



ブロックチェーン技術における国際競争力強化

一般社団法人日本ブロックチェーン協会 会員
デロイトトーマツ コンサルティング合同会社

2016年4月20日

ブロックチェーンの定義

ブロックチェーンは、P2Pの分散型データベースであり、かつ、コンセンサス・アルゴリズムを備えていると定義できます。

P2Pの分散型データベース であること

- P2Pの分散型データベースとは、複数のコンピューターにデータを分散し、相互に通信を行うことで運営されるデータベース
- 管理は煩雑になるものの、信頼性の向上、負荷分散が可能
- 国境をまたぐプラットフォームを構築する方がより安定して稼働する可能性あり

コンセンサス・アルゴリズム を備えていること

- コンセンサス・アルゴリズムとは分散型合意形成のことで、正式なトランザクションの認証を得るためのプロセス
- ネットワーク上には、虚偽の情報を伝える者がいる中で正しく合意形成できるかという問題(ビザンチン将軍問題)を仕組みとして解決する必要あり

ブロックチェーンの機能特性

ブロックチェーンは、高透明性、高信頼性、高効率性という特性を持つ一方で、処理速度等の課題もあるため、現時点では、研究開発が必要となっています。

高透明性

- 承認されたデータは全ての参加者が同時に参照可能
- 一度合意したデータが遡及的に変化しない(改ざんできない)

高信頼性

- 一部のノードが故障しても、他のノードが生存している限り応答し続ける
- ノード間のネットワークが障害等で分断されても、システムがダウンしない

高効率性

- 処理分散によるシステムコスト低減
- 障害時のメンテナンスコスト低減
- 契約・決済を扱う業務のスピードアップ・事務コスト低減 等



処理速度、セキュリティの面での課題もあるため、今後、更なる研究を重ね、課題を解消する必要性あり

ブロックチェーンに関する動向(1/3)

～グローバル

欧米金融機関では、ブロックチェーンに関する研究が盛んになってきており、世界的に注目されているIT技術となっています。中でも、R3CEVの取組は注目すべき動きと思料します。

金融機関	取組概要
R3CEVと 大手43銀行	<ul style="list-style-type: none"> ブロックチェーン技術を有するR3CEVと、日米欧の43行が共同し、コンソーシアムを結成、 ブロックチェーンによる金融システム構築に必要な業界標準規格制定、共有プロトコルの研究開発を実施中 日本からは、三菱UFJフィナンシャルグループ、みずほフィナンシャルグループ、三井住友銀行、野村ホールディングス、SBIホールディングスが参加
Linux 財団	<ul style="list-style-type: none"> 非営利団体Linux財団と、日米欧の銀行・Sler・ベンチャー企業が共同し、プロジェクト「Hyperledger」を立ち上げ オープンソースでのフレームワーク開発やアプリケーション開発を実施中 日本からは、三菱UFJフィナンシャルグループ、富士通、NEC、日立製作所、NTTデータが参加
CME・ロンドン 証券取引所等	<ul style="list-style-type: none"> CMEグループ、ロンドン証券取引所、ユーロクリア、LCHクリアネット、ソシエテ・ジェネラル、UBSが共同し、ポスト・トレードにフォーカスを焦点を当てた検討を実施中
NASDAQ	<ul style="list-style-type: none"> ブロックチェーン技術を用いた未公開株式取引システム「Nasdaq Linq」を発表 「Nasdaq Linq」は、非上場の会社の未公開株を従業員が売買できる場となっており、現在、米国の6社が利用中 ブロックチェーンでの株主の議決権行使システムも検討中
Goldman Sachs	<ul style="list-style-type: none"> ブロックチェーンを活用した資金決済および証券決済を行うシステムであるSETLcoinを開発、米国特許を出願 自社での研究開発に加え、米有カブロックチェーン企業Digital Asset Holdings等、ブロックチェーン関連企業への出資も実施
ドイツ銀行	<ul style="list-style-type: none"> ブロックチェーンおよび暗号技術を用いた分散台帳は、より広範的なアプリケーションを構築できる可能性を有しており、新産業の機会を生み出し、既存の技術やプロセスを破壊する可能性を秘めているとし、ブロックチェーン技術を研究中 ブロックチェーンが活用可能な領域として、①法定通貨の支払と清算、②識別・分割・追跡可能な有価証券の発行および転送、③有価証券の配当支払、④証券決済と清算、⑤スマートコントラクトを通じたデリバティブの自動執行および清算の効率化、⑥中央管理機関を介さない資産管理、⑦マネーロンダリング監視システム、⑧当局へ透明性の高い情報の提供、を特定
VISA	<ul style="list-style-type: none"> アメリカ、シンガポールにブロックチェーンの研究開発チームを組成。インドにイノベーションラボを新設し、研究に着手予定 ブロックチェーンベンチャー企業Epiphyteと共同で送金サービスの実証実験を実施

