ブロックチェーン（分散型台帳技術）

講演資料

グローバル金融ビジネスユニット

両角　真樹

2017年1月17日

株式会社NTTデータ経営研究所

コンサルタントプロフィール

両角　真樹　Masaki Morozumi

株式会社NTTデータ経営研究所　グローバル金融ビジネスユニット
シニアマネージャー ／ Asian Payment Network Business Sub-Committee Chairman

- アクセンチュア株式会社　戦略グループ　金融コンサルティング本部
- デロイトトーマツコンサルティング合同会社　銀行・証券ユニット、ペイメンツ・プラクティス リード
- 2015年より現職、**専門は決済（Payment）を中心とした新規事業創出、海外進出支援、等**

■代表的なプロジェクト
- ブロックチェーン技術の活用可能性と課題に関する検討
- 世界のクロスボーダー送金サービスの先進事例調査、海外進出策定支援
- アジアの決済高度化推進に向けたAPN（Asian Payment Network）の戦略的活用
- 米国ATM市場の先進事例・技術調査、参入戦略の策定

他多数

■執筆、講演
- ブロックチェーンと分散型台帳技術　（某クレジットカード会社 講演）
- ASEANにおける「ブロックチェーン」の可能性　（情報未来 No.50　NTTデータ経営研究所）
- 検証・ビットコイン事件「ネット仮想通貨」の未来を探る（日経ビジネス／コンピュータ主催 講演）
- ビットコイン、「規制」の成否（日経ビジネス）

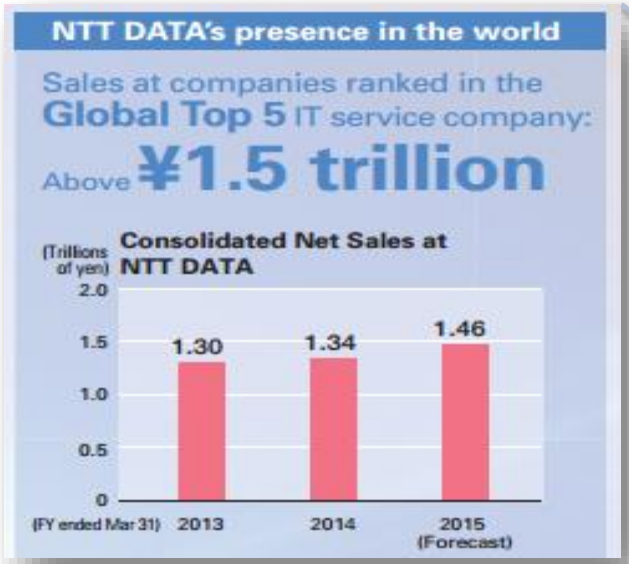
■アドバイザー等
- 自民党 IT戦略特命委員会 資金決済小委員会 アドバイザー
  （ビットコインをはじめとする「価値記録」への対応に関する中間報告、日本価値記録事業者協会設立、デジタル・ニッポン2014策定、等に関する提言・取り纏め支援）

