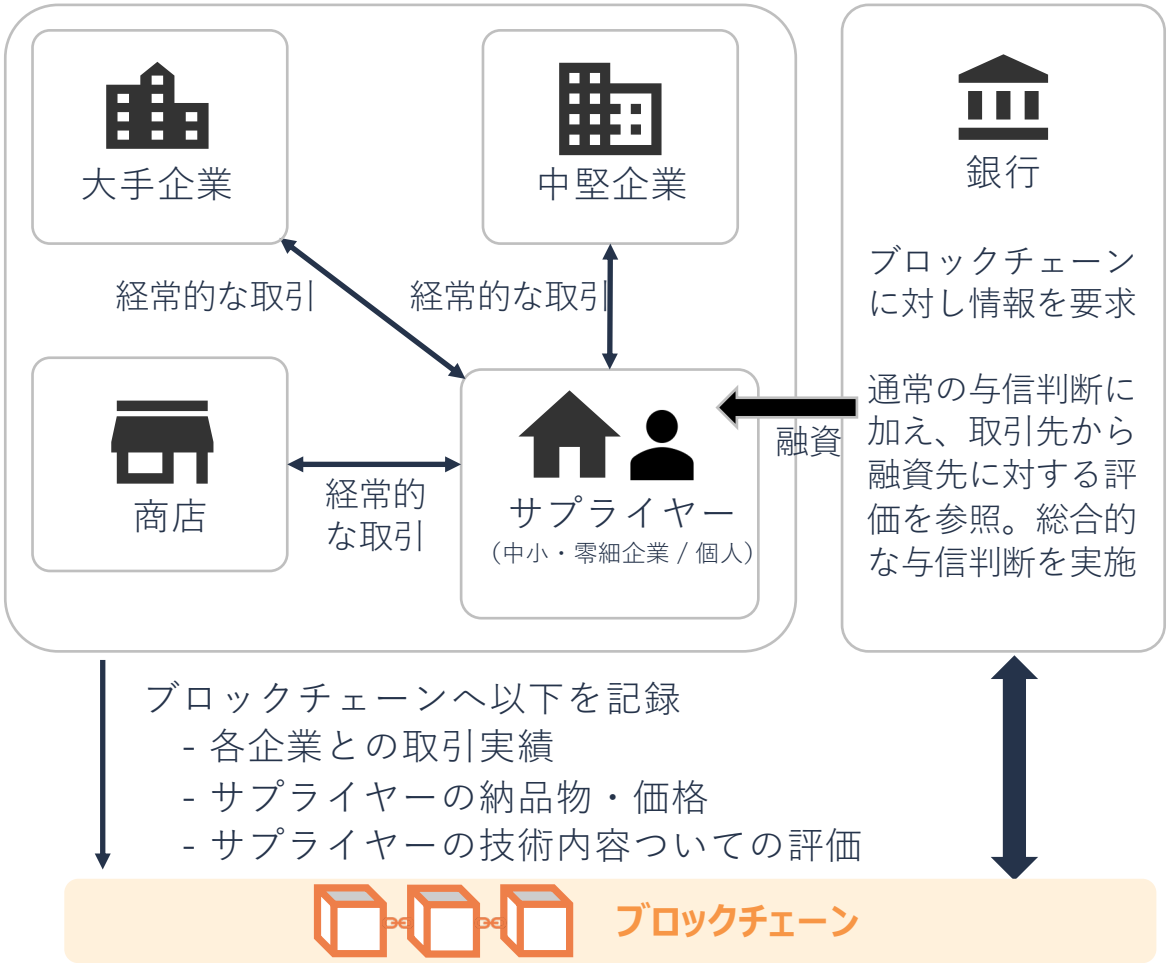
サービス概要	■ 社内コインを生成 ■ 給与以外のインセンティブコインを業績や行動に応じて付与 ■ 付与されたコインは社食等で利用可
対象顧客	■ 営業等、定量的な業績評価ができる従業員を雇用する企業 ■ 健康経営・働き方改革等推進企業
提供価値	■ 企業内の従業員へのインセンティブによる行動の促進（業績向上・自己啓発促進・ルール順守・離職防止など）
実現方式	■ 中央集権的管理者不在でも信頼性を確保したまま、組織横断取引がスマートコントラクト(条件付きプログラム)を用いて実現できる