ブロックチェーンに関する動向(2/3)

～R3CEVの取組

R3CEVの取組は、世界の名だたる金融機関が参画し、ブロックチェーンを中心とした技術の業界標準規格を導入し、かつ、ネットワーク構築することを狙いとしており、日本にとっては脅威となります。

R3CEVの取組概要

- R3CEVとは
 - ニューヨークとロンドンに拠点を置く、次世代の金融サービス技術を開発するスタートアップ
 - CEOは、ウォール街で24年間の経験をもつ、デビッド・ラター氏(インターバンク最大手:ICAPエレクトリック・ブローキングの元CEO)
- プロジェクトの狙い
 - ブロックチェーンやその派生技術の業界標準規格を検討し、金融セクターへの新技術の採用を促進しネットワークを構築すること
- パートナーシップの締結
 - グループは、セキュリティ、信頼性、効率性、スケーラビリティ、可視性の5軸から分散型元帳技術を検討し、情報の相互共有を行いつつ金融機関のための共有プロトコルの研究、実験、設計、開発を行うことを合意

参加行

- バークレイズ
- UBS
- BBVA
- JPモルガン
- クレディ・スイス
- ゴールドマン・サックス
- ステートストリート
- RBS
- バンク・オブ・アメリカ
- BNYメロン
- シティ・グループ
- ドイツ銀行
- HSBC
- モルガンスタンレー
- 三菱東京UFJフィナンシャルグループ
- ソシエテ・ジェネラル
- コメルツ銀行
- カナダロイヤル銀行
- みずほフィナンシャルグループ
- ウニクレディト・イタリアーノ
- BNPパリバ
- ウェルズファーゴ など

直近の取組状況(2016/4/5)

- 実証実験は金融業界での現実のビジネスを想定したもので、世界で最大規模の実験(加盟行43行が参加)
- 「スマートコントラクト」に焦点を当て、社債など短期資金の調達を主眼に置いたユースケースを想定し、債券の発行や二次流通、配当などの自動執行のテストを実施
- システム基盤は、「Chain」「IBM」「Intel」「Ethereum」「Eris」の協力により、AWS、Azureを利用
- 金融機関向け契約管理プラットフォームCordaを発表

ブロックチェーンに関する動向(3/3)