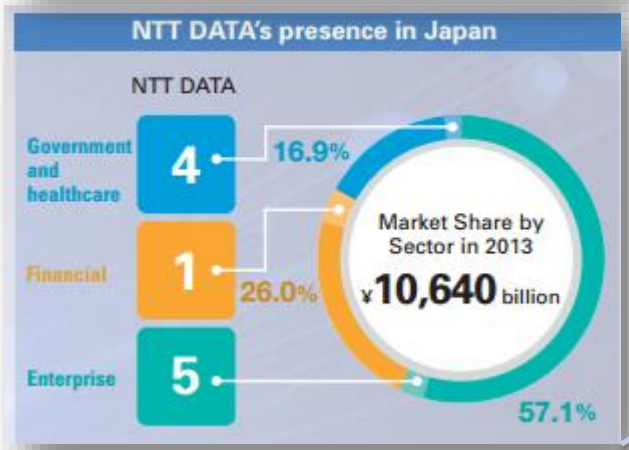
他多数

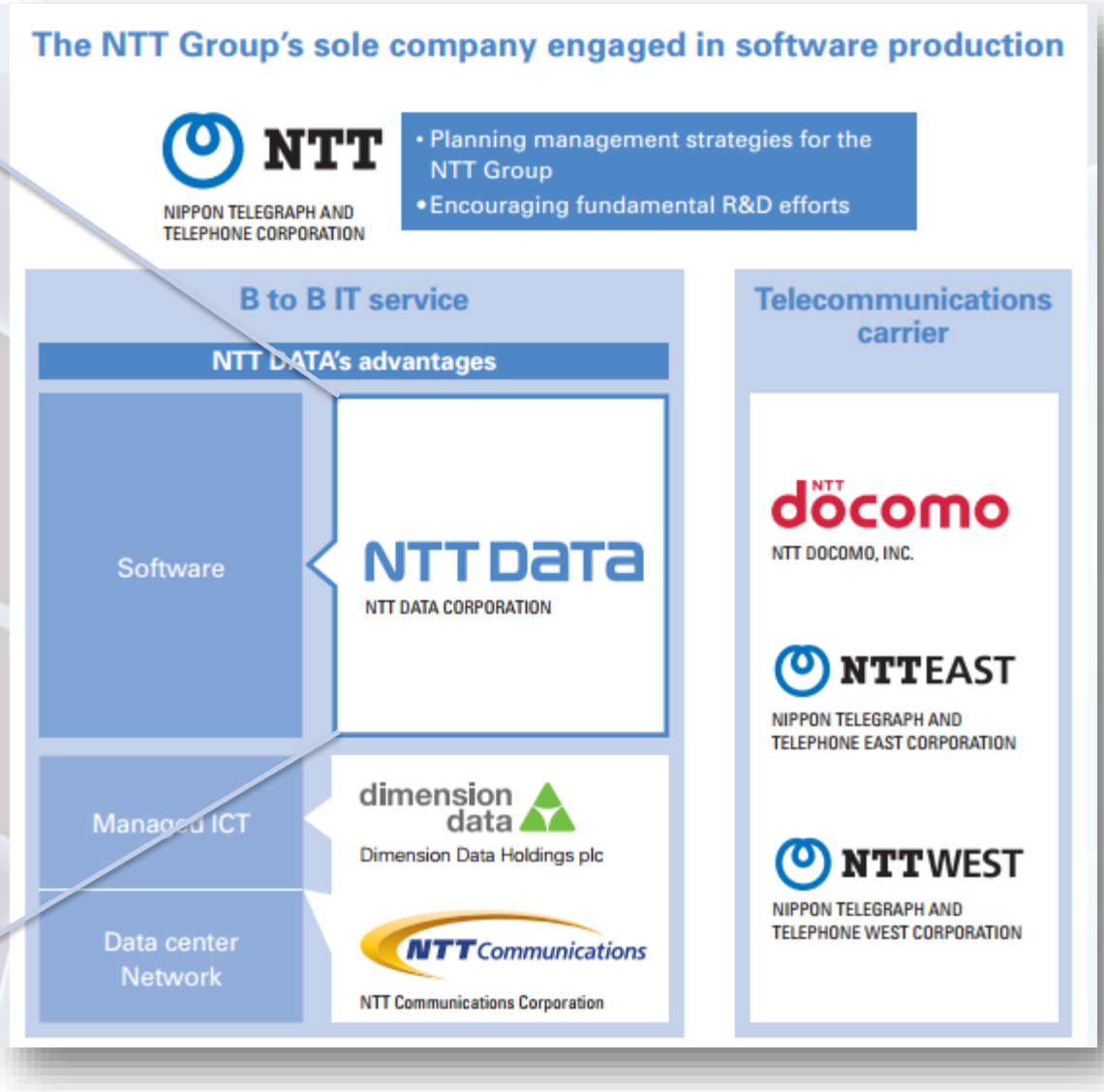
NTTグループのご紹介

NTT DATA

NTTデータとしては、全世界で約1.5兆円の売上、日本では金融分野でシェアNo.1。







NTTデータ経営研究所のご紹介

NTTデータの100%子会社として様々なコンサルティング機能を提供。
弊ユニットは、グローバル案件を中心に銀行やカード会社等にコンサルティングを実施。

NTTグループにおけるグローバル・コンサルティング・カバレッジ

Japan & Singapore

NTTデータ経営研究所

公共分野 | 産業分野 | 金融分野

EU & LATAM

everis
an NTT DATA Company

North America

Carlisle & Gallagher Consulting Group
an NTT DATA Company

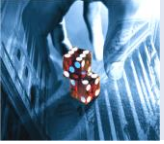
金融戦略コンサルティング部門

グローバル金融ビジネス	金融コンサルティング	金融政策コンサルティング