■ 将来的に、融資先の企業の活動情報を収集し、与信や経営コンサルティングに活用することで、事業性評価の推進に活用するなども検討が可能です。

何から取り組むか (4/4)：事業性評価への活用

中小・零細企業または個人が、信用力のある企業と取引をした履歴をブロックチェーン上に記録します。
このデータを信用力とし、融資に活用することが可能と考えられます。

サプライヤーとの取引実績・技術力を生かした融資例



導入のメリット例

銀行

- 決算内容というある一時点の評価だけではなく**技術力・競争力などを測ることが一定程度可能**
- **与信コストの削減・与信の拡大化の可能性**
- 事業性評価に基づいた経営支援やサービス化

サプライヤー

- 過去の実績に基づいて**与信条件が良くなる可能性あり**
- 決算内容がよくない場合でも、**別の評価基準として信用力補完が可能**

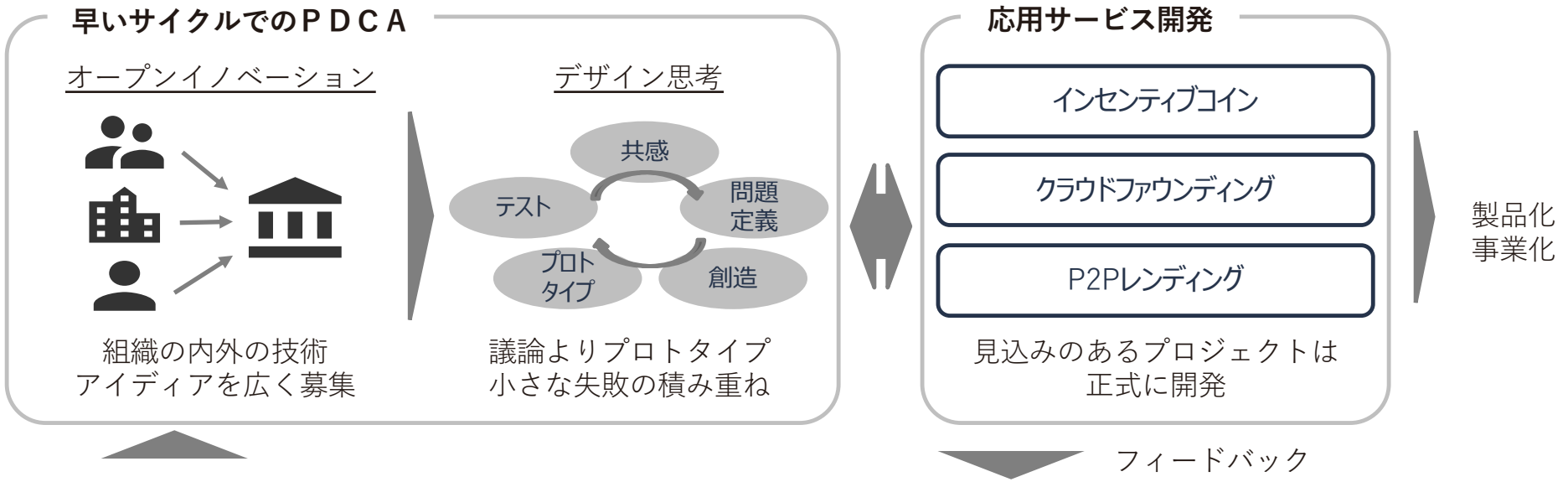
取引企業

- 支払条件緩和以外で、**サプライヤーへの信用力補完に貢献**
- サプライヤーとの関係強化につながる可能性

どのように進めるか (1/2)

- 長期間の検討と多額のコストを要する従来のIT投資とは異なり、新しい技術の活用には 「事業の卵となる技術基盤」の上で幅広いアイディアを募り、プロトタイプによる「早いサイクルでのPDCA」を回すことが有効と考えられます。