～国内

国内金融機関は、グローバルの動向に歩調を合わせ、システムインテグレータと共同して、決済・証券管理等への実装に向けた実証実験への取組を開始しています。

金融機関	取組概要
三菱東京UFJ銀行	<ul style="list-style-type: none">行内のみで流通する独自通貨「MUFGコイン」を実験中。スマートフォン向け決済アプリは開発済み将来的には、顧客が日本円と交換できるようにする計画
みずほフィナンシャルグループ	<ul style="list-style-type: none">電通国際情報サービス、カレンシーポート、日本マイクロソフトと共同で、シンジケートローン業務の契約事務において実証実験中。契約事務の省力化を期待富士通、富士通研究所と共同で、証券クロスボーダー取引での実証実験を実施。決済期間の短縮を期待
三井住友銀行	<ul style="list-style-type: none">国立情報学研究所と共同で、技術に関するノウハウ蓄積に取り組み将来的には、金融ビジネスへの適用、ベンチャー企業と提携しての新サービス開発を展望
静岡銀行 オリックス	<ul style="list-style-type: none">オリックス銀行、NTTデータ、NTTドコモ・ベンチャーズ、Orbと共同で、国際送金や各種決済などの金融サービス開発に向けた研究を開始
住信SBI ネット銀行	<ul style="list-style-type: none">野村総合研究所と共同で、将来の基幹・業務システム構築を目的とした実証実験を開始実装はDrangonfly FinTech社が担当
日本取引所 グループ	<ul style="list-style-type: none">日本IBMと共同で、低トランザクション市場における、ブロックチェーンの活用効果を検証する実証実験を実施(Linux財団が主導して開発を進めるオープンソースの分散台帳フレームワーク「Hyperledger」を利用)野村総合研究所、野村証券、SBI証券、三菱UFJフィナンシャルグループ、カレンシーポートと共同で、低トランザクション市場を想定した場合の、技術的な限界や可能性について評価を行う実証実験を実施

ブロックチェーンの適用可能領域

ブロックチェーンの高透明性・高信頼性・高効率性が求められる業務は多く、課題を解消できれば、適用先は広いと言えます。特に、国民生活や経済活動の基盤となる「社会インフラ」の領域については、実用化された場合、国民が幅広く技術革新の恩恵を享受することが可能になります。

ブロックチェーンの既存のユースケース

— 分類 — 金融部門 公共部門 その他部門

社会
インフラに
相当

- 送金・決済※
- 証券発行・流通・管理※
 - 株式・社債等
- 金融情報管理
 - 信用情報・自動車保険等級

※ 処理速度等の制約条件を克服することが前提

- ID管理(例:マイナンバー)
- 登記
- 公証
- 健康保険
- 投開票
- 政府調達
- 政府調査(国勢調査等)

- 物流・トレーサビリティ
- IoT

民間で
対処
すべき
領域

- シンジケートローン
- デリバティブ契約管理
- 保険金請求・支払
- 予測市場(多数の参加者の予測を基に発生確率を算出)
- 金の名義管理

- 予算開示
- 宇宙開発等大規模プロジェクト

- スマートコントラクト
- 契約管理(ワークフロー)
- 文書管理
- サプライチェーン
- デジタル資産管理
- チケット発行
- ギフトカード
- ドメイン管理

ブロックチェーン適用の効果が高いと見込まれる領域

実用化に向けて、効果や課題を明らかにするため、ブロックチェーンを適用した場合の効果が高いと見込まれる、送金・決済、マイナンバー、物流・トレーサビリティの3領域についてプロトタイプ構築を通じた研究が必要と思われます。

透明性: 参加者が内容を確認できることが必要⇒高 信頼性: システム停止時の影響が甚大⇒高 効率性: 現状高コストであるもの⇒高

分野	領域	システムに求められる要件			評価
		透明性	信頼性	効率性	
金融	送金・決済	高	高	高	A
	証券発行・流通・管理	高	高	高	A
	金融情報管理	高	中	高	B
公共	マイナンバー	高	高	高	A
	登記	高	中	高	C
	公証	高	中	高	B
	健康保険	高	中	高	B
	投開票	高	高	高	A
	政府調達	中	中	高	C
	政府調査	中	中	中	C
その他	物流・トレーサビリティ	高	高	高	A
	IoT	中	高	高	B


