資料３

Blockchainに関する最近の**動向**

2016年6月3日

楠 正憲

本日の**構成**

- 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　**「ブロックチェーン技術を利用したサービスに関する国内外動向調査」**についてのご紹介

- Blockchainに関する**私見**
  - Blockchainを巡る**動向調査後**の動きについて
  - Bitcoinへの幻想とBlockchainに対する**過剰な期待**
  - Blockchainが情報システムに**もたらし得る影響**

「ブロックチェーン技術を利用したサービスに関する国内外動向調査」の趣旨

背景

- ビットコイン等の価値記録の取引に使用されているブロックチェーン技術は、その構造上、従来の集中管理型のシステムに比べ、
  ①『改ざんが極めて困難』であり、
  ②『実質ゼロ・ダウンタイム』なシステムを
  ③『安価』に構築可能
  という特性を持つともいわれ、IoTを含む非常に幅広い分野への応用が期待されており、**「フィンテックの次」**の注目技術である
- 我が国企業は個別に技術検証が始まった段階であり、あらゆる産業分野における次世代プラットフォームとなる可能性をもつ当該技術において、主導権を海外企業等に握られる恐れがある

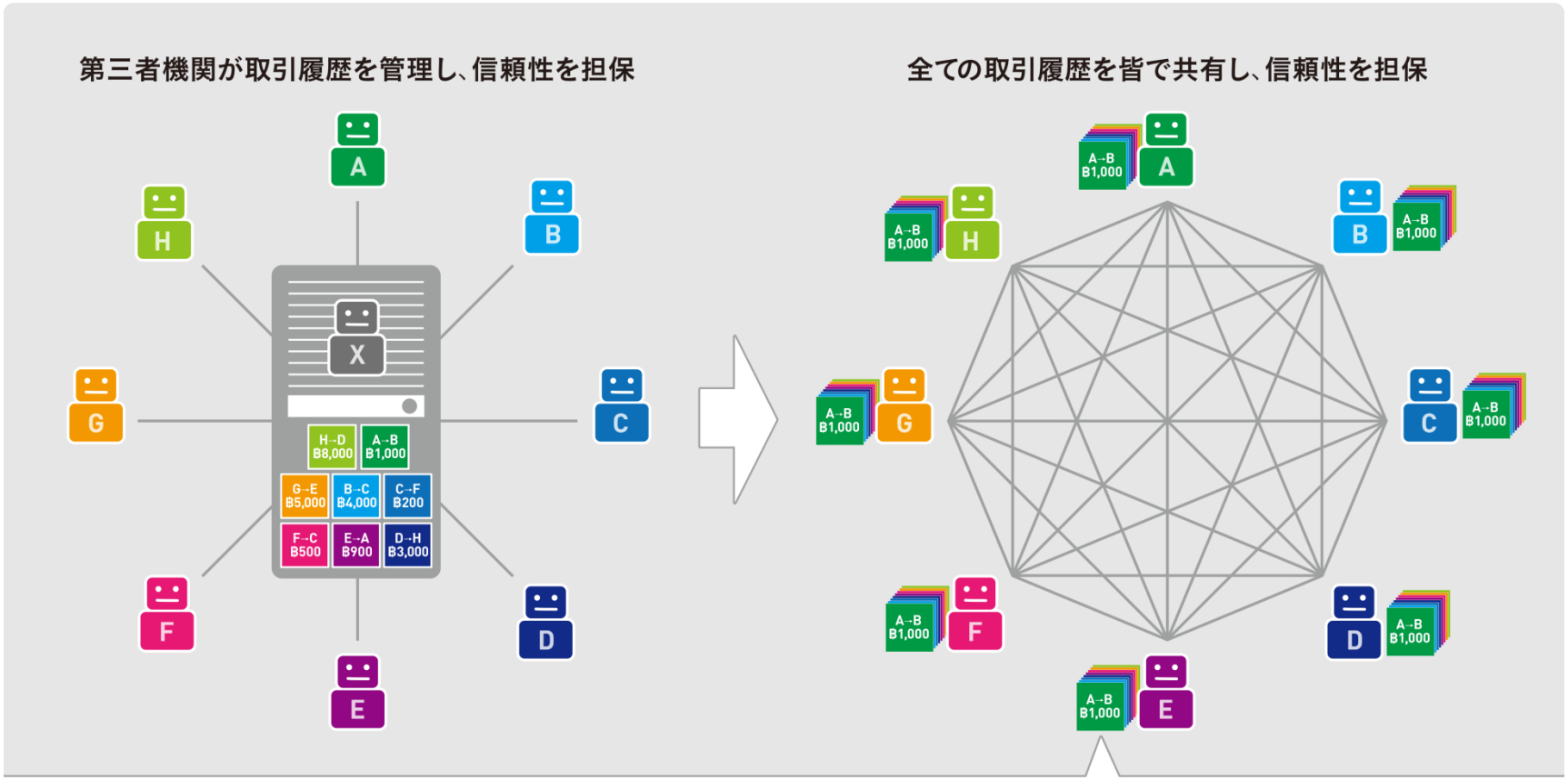
目的

- 数あるブロックチェーン技術の詳細とその優位性・課題を比較分析する。
- 当該技術が活用されるべき有望分野を把握する。
- 当該技術が社会経済に与えるインパクトを把握する。
- 今後の当該技術を用いた産業促進に向けた政策の指針を得る。