早いサイクルでPDCAプロセス例



事業の卵となる技術基盤例

ブロックチェーンを活用したコインによる価値流通基盤

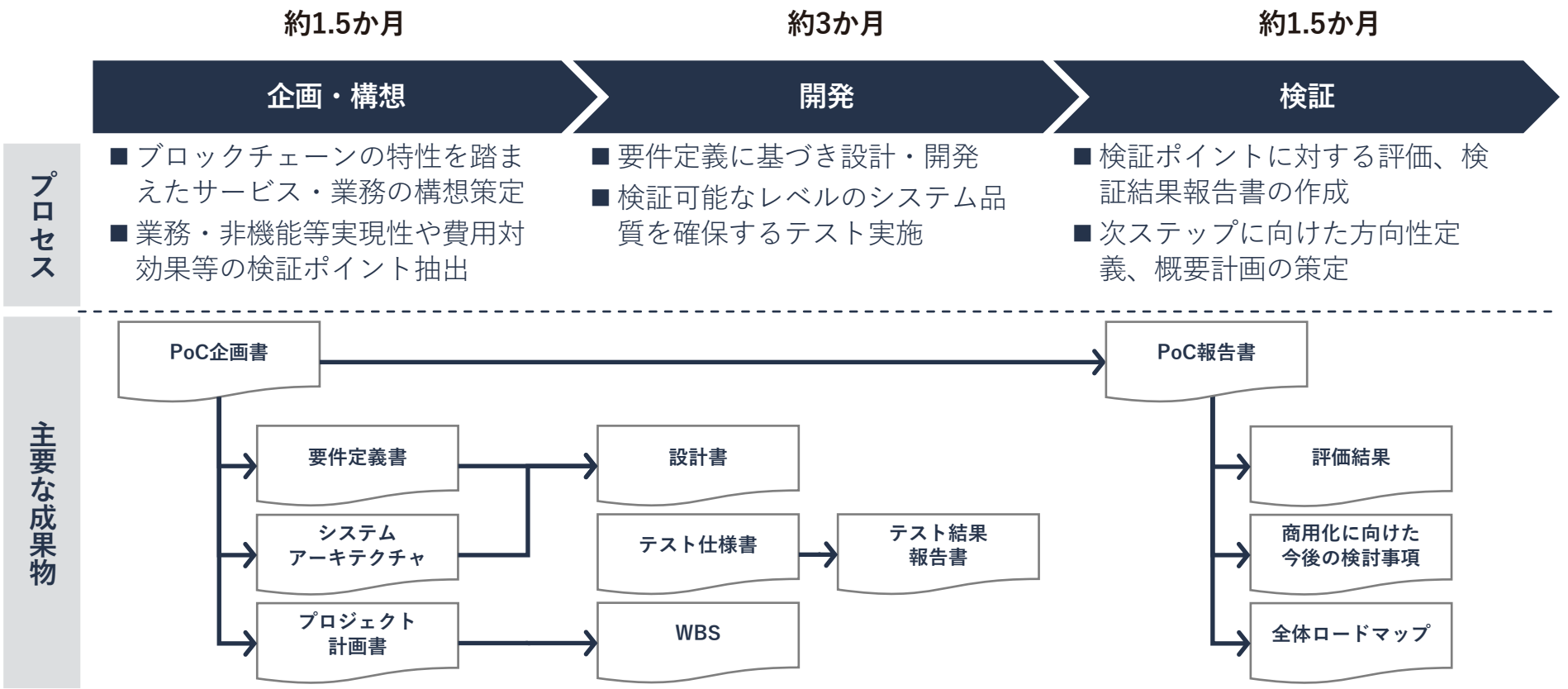
コイン発行 | コイン配布 | 送金 | 決済 | チャージ チャージバック

どのように進めるか (2/2)