ブロックチェーン適用の効果や課題を明らかにするため

1. 送金・決済
2. マイナンバー
3. 物流・トレーサビリティ

についてプロトタイプ構築を通じた研究が必要

次頁以降にシステムのイメージを記載

【凡例】 A: 高い効果が見込まれる B: ある程度効果あり C: 効果は見込みにくい

: プロトタイプ構築対象

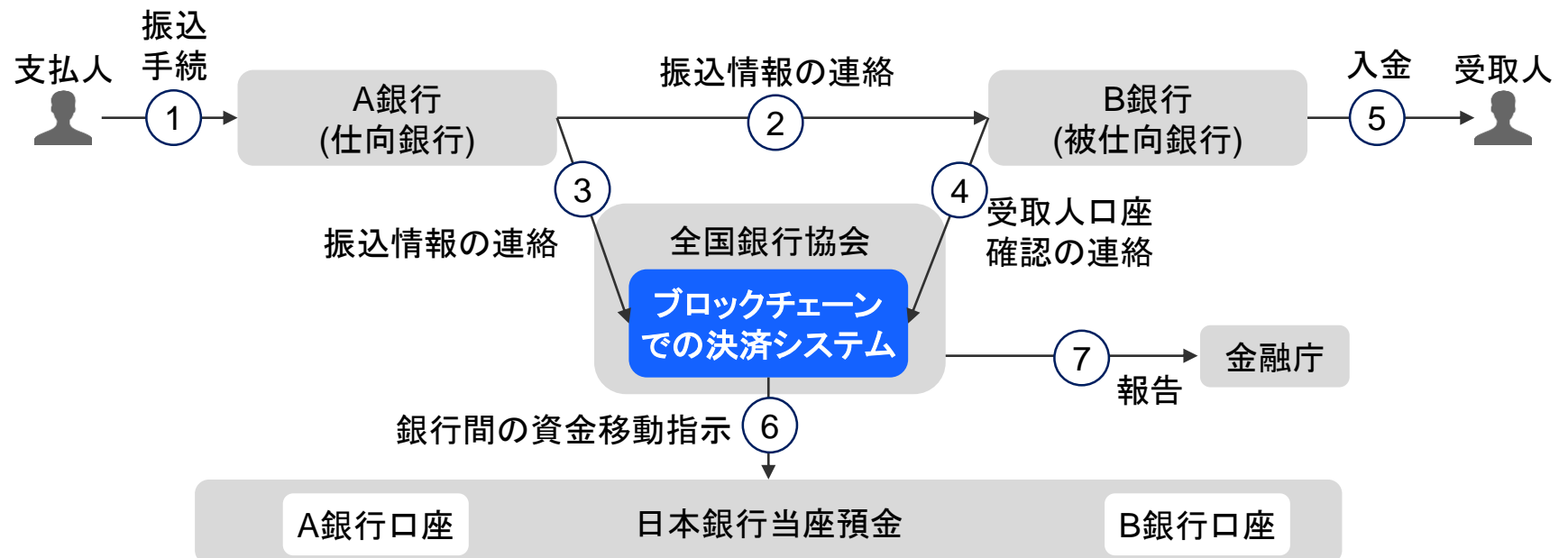
[参考]実現イメージ(1/3) —送金・決済—

決済・送金領域では、現在全銀システムが担う銀行間の決済をブロックチェーンが行うことで、機能を維持しつつ、コスト効率の高いシステム運用が実現できる可能性があります。

関係者

- 銀行 (送金・決済の執行者)
- 全国銀行協会 (決済システムの運用)
- 日本銀行 (銀行間の資金移動の実施)
- 金融庁 (取引結果のモニタリング)