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーンとは

- ビットコイン等の価値記録の取引を第三者機関不在で実現している

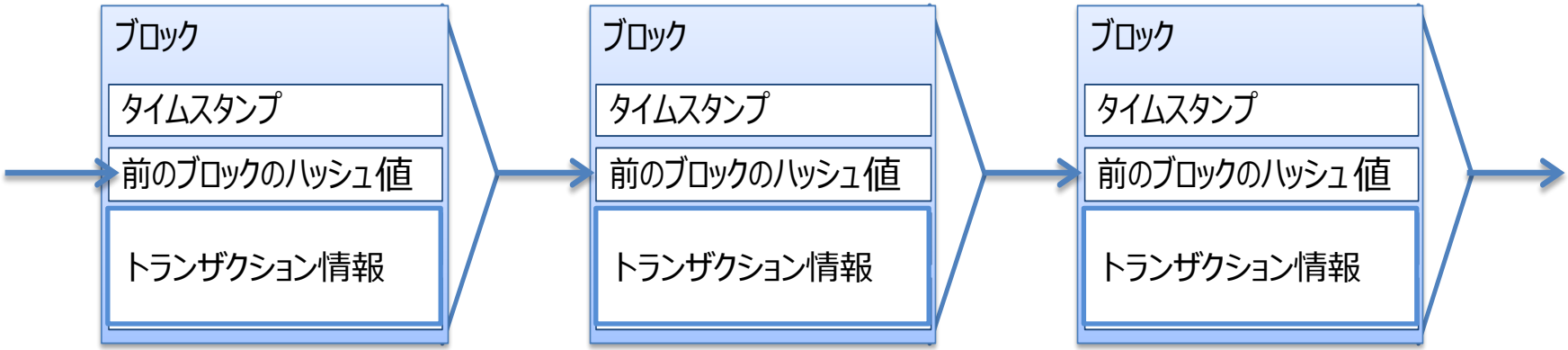


出典：平成27年度　我が国経済社会の情報化・サービス化に係る基盤整備 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術とは

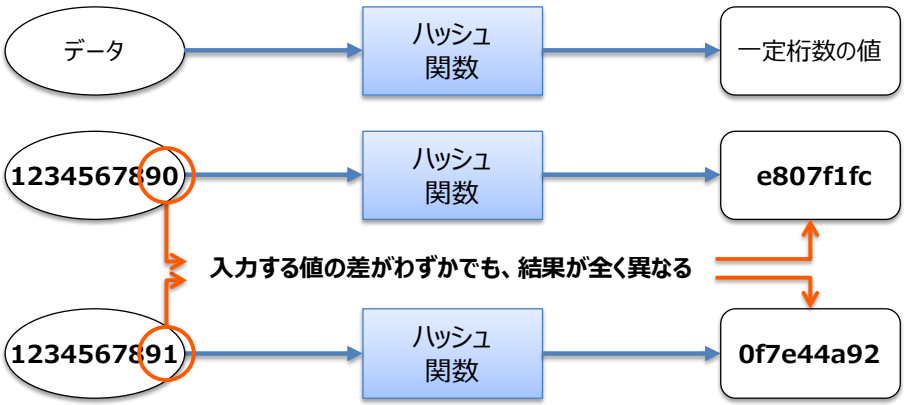
- ビットコインを実現させるために生まれた技術であり、いくつかの暗号技術がベース
- P2Pネットワークを利用してブロックチェーンデータを共有し、中央管理者を必要とせずにシステムを維持することを実現

ブロックチェーン概念図



・トランザクション情報の集合等を含んだブロックがチェーン状に連なっているもの
・ネットワーク上の複数ノードが、新しいブロックを相互に承認し、チェーンに足していく

ハッシュ値（暗号技術）



トランザクション情報

ビットコインでは、アドレスAから
アドレスBへ5BTC移動等の取引情報

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術のもたらす社会

○経済活動の基盤となる**取引相手の信頼性の担保**の手段として、これまで様々な制度や仕組みを構築してきた。**ブロックチェーン技術は、これらの仕組みを代替**し、従来の社会システムを大きく変容させる画期的な発明

（参考）信頼性担保の仕組みの例
- 格付け、会計監査：会社の弁済能力や会計の適切性の外部機関による評価
- 公証人：第三者による適法性の担保
- 登記：権利保有者の透明性の担保
- 商法：会社が取引に参加するために必要な信頼を担保するためのルール
- 中央銀行：通貨の発行主体であり、通貨の信用の担保機関

○具体的には、参加者同士が対等の関係で相互に協力・監視することで、これまで社会システムを維持するために**多大なコストを払って構築してきた中央集権的な第三者機関（中央機関）を不要**とするもの

（参考）第三者機関のコスト
- 冗長的な情報システム、運営・メンテナンス費用、組織を維持するための経営と従業員、制度・ルールなど。基本的には、利用者はこれらのコストを利用料の中で負担