全社戦略、事業／商品戦略、
マーケティング／チャネル戦略
オペレーション戦略、各種調査

海外進出支援、M&A、ルール形成戦略

FinTech、アクセラレーター／インキュベーター、
デジタル・バンキング・トランスフォーメーション、

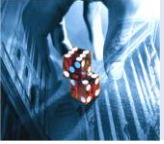


NTTデータグループにおけるブロックチェーン関連の実績

NTT DATA

ブロックチェーン技術に関する共同研究や実ビジネス検討と共に、関連する暗号化／P2P技術等の検討も幅広く実施。

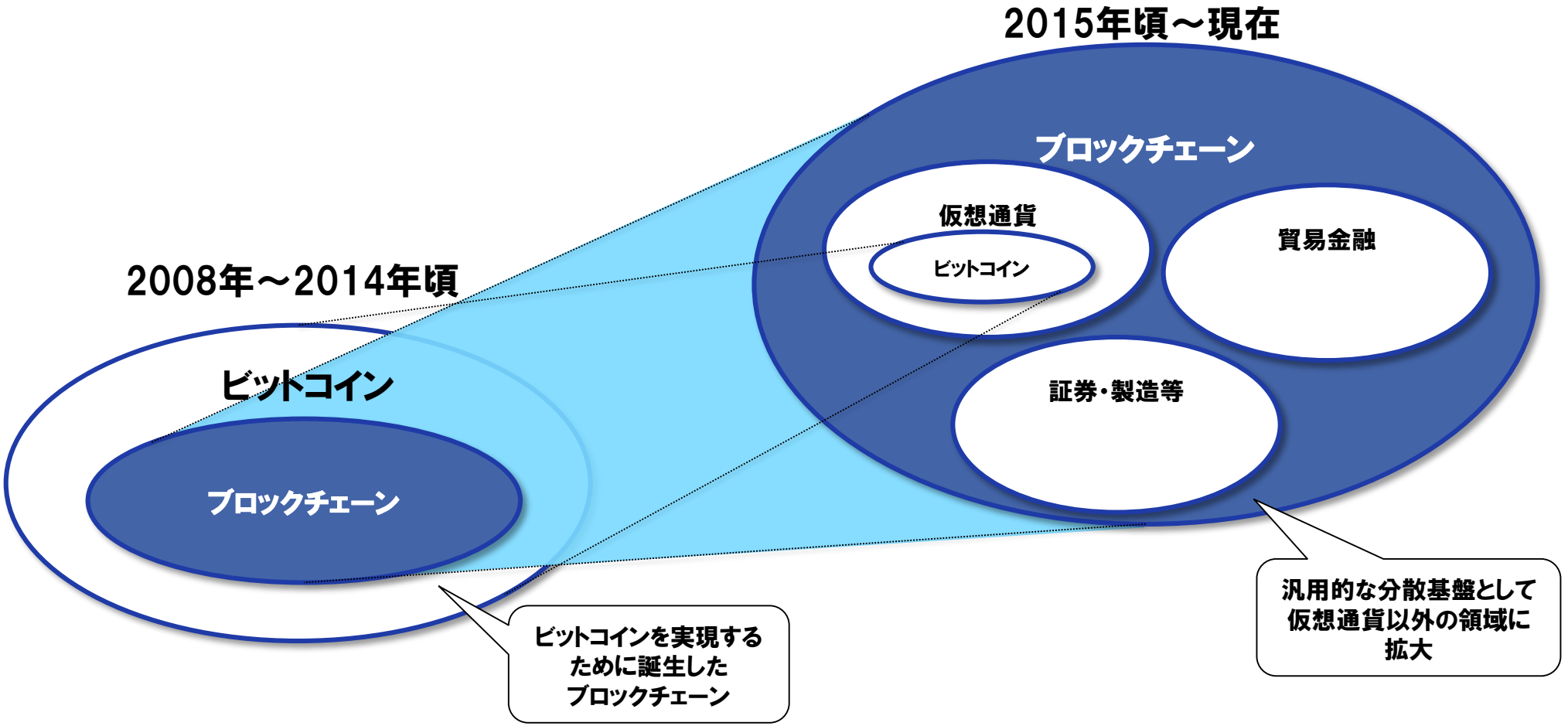
カテゴリ	主な実績
ブロックチェーン技術	● NTTデータ先端技術にてEthereumに関するトランザクション処理、マイニング処理、及びクライアント実装の比較等に関する検証を実施 ● 2015年9月よりNTTデータの各部門横断で有識者を集め、ブロックチェーン技術を利用したビジネス展開の検討をサブワーキンググループ形式にて開始 ● 2016年2月には、エンタープライズ領域でのブロックチェーン技術活用促進を目指す国際コンソーシアム「Hyperledger Project」に創立メンバーとして参画 （他に、SWIFTやJ.P.Morgan、IBM、日立製作所、Airbusなど計99社・機関が参画） ● 2016年7月には、貿易金融をテーマにしたブロックチェーン適用に関する実証実験を、オリックス株式会社、オリックス銀行株式会社、株式会社静岡銀行と合同で実施 （貿易金融の領域でブロックチェーン活用を検証した国内初の事例） ● 全国銀行協会 ブロックチェーン技術の活用可能性と課題に関する検討会、の支援 ● IPFA、APN、IPayments Forum等の国際決済標準化団体とブロックチェーンに関する情報交換を実施
暗号化技術	● PCの盗難・紛失による情報漏洩を防ぐための暗号化ソリューションの検証と販売 ● 電子メールのセキュリティ高度化のための暗号化機能の検証とソリューション販売 ● PCIデータセキュリティ標準における暗号化手法を含むガイドライン作成 ● Red Hatなど複数ベンダーにおけるtelnetdの暗号鍵処理に起因する脆弱性の検証
P2P技術	●『モバイルでのP2P関連サービス事例／Pushによるサービス事例』調査を実施 ● SkypeのP2P技術を活用したバーチャル・リアリティに関する開発を支援