ブロックチェーンにより銀行間の決済を実施



システムの概要

[参考]実現イメージ(2/3) –マイナンバー–

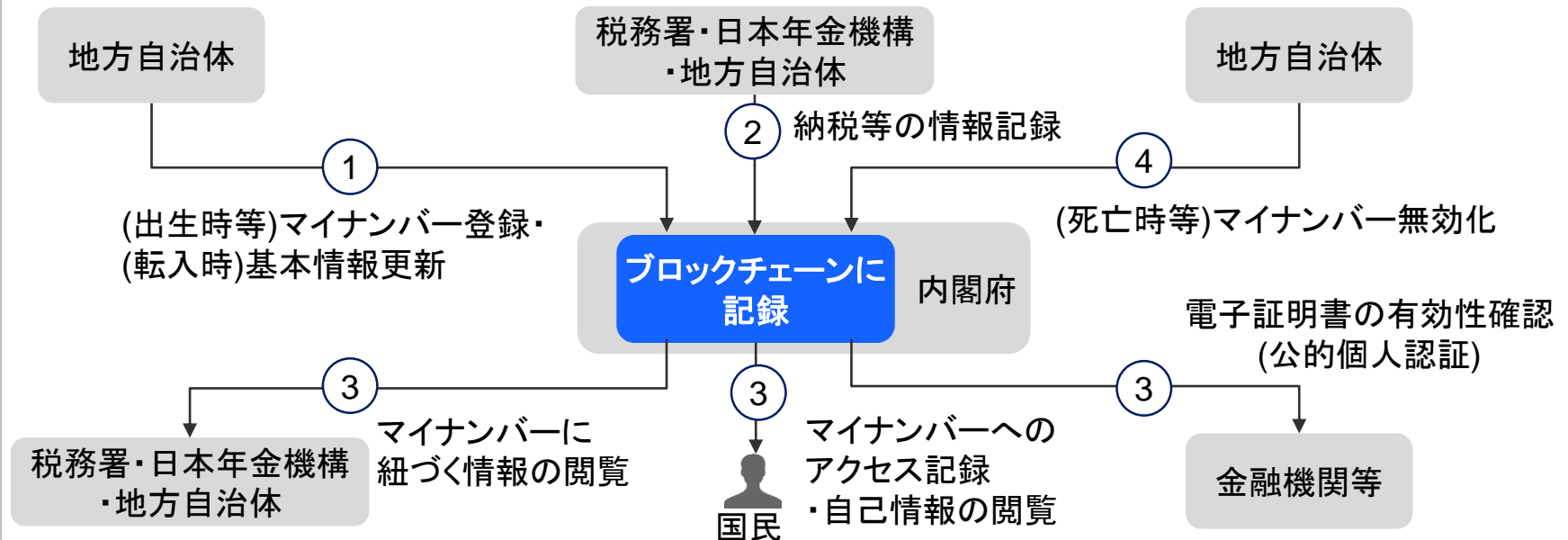
マイナンバー領域では、マイナンバーや電子証明書をブロックチェーンで管理することにより、ブロックチェーンが改ざんできないという特性を生かして、国民の情報をセキュアに管理することが可能になります。

関係者

- 地方自治体 (マイナンバーの登録・更新・無効化)
- 税務署・日本年金機構・地方自治体 (税・社会保障・災害対応の情報記録・閲覧)
- 金融機関等民間事業者・行政機関 (電子証明書を利用した本人確認の実施)
- 内閣府 (システムの運用)