- プロジェクトは、サービス構想の企画書作成から、システム開発・実証実験を行い、結果報告まで原則４～6か月程度で実施します。

※プロジェクト内容等により長期間にわたる場合もあり得ます。

ブロックチェーン実証実験プロセス

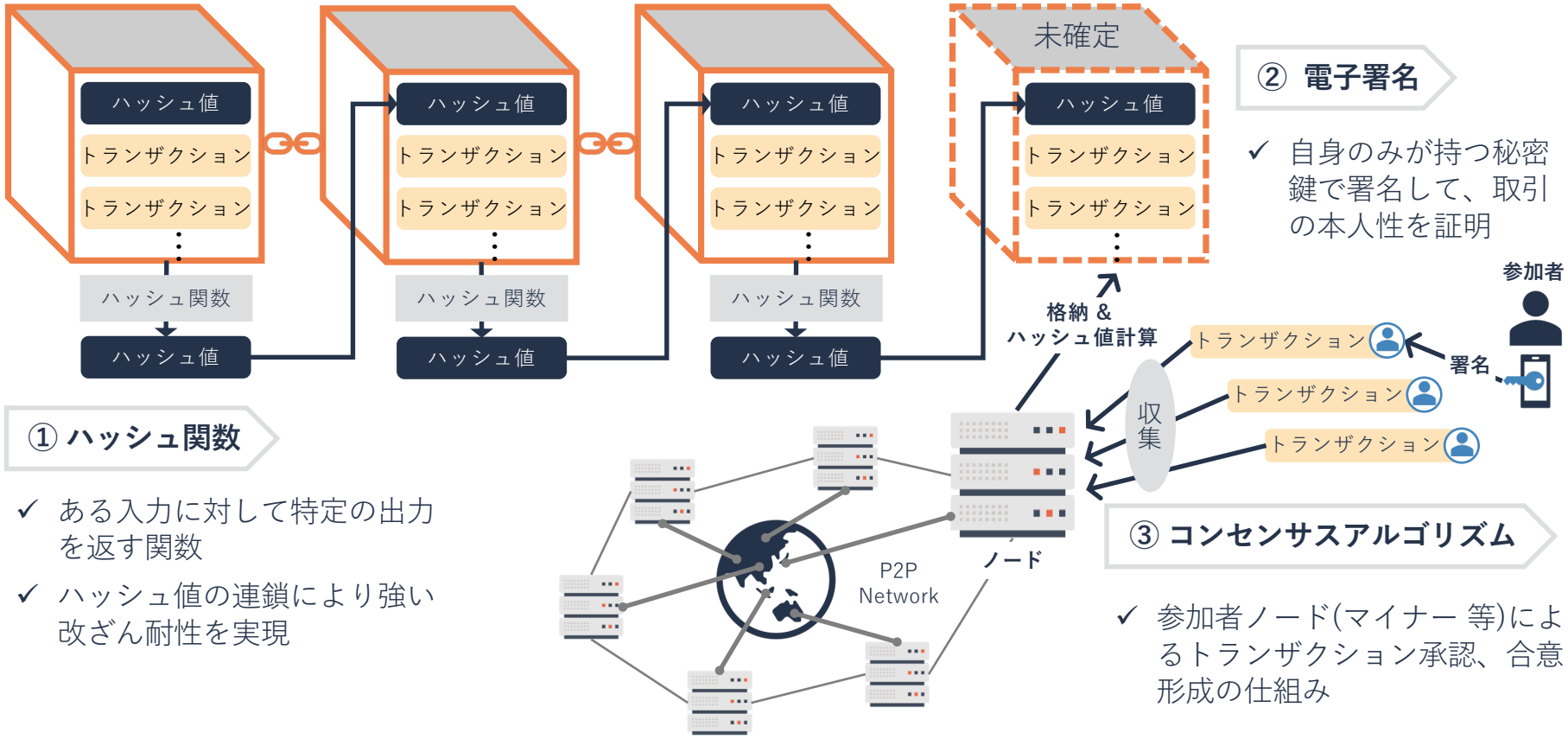


Appendix

ブロックチェーンの技術要素 (1/4)

ブロックチェーンは特定の管理者を介さずに、不特定多数の参加者がセキュアに取引可能な革新的なテクノロジーです。

ブロックチェーン技術要素の全体像



① ハッシュ関数

- ✓ ある入力に対して特定の出力を返す関数
- ✓ ハッシュ値の連鎖により強い改ざん耐性を実現

② 電子署名

- ✓ 自身のみが持つ秘密鍵で署名して、取引の本人性を証明

③ コンセンサスアルゴリズム

- ✓ 参加者ノード(マイナー 等)によるトランザクション承認、合意形成の仕組み

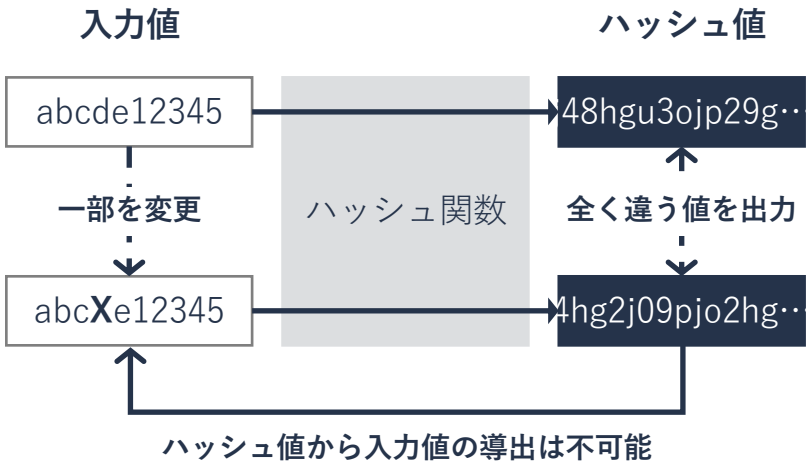
ブロックチェーンの技術要素 (2/4)