匿名性を維持したまま、信頼可能な社会システムが構築できる様は、以下の特徴を相互補完。
・隣人も知らないような**匿名性が高い環境**なので気兼ねなく過ごせるが、危険も多い都市部
・顔見知りが多く匿名で過ごすことはできないが、**安心・信頼して過ごせる**地方共同体

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

（参考）ブロックチェーン技術がもたらす将来イメージ

- 中央集権型から分散型に移行することで、様々な機関が不要になる

現在

将来

中央集権型

・ポイント発行者（電子マネー）
・エスクロー機関（電子商取引）
・登記簿管理者（土地登記）
・仲介者（シェアリング）
・中央銀行（通貨）

分散型

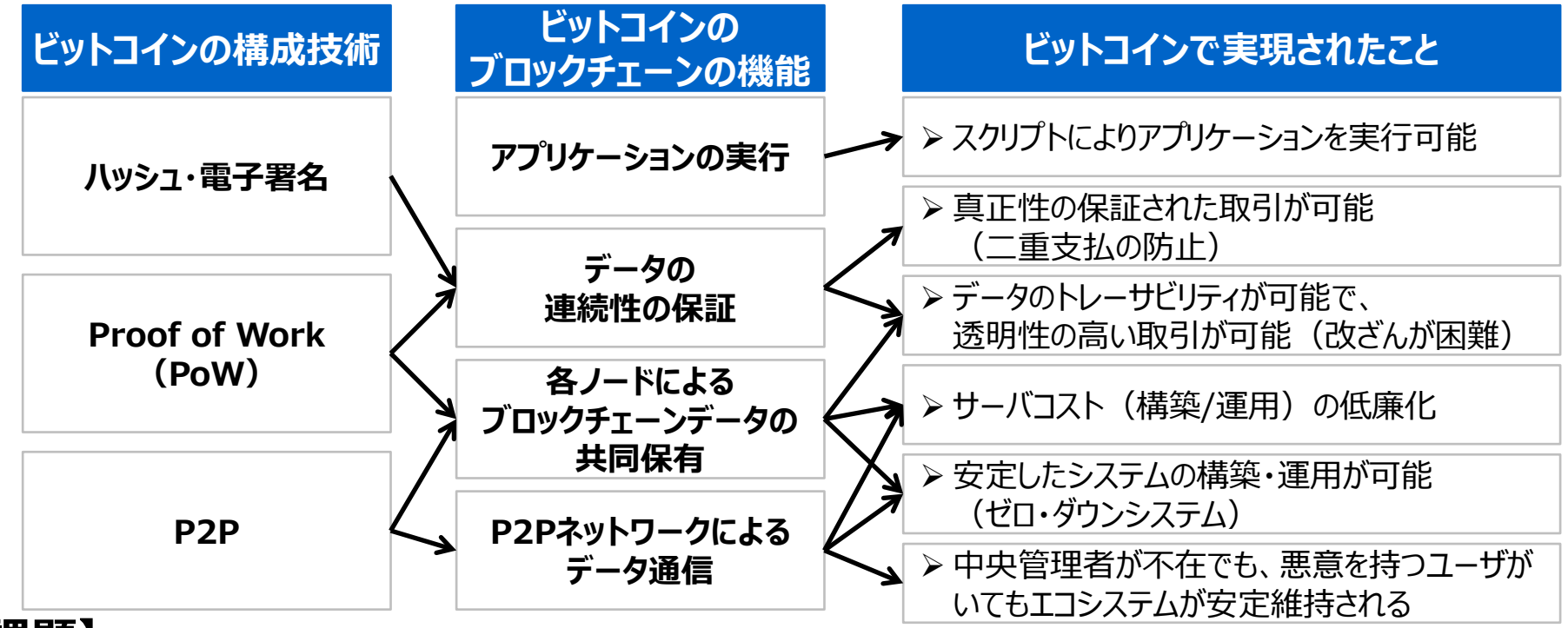
×

IBM社資料をもとに経済産業省で加工

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ビットコインからみるブロックチェーン技術の特徴と課題

- ビットコインだけでなく、様々な分野に適用可能な特徴と課題がある



【課題】

1．新ブロック生成に時間がかかる

ブロックチェーンの種類によるが、データ処理の確定に数秒～10分程度かかるので、即時性が必要なアプリケーションには不向き。

2．単位時間あたりのトランザクション件数が限られている

規定されているブロックに格納できるデータ量の上限と、新ブロック生成にかかる時間との関係から算出する、1秒間に処理できるトランザクション件数がVISA等の既存決済システムと比べて劣っている。