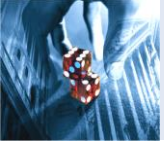


目次

ビットコインはブロックチェーン技術を利用した実装例でしかない。

ビットコイン ≠ ブロックチェーン





Ⅰ-A ブロックチェーンの構成要素
4つの構成要素

NTT DATA

ブロックチェーン技術とは、「取引履歴を暗号技術によって過去から1本の鎖のように繋げ、ある取引について改ざんを行う為には、それより新しい取引について全て改ざんしていく必要がある仕組みとする事で、正確な取引履歴を維持しようとする技術」

1. ピア・ツー・ピア (P2P) ネットワーク

・特定の管理主体が存在するクライアント・サーバ型ではなく、**各コンピュータ (ノード) が対等に直接通信し、ネットワークを形成する方式**

2. コンセンサス・アルゴリズム (PoW、PoS、PBFT、等)

・P2Pネットワークなどの分散ネットワーク上で**合意形成を行う為のアルゴリズム**
・ブロックチェーンを複数ノード間で共有する為に最も重要な仕組み

3. 電子署名・ハッシュ関数

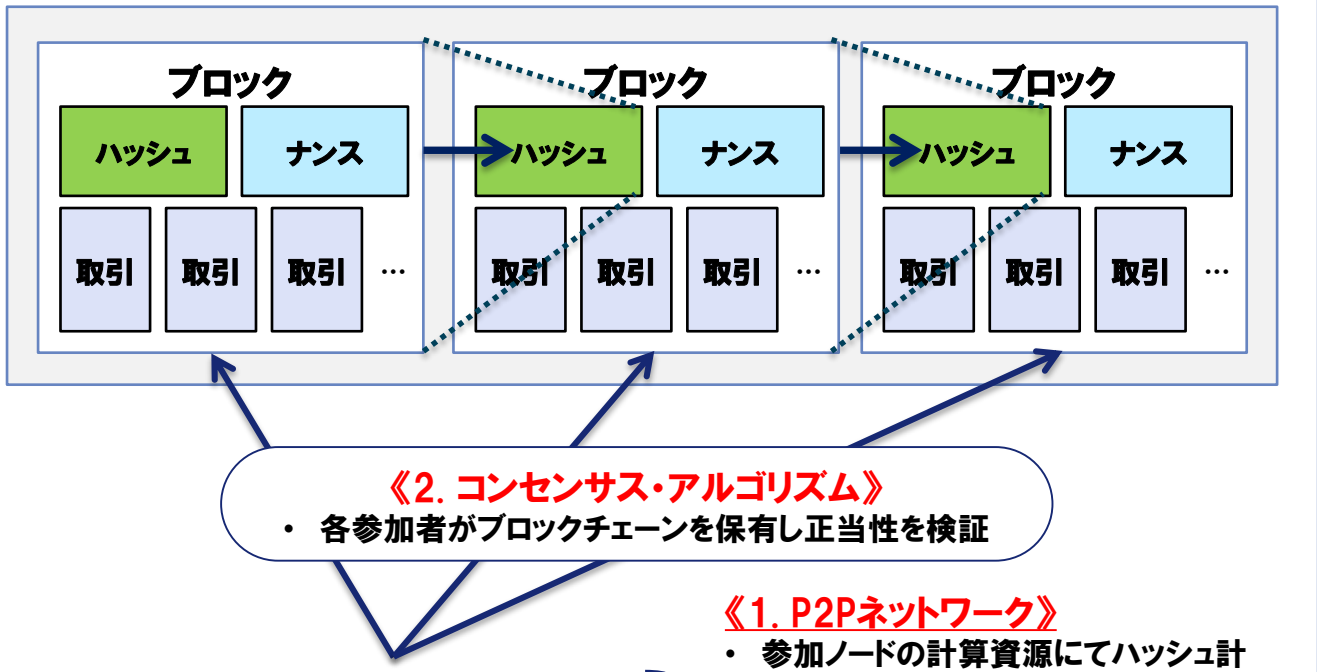
・トランザクション (取引) を発行する人の正当性を保証する仕組みや、取引・ブロックチェーンの改ざん防止や暗号化など、**セキュリティーに関する仕組み**

4. スマートコントラクト

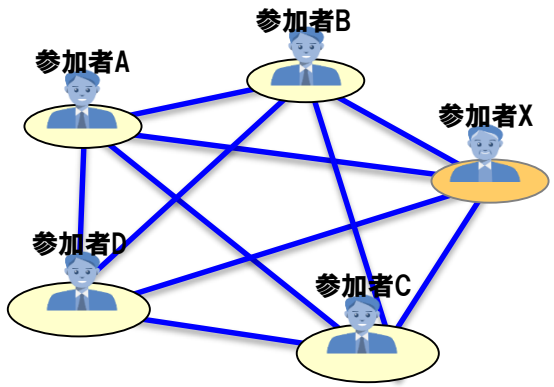
・「特定コインに対して一定期間は誰も引出せず、これが過ぎると指定したアドレスに送金 (預託) 」等、**ブロックチェーンネットワーク上で自動で動作するプログラム**の事
・プログラム言語によって、非常に自由度の高い処理を記述する事ができ、個々の業務領域に対応させるには、スマートコントラクトをビジネス要件に合わせて記述する必要