ハッシュ関数で得られるハッシュ値により、各種の改ざんを検知可能となります。

① ハッシュ関数

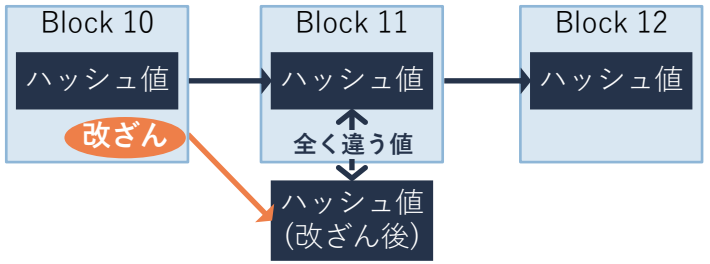
■ **ハッシュ関数**とは、ある入力に対して特定の出力を返す関数

- ハッシュ関数の出力値(ハッシュ値)は、入力値の長さに関わらず固定長 (128bit／160bit 等)
- ハッシュ値はダイジェスト／要約値と呼ばれる



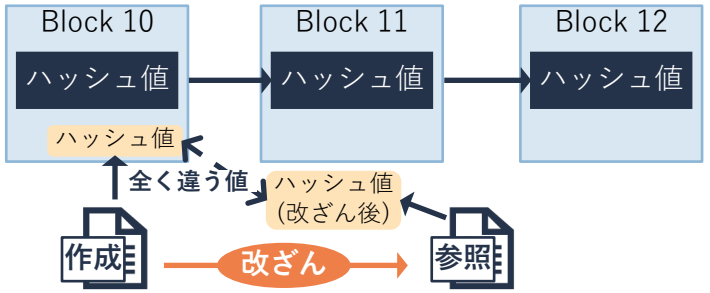
ハッシュ関数(ハッシュ値)は改ざん検知に効果を発揮

ブロック内容の改ざん



✓ ブロック内容が改ざんされると続くブロックのハッシュ値が変わるため、検知が可能

ローカルデータの改ざん



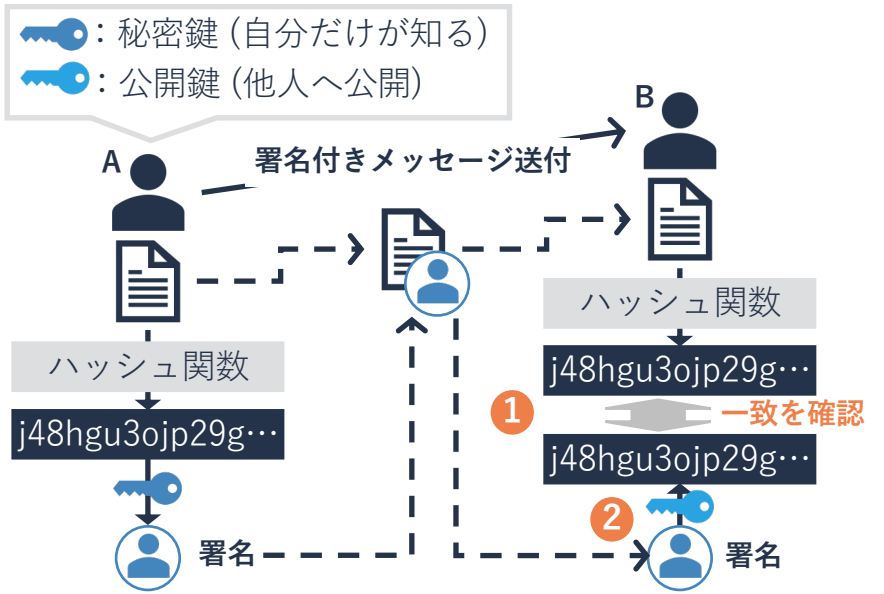
✓ 文書等のハッシュ値をブロック格納することで、参照時に改ざんがないかの検証可

ブロックチェーンの技術要素 (3/4)