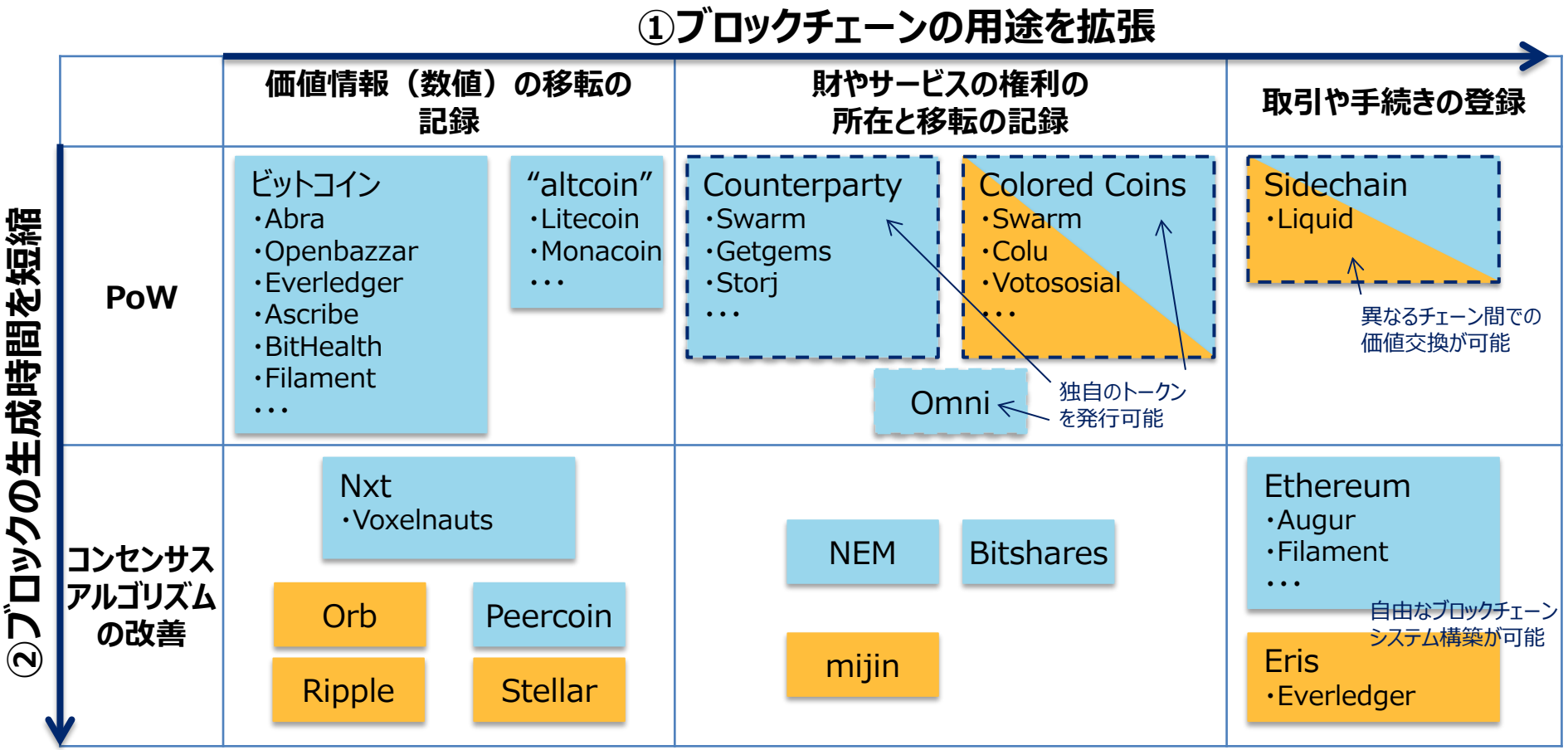
3．実ビジネスでの運用手法等が確立されていない

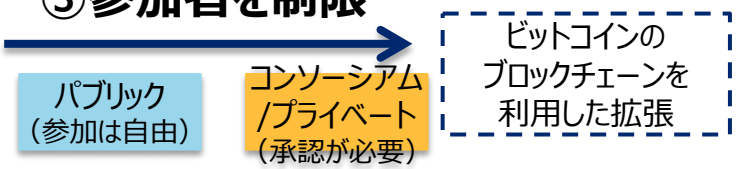
実ビジネスへの適用例が少ないこともあり、ブロックチェーンに関わる各性能要件や仕様が明確ではなく、いわゆるSLA(Service Level Agreement)が整備されていない。

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術の発展トレンド

- 3つの軸（注）で、ブロックチェーン技術の改変・発展が進んでいる





（注） 3軸の説明
①記録内容を数値に限らず、権利や契約条件等にも拡大
②ブロック生成時間の短縮のための承認アルゴリズム等の改善
③ブロック生成時間短縮やシステム堅牢性の負担軽減のため参加者を限定

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術活用のユースケース

- ビットコイン発祥のブロックチェーン技術を改良しながら、金融以外の分野にもユースケースが広がっており、「ビットコイン2.0」と呼ばれている

金融系

- 決済（SETL、FactoryBanking）
- 為替・送金・貯蓄等（Ripple、Stellar）
- 証券取引（Overstock、Symbiont、BitShares、Mirror、Hedgy）
- bitcoin取引（itbit、Coinffeine）
- ソーシャルバンキング（ROSCA）
- 移民向け送金（Toast）
- 新興国向け送金（Bitpesa）
- イスラム向け送金/シャリア遵法（Abra、Blossoms）