Ⅰ-A ブロックチェーンの構成要素
ブロックチェーンの基本的な仕組み

ブロックが鎖の様に繋がれるので、ブロックチェーンと呼ばれる。



《2. コンセンサス・アルゴリズム》
- 各参加者がブロックチェーンを保有し正当性を検証



《1. P2Pネットワーク》
- 参加ノードの計算資源にてハッシュ計算が正しい事とブロック内の取引が正しいものである事を確認
- 参加者全員が同じ内容のブロックチェーンを保有

※ノードとは、ブロックチェーンのP2Pネットワークに接続される通信機器（銀行間取引では銀行が保持するサーバ、個人間取引では個人が保持する端末等がノードとなる）

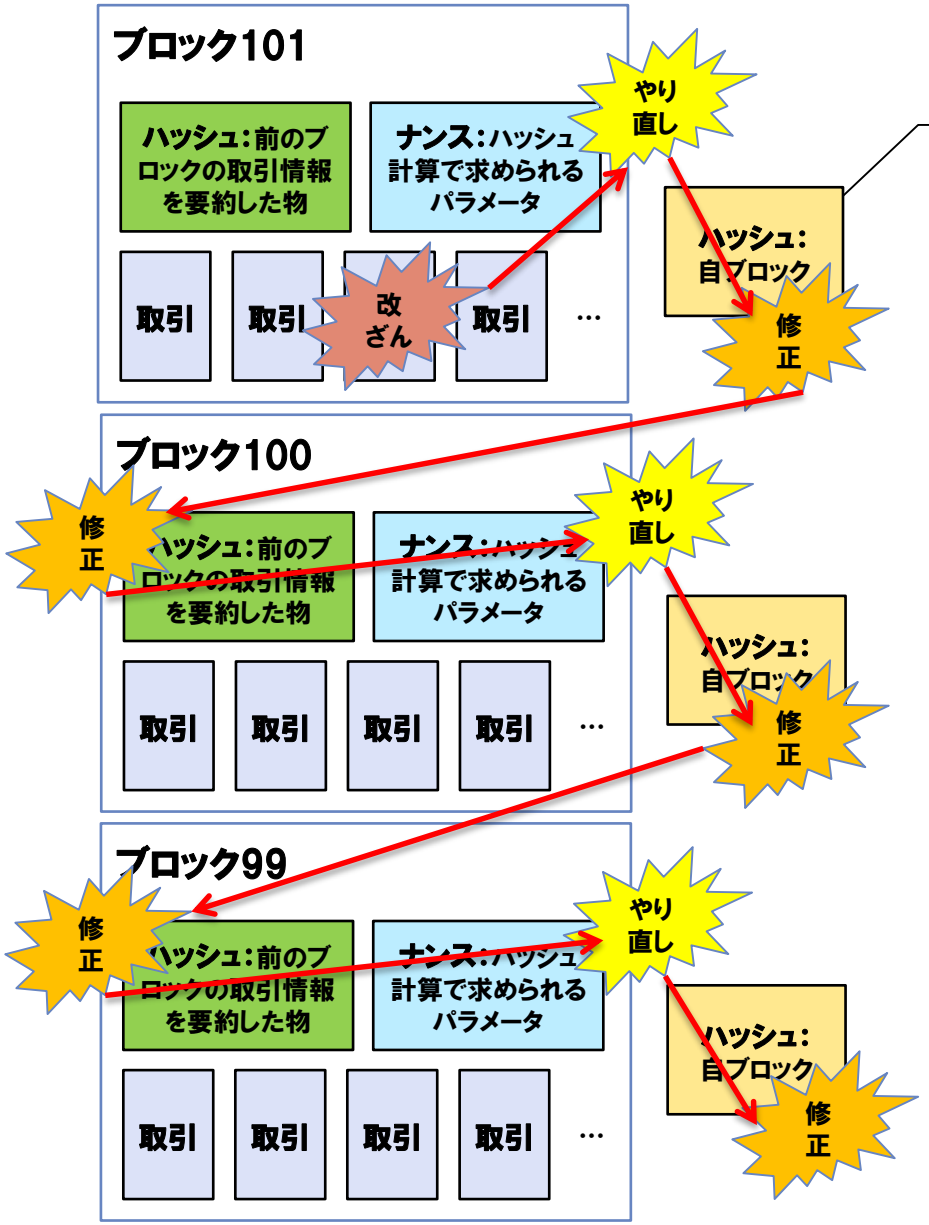
《3. 電子署名・ハッシュ関数》
- 各トランザクションに1つずつ付与される電子署名と、各ブロックで前ブロックのハッシュ値を保有する仕組みにて、ブロック順序維持と耐改ざん性を高めている