個々のトランザクションには電子署名が付与されるため、取引の本人性を確保できるうえ、細かな単位でトレーサビリティを得ることができます。

② 電子署名

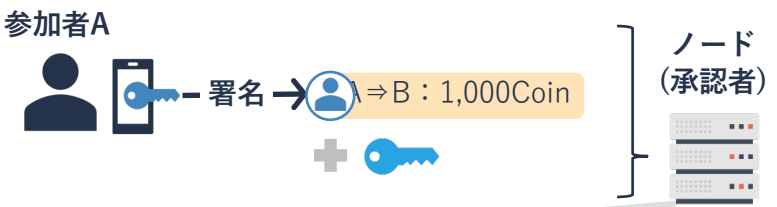
- **電子署名**とは、メッセージの本人性と完全性(改ざんされていないこと)を証明する仕組み
- 送信者の秘密鍵で行われた署名は、対となる公開鍵でのみ検証が可能



1. ハッシュ値が不一致 ⇒ メッセージ改ざんあり
2. ハッシュ値を得られない ⇒ 不正な秘密鍵による署名

電子署名は取引(トランザクション)の本人性を証明

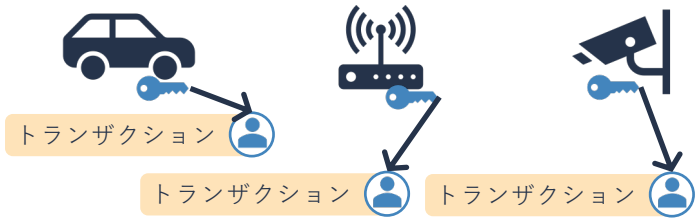
トランザクションの署名



ノードはAの公開鍵を用いてAの署名を検証し、確かに本人による取引であることを確認

秘密鍵紛失・盗難による影響大（厳重な管理要）

様々な署名の主体



✓ デバイスが署名を行うことで、デバイス単位でデータ生成主体・内容等をトレース可能

ブロックチェーンの技術要素 (4/4)

ブロックチェーンにおける大きな発明であるコンセンサスアルゴリズム例は、ビットコイン(PoW)の出現以来、その弱点を補う形で進化を続けています。

③ コンセンサスアルゴリズム

種類	説明	特徴	利用ケース	
PoW (Proof of Work)	■ 膨大な計算リソースによる取引承認 (マイニング) ■ ブロック生成は全ノードが可能	■ 改ざん耐性は極めて高い ■ コンピュータリソース無駄遣い ■ 可用性は極めて高い	bitcoin	パブリック・ブロックチェーン*1
PoS (Proof of Stake)	■ Coin保有量・期間が大きいノードはマイニング成功率UP ■ ブロック生成は全ノードが可能	■ Coin長者による改ざんリスク有 ■ リソース無駄遣い改善・高速化 ■ 可用性は極めて高い	ethereum * 現段階ではPoWだが、PoSに変更される予定	
PoI (Proof of Importance)	■ Coin保有量・期間+使用頻度大のノードはマイニング成功率UP ■ ブロック生成は全ノードが可能	■ PoSの特徴に加え、「Coin長者がマイニングで有利となるためCoinを溜め込む」懸念を排除	nem	
PBFT (Practical Byzantine Fault Tolerance)	■ 特定ノードにブロック生成権限を集中。当該ノードの合議(2/3以上の承認)でブロック生成	■ 取引承認機関への信用が必要 ■ 権限を一部ノードに集中させることで、承認時間を更に短期化	HYPERLEDGER	プライベート・ブロックチェーン*2
Paxos	■ 特定ノードの合議制 (PBFT同様) ■ ブロックの生成には過半数以上のノードの承認が必要	(PBFTと同様)	Google Chubby	

*1：不特定多数が誰でも参加可能であり、全参加者がブロック生成(取引承認)の権限を持つブロックチェーン
*2：参加者は原則許可制であり、ブロック生成権限はその中でも限られた参加者にのみ与えられるブロックチェーン

技術の応用 ~ スマートコントラクト (1/3)

イーサリアムで初めて実装されたスマートコントラクトは、ブロックチェーン上で条件付き処理(プログラム)を自動実行させるための仕組みです。

スマートコントラクトとは

定義

- 契約[*1]をプログラムで表現し、自動実行させること
- 概念自体は古く、自動販売機が初めての導入事例と言われる
  - 「ジュースの代金を投入」「ジュースのボタンを押下」の2つの条件が揃うとジュースが自動的に出力

特徴

- スマートコントラクトをブロックチェーンに分散することで、契約の内容・実行結果を参加者間で検証可能
- これまでの、Coinの移転という単純なものから、より柔軟・複雑なサービスをブロックチェーン上で表現可能に