ポイント／リワード

- ギフトカード交換（GyftBlock）
- アーティスト向けリワード（PopChest）
- プリペイドカード（BuyAnyCoin）
- リワードトークン（Ribbit Rewards）

資金調達

- アーティストエクイティ取引（PeerTracks）
- クラウドファンディング（Swarm）

コミュニケーション

- SNS（Synereo、Reveal）
- メッセンジャー、取引（Getgems、Sendchat）

資産管理

- bitcoinによる資産管理（Uphold(旧Bitreserve)）
- 土地登記等の公証（Factom）

ストレージ

- データの保管（Stroj、BigchainDB）

認証

- デジタルID（ShoCard、OneName）
- アート作品所有権/真贋証明（Ascribe/VeriSart）
- 薬品の真贋証明（Block Verify）

シェアリング

- ライドシェアリング（La'ZooZ）

商流管理

- サプライチェーン（Skuchain）
- トラッキング管理（Provenance）
- マーケットプレイス（OpenBazaar）
- 金保管（Bitgold）
- ダイヤモンドの所有権（Everledger）
- デジタルアセット管理・移転（Colu）

コンテンツ

- ストリーミング（Streamium）
- ゲーム（Spells of Genesis、Voxelnauts）

将来予測

- 未来予測、市場予測（Augur）

公共

- 市政予算の可視化（Mayors Chain）
- 投票（Neutral Voting Bloc）
- バーチャル国家/宇宙開発（BitNation/Spacechain）
- ベーシックインカム（GroupCurrency）

医療

- 医療情報（BitHealth）

IoT

- IoT（Adept 、Filament）
- マイニング電球（BitFury）
- マイニングチップ（21 Inc,）

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術に関する海外事例

- 海外では大企業や行政も巻き込み様々な分野での実証が展開されつつある

NASDAQ

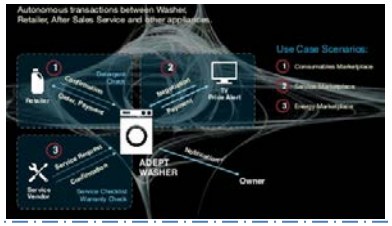
Chain社 他

ブロックチェーン技術を活用した未公開株式取引システム「Nasdaq Linq」を発表。

ADEPT

IBM社、Samsung社

膨大な機器を管理し、制御するIoT時代に対応するため、洗濯機が自律的に洗剤を補充する契約を締結・履行する分散的なシステムを実証。



FACTOM社

土地の登記謄本の記録管理の実現。中国における「スマートシティ計画」にも参画。

エストニア行政

Bitnation社

国民の医療データの記録管理に改ざんが難しいブロックチェーン技術を活用すべく利用試験開始。

REPUBLIC OF ESTONIA
E-RESIDENCY
BITNATION
GOVERNANCE 2.0

Everledger社

ダイヤモンドの所有権や権利移転履歴の証明に元帳として、シリアル番号、4C（カラット数等）等のデータをブロックチェーン上に記録。すでに100万近くのダイヤモンドの記録が載っている。

各社HP等より引用

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

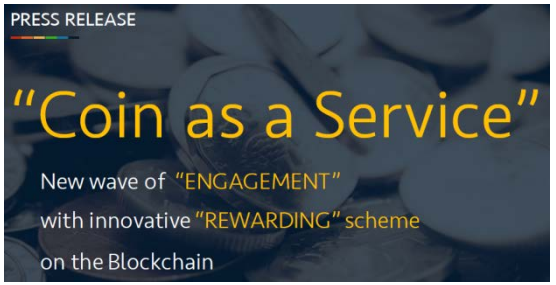
ブロックチェーン技術に関する国内事例

- 大企業の利活用の動きは鈍いが、サービス提供を行うベンチャー企業の動きは徐々に活発化

アプリケーション事例

ゼロビルバンク社

顧客の行動をポイント化し、価値として交換可能化するサービス提供を目指している。



プラットフォーム事例

Orb社

ビットコインのブロックチェーン技術を改良し、高速処理を実現。
ユースケース例として、地域通貨や電子チケット発行等。

orb
Beta

人材育成事例

ブロックチェーンハブ社

ブロックチェーン技術に関するオープンな情報プラットフォーム構築を目指し、ビジネスへの応用促進を目的として設立。

情報提供・教育・勉強会

・ブロックチェーン関連技術情報の定期的提供(日本語・英語)
・セミナー、講義、大学連携教育等
・少人数のクローズドな研究会

コミュニティー運営

・ユーザーコミュニティー運営
・開発者コミュニティー運営と開発者ネットワークデータベース作り

企業向けコンサルティング

・ブロックチェーン技術の活用方法コンサルティング
・大企業とスタートアップのマッチング

各社HP等より引用

出典: 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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