マイナンバーおよび電子証明書をブロックチェーンに記録

システムの概要



[参考]実現イメージ(3/3) ー物流・トレーサビリティー

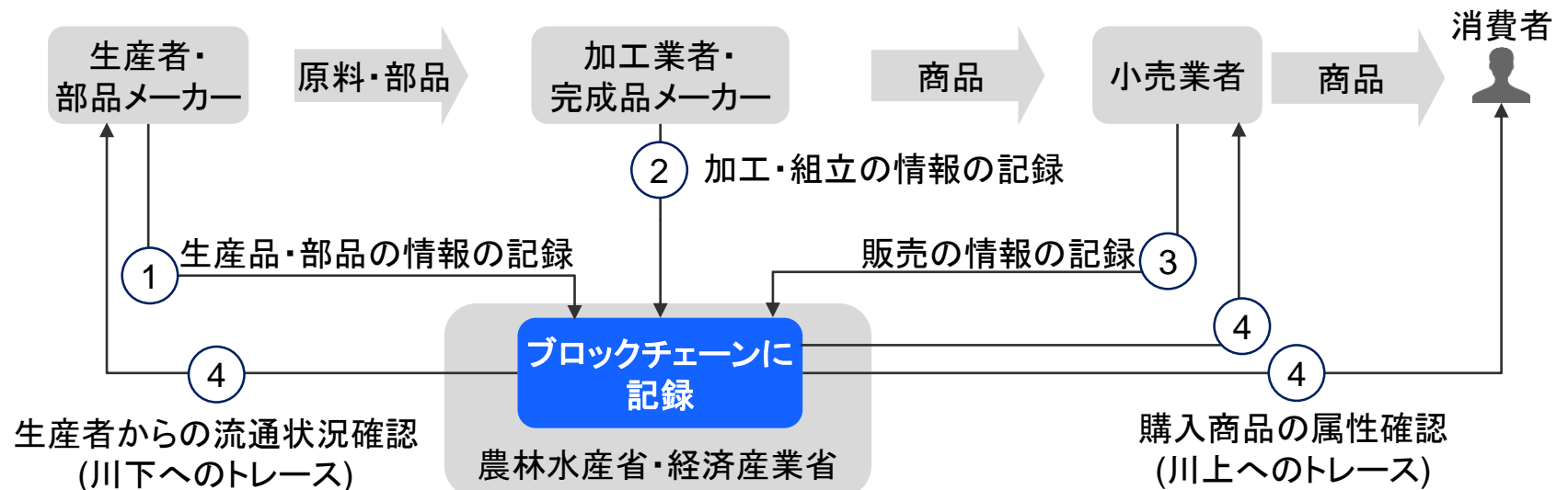
物流・トレーサビリティ領域では、食品等の生産・流通の記録をブロックチェーンに記録することで、商品の属性(川上へのトレース)および生産者からの流通の状況(川下へのトレース)の閲覧が可能となり、安心安全な消費活動が実現できます。

関係者

- ・ 生産者・部品メーカー (生產品の情報の記録)
- ・ 加工業者・完成品メーカー (加工・組立の情報の記録)
- ・ 小売業者 (販売の情報の記録)
- ・ 農林水産省 (記録システムの運用)
- ・ 経済産業省 (記録システムの運用)