スマートコントラクトの基本プロセス

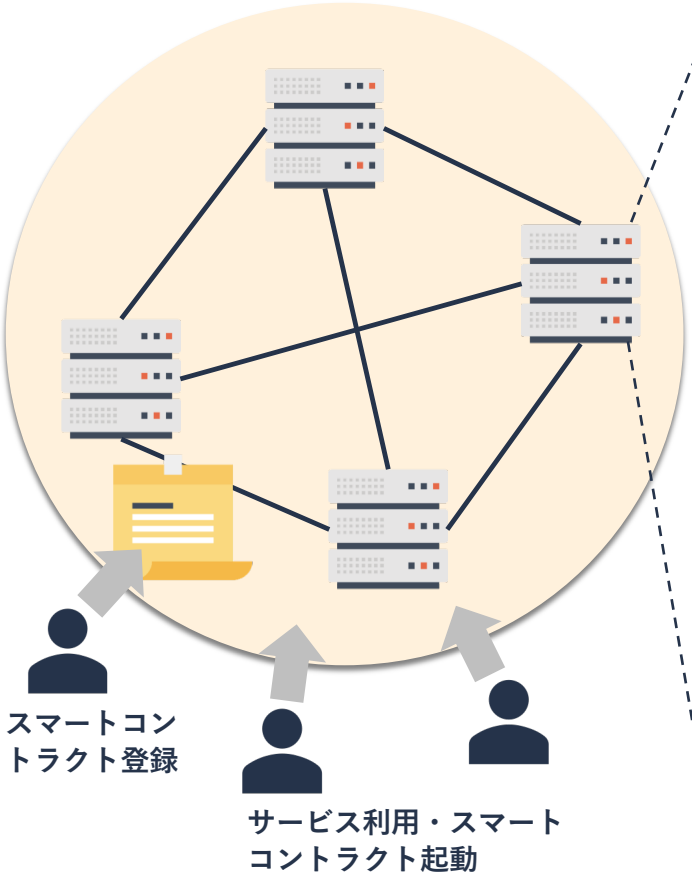
- ✓ 契約内容(条件の組み合わせ)をプログラムで定義
- ✓ モニタリングし、条件が揃うと契約実行
- ✓ 契約内容に基づく処理を自動実行
- ✓ 現物資産が絡む場合はブロックチェーン外での決済を経て取引が完結

*1：スマートコントラクトにおける「契約(コントラクト)」とはプログラムのことであり、本用語の一般的な意味合いである「法的な拘束力を持つ当事者間の合意」を指すものではない

技術の応用 ~ スマートコントラクト (2/3)

スマートコントラクトは分散ノード上のブロックチェーンに組み込まれることで、コントラクトによる処理結果の正しさを含めてノード間での相互検証が可能となります。

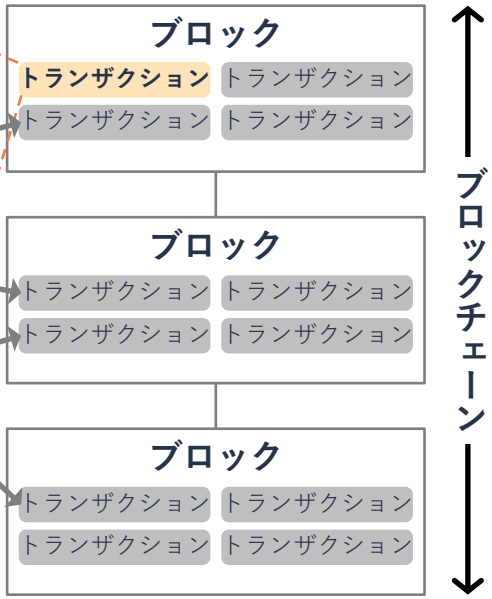
— ブロックチェーン・ネットワーク —



各ノードにおける動作

スマートコントラクト
（プログラム例）

- **コントラクト1：**参加者が100名に達したら各人に1000Coinを発行
- **コントラクト2：**各ユーザ、100Coin利用毎に1Coinを追加付与
- **コントラクト3：**Coinの利用可能期間は2018/1/1～2018/12/31
- **コントラクト4：**2019/1/1、全ユーザーのCoinをユーザーXに送金