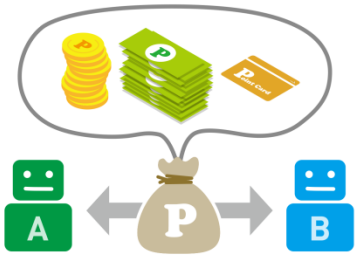
ブロックチェーン技術の展開が有望な事例とその市場規模

- 幅広い分野へ影響を与える可能性がある

ブロックチェーン技術による社会変革の可能性

※記載金額は、ブロックチェーン技術が影響を及ぼす可能性のある市場規模

01 価値の流通・ポイント化プラットフォームのインフラ化



地域通貨 / 電子クーポン / ポイントサービス

自治体等が発行する地域通貨を、ブロックチェーン上で流通・管理

市場規模※ 1兆円

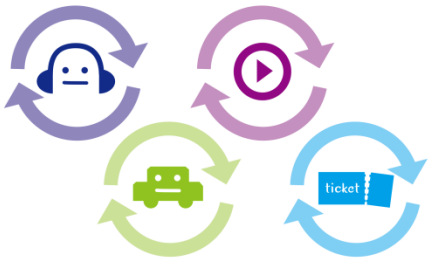
02 権利証明行為の非中央集権化の実現

土地登記 / 電子カルテ / 各種登録(出生・婚姻・転居)

土地の物理的現況や権利関係の情報を、ブロックチェーン上で登録・公示・管理

市場規模 1兆円

03 遊休資産ゼロ・高効率シェアリングの実現



デジタルコンテンツ / チケットサービス / C2Cオークション

資産等の利用権移転情報、提供者/利用者の評価情報をブロックチェーン上に記録

市場規模 13兆円

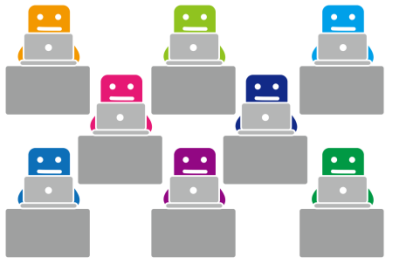
04 オープン・高効率・高信頼なサプライチェーンの実現

小売り / 貴金属管理 / 美術品等真贋認証

製品の原材料からの製造過程と流通・販売までを、ブロックチェーン上で追跡

市場規模 32兆円

05 プロセス・取引の全自動化・効率化の実現



遺言 / IoT / 電力サービス

契約条件、履行内容、将来発生するプロセス等をブロックチェーン上に記録

市場規模 20兆円

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

ブロックチェーン技術が社会経済に与えるインパクト

- 市場だけでなく、産業構造へ影響を与える可能性がある

※ボックス内は将来起こり得る産業構造へのインパクト例

【価値の流通・ポイント化プラットフォームのインフラ化】

※

- ポイントが、発行体以外との取引にも利用されるようになる。その結果、ポイントが転々流通することで通貨に近い利用が可能となるとともに、ポイント発行額以上の経済波及効果が生じる。
- さらにポイントサービスが預金・貸出に類する機能を獲得することで、信用創造の機能を獲得し、**日銀による景気対策(金融政策)以外にも民間企業による仕掛けができる可能性。**

【権利証明行為の非中央集権化の実現】

- 土地の登記や特許など、国管理のシステムをオープンな分散システムで代用可能になり、**届出管理等の地方自治体業務減少といった、政府の業務負担減少が可能。**
- 本人証明としての印鑑文化や、各種契約時（スマホ、銀行口座開設等）の際の本人確認のための書類提出等のプロセスが変化・代替される可能性がある。

【遊休資産ゼロ・高効率シェアリングの実現】

- 遊休資産の稼働率のほか、入場券、客室、レンタカー、レンタルビデオ等の利用権限管理に劇的な効率化がもたらされる。
- 究極的にはC2C取引が、現在のシェアリングエコノミーのプラットフォーム事業者を介在せずに行われる環境が構築される
- **「生産者/サービス提供者」と「消費者」の境界がなくなることで、「プロシューマ」というあり方が一般化**する。

【オープン・高効率・高信頼なサプライチェーンの実現】

- 小売店(川下)、卸(川中)、製造(川上)で分断されている在庫情報や、川下に集中していた商流情報が共有されることで、サプライチェーン全体が活性化/効率化するとともに、**川上の交渉力の強化につながる。⇒流通のアンバンドル化**
- 電化製品等は、IoTの進展や製品保証とも連携することで、最終消費者への販売後のプロダクトライフサイクルをトラッキング可能となり、売切りではないビジネスへ転換することが容易になる。

【プロセス・取引の全自動化・効率化の実現】

- 各企業におけるバックオフィス業務（契約や取引の執行、支払・決済、稟議などの意思決定フロー等）の大半を置きかえることが可能。
- IoTとスマートコントラクトによるマイクロペイメントを組み合わせることで、**受益者負担をより正確に反映した公共サービス等のコスト負担の仕組みが構築可能。**
（例えば、ゴミの量や道路の利用量に応じた課金による税徴収等）