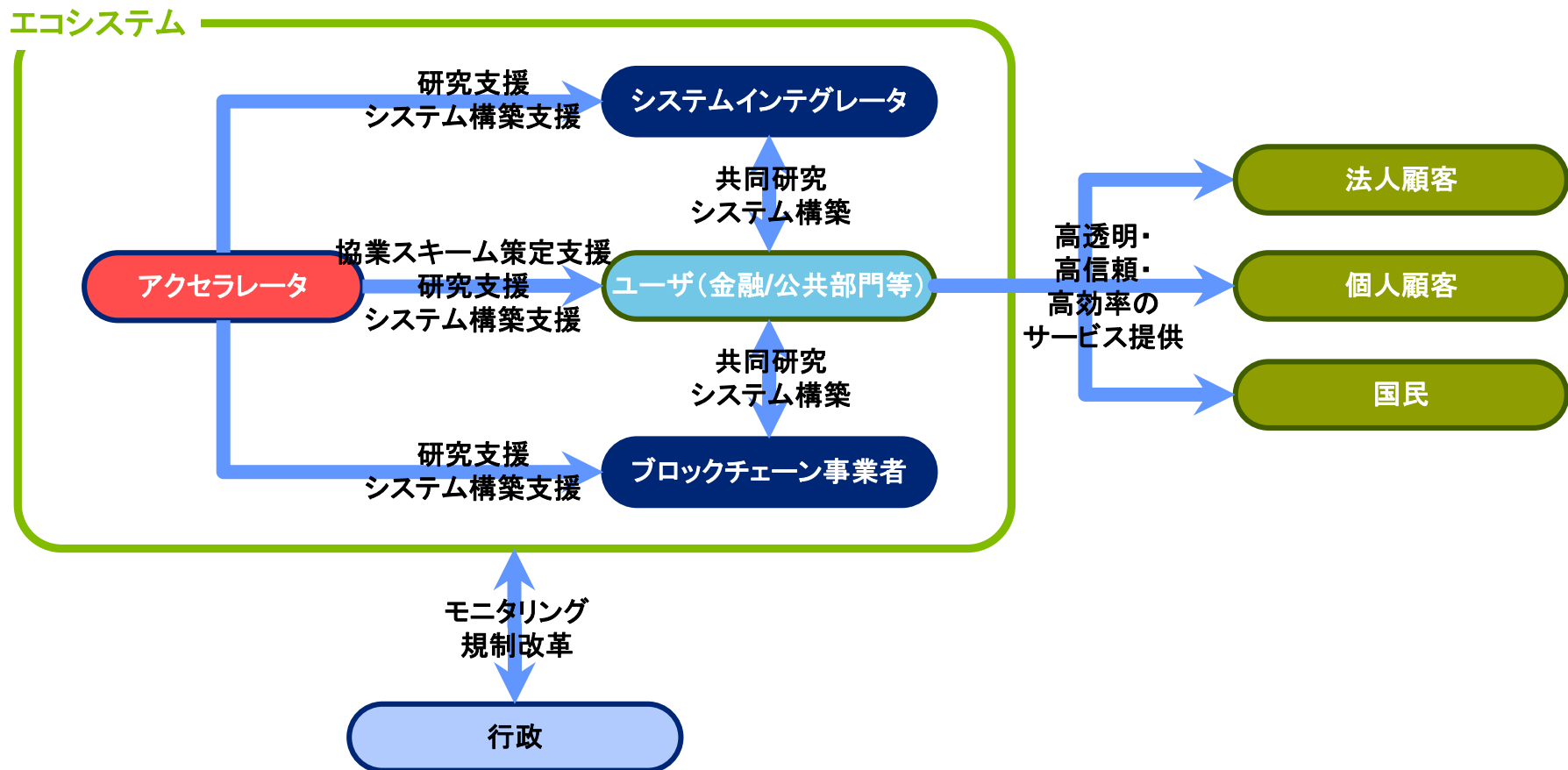
生産・加工の記録をブロックチェーンに記録

システムの概要



IT産業におけるブロックチェーンの技術開発

現状、ユーザ(金融/公共部門等)・システムインテグレータと、ブロックチェーン事業者間において、プロジェクトを進める上での垣根は高く、協業は十分ではありません。ブロックチェーンの技術開発を進め、産業化するためには、ブロックチェーン研究のためのエコシステムが必要であり、そのキーとなるのが、Win-Winの関係を創るアクセラレータとなります。



Appendix

コンセンサス・アルゴリズム

ブロックチェーンで用いるコンセンサス・アルゴリズムには、主要なもので4種類あります。

プルーフ・オブ・ワーク (Proof of Work)

- ビットコインに適用されているコンセンサス・アルゴリズム
- 宝くじを当てるようにコンピューターに無駄な計算をさせ、その結果当たったノードにブロックを生成する権利を与える方法

プルーフ・オブ・ステーク (Proof of Stake)

- コイン保有量と保有期間の掛け算で表されるコイン・エイジが大きいほど簡単にマイニングを実施することが可能

プルーフ・オブ・インポートランス (Proof of Importance)

- プルーフ・オブ・ステークを改良したもの
- 保有量に加え、ウォレットからどれだけ取引が行われているか評価

プルーフ・オブ・バーン (Proof of Burn)

- 仮想通貨を絶対に取り出せないアドレス (vanity address) に送付し、その対価として別のコインを受領



Deloitte(デロイト)は、監査、コンサルティング、ファイナンシャルアドバイザーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約225,000名を超える人材は、“making an impact that matters”を自らの使命としています。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイトトウシュートーマツ リミテッド(“DTTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2016. For information, contact Deloitte Tohmatsu Consulting LLC.