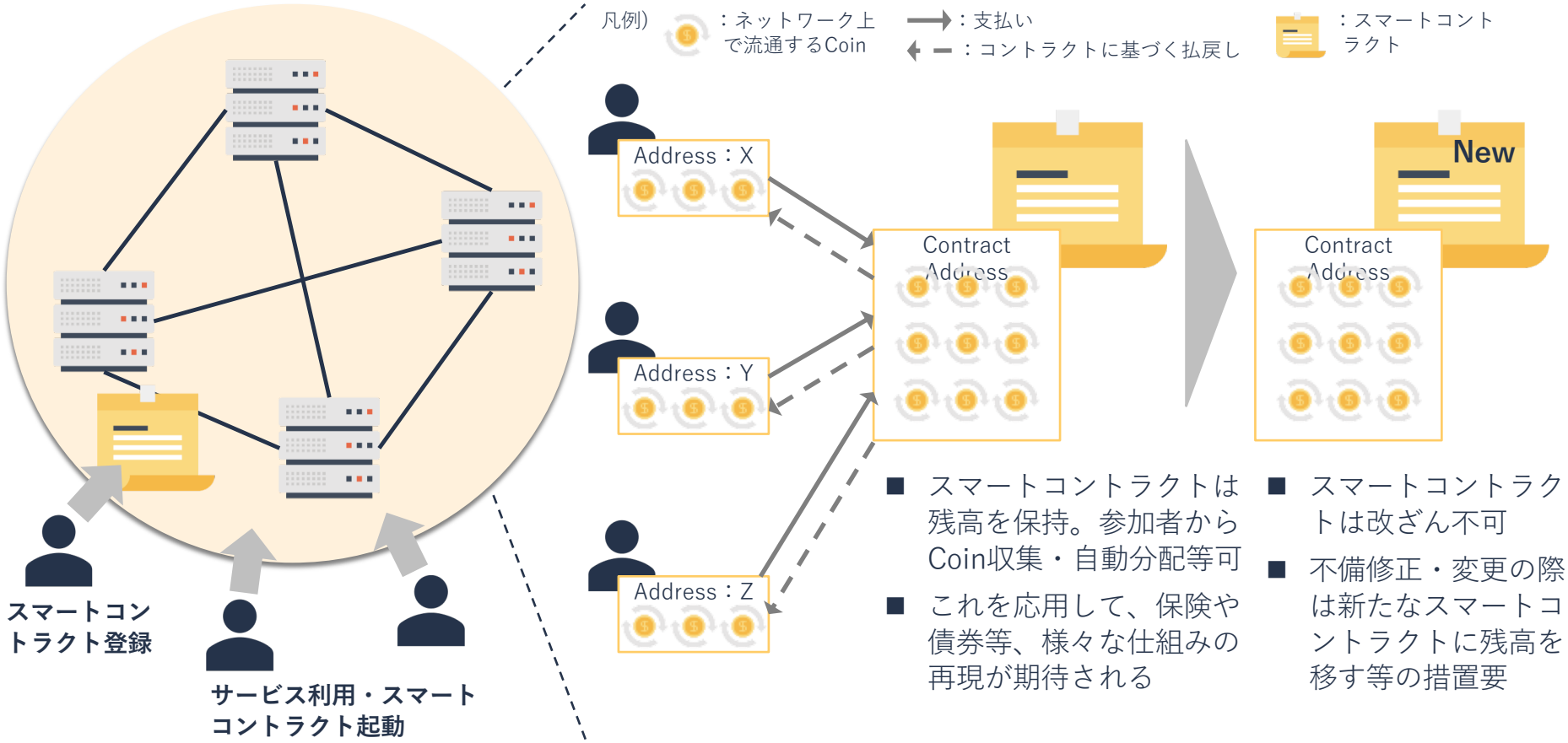


- スマートコントラクトはトランザクションとしてブロックチェーンに組み込まれ、ノード全体に共有
- ビジネス要件に応じて様々なコントラクトを自由に定義可能

実行結果の正しさは、分散ノードが相互に検証・合意

技術の応用 ~ スマートコントラクト (3/3)

スマートコントラクトには残高を持たせることができるため、参加者から集めたCoinを一定のルールで配分する等、様々な仕組みを表現することが可能です。



- スマートコントラクトは残高を保持。参加者からCoin収集・自動分配等可
- これを応用して、保険や債券等、様々な仕組みの再現が期待される

- スマートコントラクトは改ざん不可
- 不備修正・変更の際は新たなスマートコントラクトに残高を移す等の措置要


bitFlyer