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

政策に求められること

民間における社会実装を促進するため、実証事業の支援や、政府自らも実証していくことで広くブロックチェーン技術の有用性を周知する

①12ページのようなブロックチェーンを活用した新ビジネスの検証のための民間実証の促進と、成果及び課題の集積を行い、広く公開していくことで市場の発展を促すこと。

例：地域限定ポイント、電子チケットサービス等の実証や、そうした実証を通じたSLA(Service Level Agreement）の策定　等

②暗号分野など既存の技術的蓄積を生かしつつ、これまで不十分だったブロックチェーンの数理的、情報理論面からの検証を後押しすること。

例：大学等での研究拠点、研究者間のネットワーク　等

③行政分野におけるブロックチェーン技術の導入を進めることで、行政の効率化、高度化を推進しつつ、率先垂範すること。

例：文書管理、特許、土地登記、投票、徴税、婚姻・出産届　等

④ブロックチェーンの社会実装を円滑に行うため、必要に応じて規制等を見直すこと。

例：消費税法（仮想通貨やポイントへの課税）、資金決済法（国際送金）、電子署名法（法的証拠能力の明確化）　等

出典：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 ブロックチェーン技術を利用したサービスに関する国内外動向調査 2016年4月

補足: Blockchainを巡る動向調査後の動きについて

- オーストラリアがISOにBlockchain**国際標準化**のためのTC設立を提案 (4/14)
- Goldman Sucksが**現物取引で年間約60億ドル削減可能**と試算 (5/24)
- **仮想通貨を規制**する資金決済法・犯罪収益移転防止法改正が成立 (5/25)
- 暗号ファンド**The DAO**が1億3232万ドル相当の資金調達に成功 (5/28)

ISO

Ch. de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland | T: +41 22 749 01 11 | iso.org | central@iso.org

Form 1: Proposal for a new field of technical activity

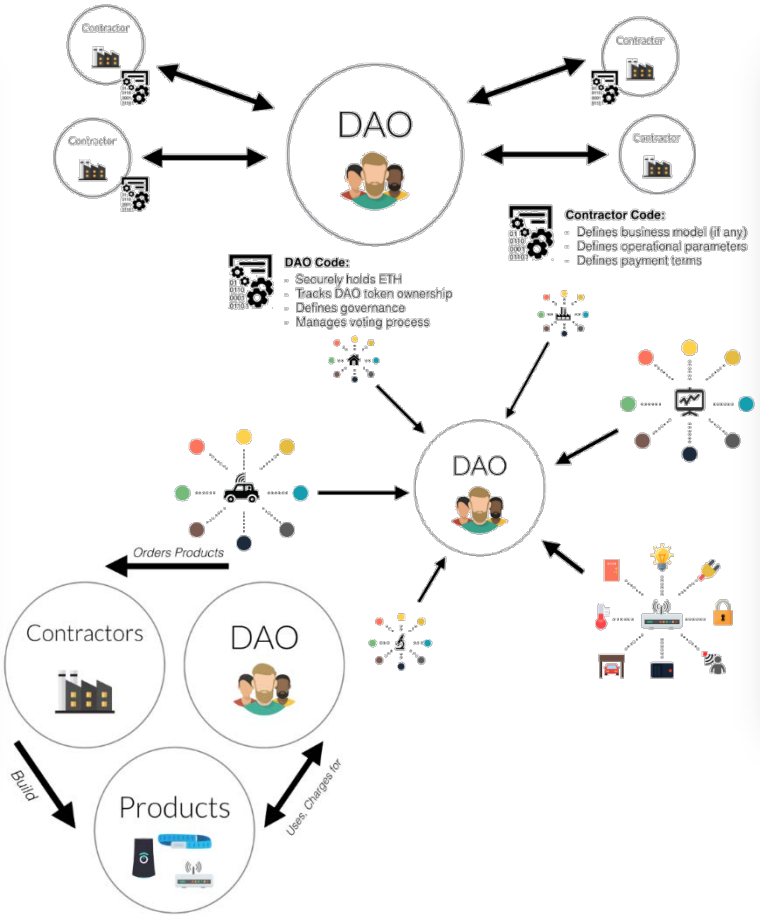
Circulation date: 2016-04-14 Closing date for voting: 2016-07-14	Reference number (to be given by Central Secretariat)
Proposer: Standards Australia	ISO/TS/P 258

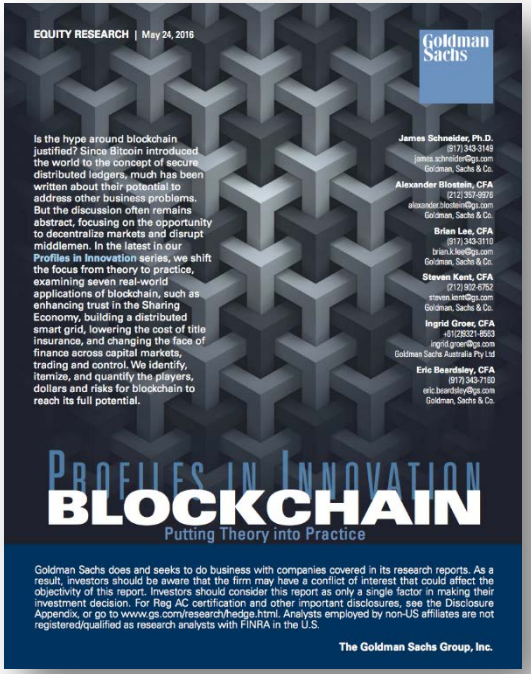
A proposal for a new field of technical activity shall be submitted to the Central Secretariat, which will assign it a reference number and process the proposal in accordance with the ISO/IEC Directives (part 1, subclause 1.5). The proposer may be a member body of ISO, a technical committee, subcommittee or project committee, the Technical Management Board or a General Assembly committee, the Secretary-General, a body responsible for managing a certification system operating under the auspices of ISO, or another international organization with national body membership. Guidelines for proposing and justifying a new field of technical activity are given in the ISO/IEC Directives (part 1, Annex C).

The proposal (to be completed by the proposer)

Title of the proposed new committee (The title shall indicate clearly yet concisely the new field of technical activity which the proposal is intended to cover.) Blockchain and electronic distributed ledger technologies
Scope statement of the proposed new committee (The scope shall precisely define the limits of the field of activity. Scopes shall not repeat general aims and principles governing the work of the organization but shall indicate the specific area concerned.) Standardisation of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems.

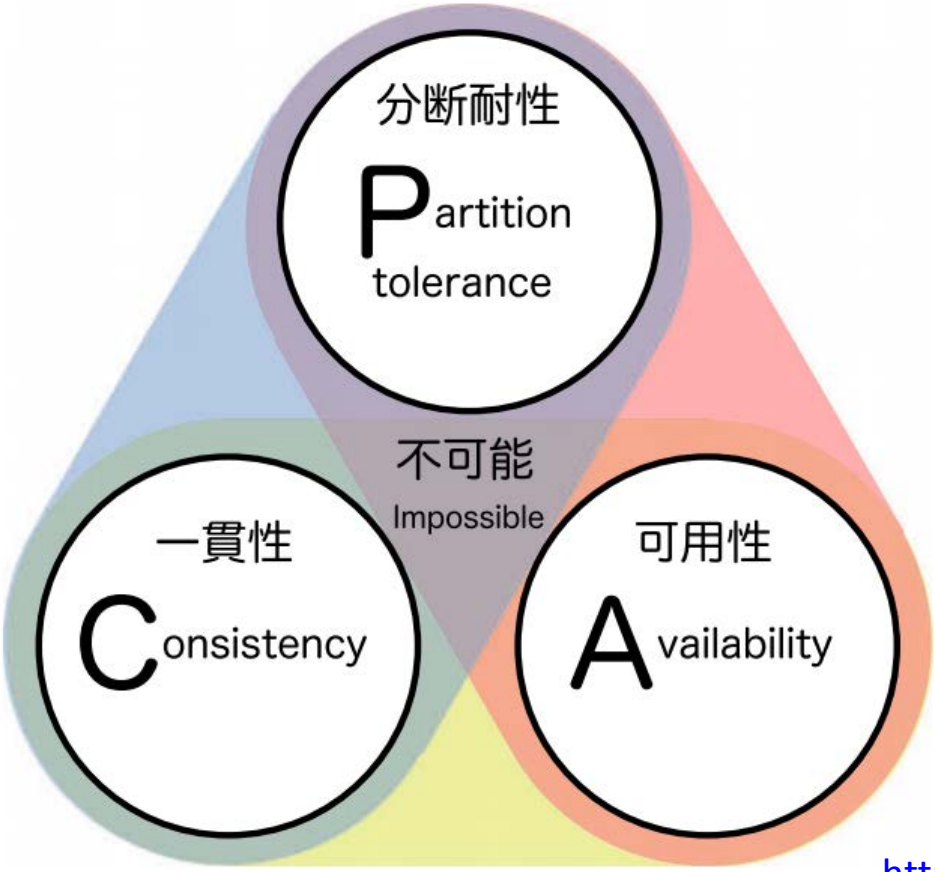
FORM 1 – Proposal for a new field of technical activity
Version 8/1/2015





私見: BitcoinとBlockchainに対する過剰な期待について

- 現時点で大規模運用されているBlockchainであるBitcoinは、採掘は中国に集中しており、スケーラビリティーは限定的で、データの整合性しか保証されない
- Blockchainも分散システムのひとつとしてCAP定理からは逃れられない



https://twitter.com/lopp/status/673398201307664384

私見: Blockchainが情報システムにもたらし得る影響について

- 個別の業務を電算化した個別システム・独自スキーマから、共通のデータ・暗号化方式・プロトコル等を共有することで組織を超えた疎結合システムを実現できる
- データ保全のための境界セキュリティーに対する考え方について見直しが進む

オープンシステムで異システム間の通信そのものは容易になったが、データ構造やアクセス制御は縦割りで設計されてきたため、相互接続を実現するには仕様レベルでの複雑な擦り合わせと接続テストが必須となり、BCPを実現するには個別システムで冗長性を確保する必要がある

境界を突破された途端に全てデータを抜かれてしまう従来型の境界セキュリティーから、最初から全てのデータにアクセスできる前提でオブジェクト単位の署名・匿名加工を行うBlockchainの発想に

データ層の設計・運用を共有することで異システム間の相互連携とBCPを容易に