※ハッシュとは、ハッシュ関数を用いた計算によって前のブロックが持つ情報を要約した結果
ビットコインではSHA-256という256ビットのハッシュ
電子データでは無く常に256ビットという小さなサイズのハッシュの使用により検証時間の短縮を図る事が可能

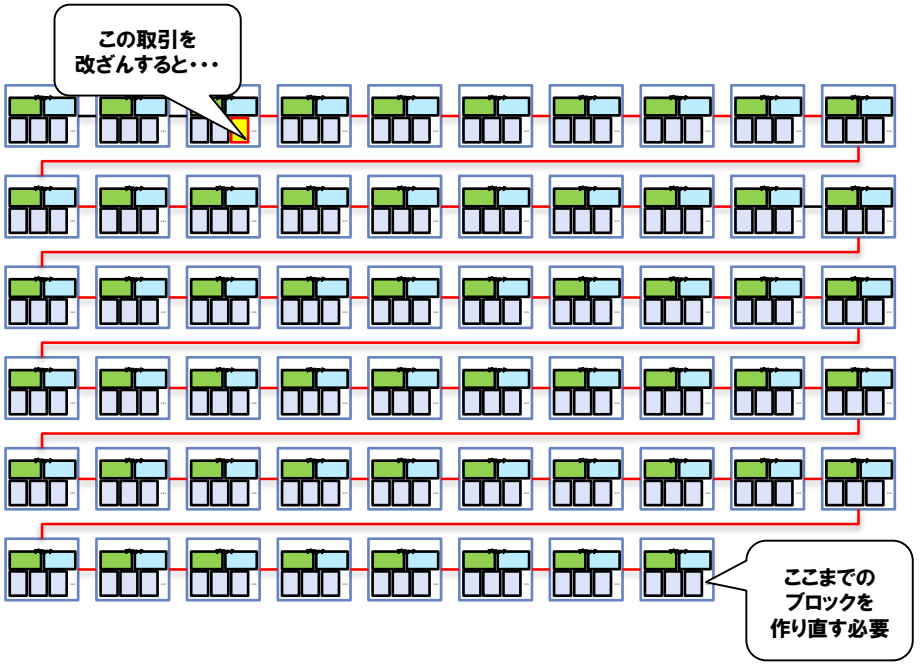
※ナンスとは、新しいブロックを作成する際にハッシュ計算に与えるパラメータ

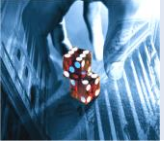
《4. スマートコントラクト》
- ブロックチェーン基盤の種類によってスマートコントラクトの仕組みは、トランザクションに組み込まれる形で処理されプログラムの伝播や実行もブロックを介して行われるパターンと、各ブロックとスマートコントラクトで管理されるデータとを明確に分離してP2Pネットワーク上で共有するパターンが存在

Ⅰ-A ブロックチェーンの構成要素
（参考）電子署名・ハッシュ関数による耐改ざん性



- ある取引を改ざんすると、そのブロックのハッシュが変わる為、ナンス計算がやり直し
- そのハッシュが変わると、次のブロックにあるハッシュも変わる
- するとまたナンスの計算がやり直し・・とマイニングが数珠繋ぎに必要
- このようにブロックが過去の情報を保持した状態で繋がれていく為、**不正な取引を成立させる為には、改ざんした以降のブロックを全て作り直し、正当に伝搬しているブロックよりも早くブロックを成立させる必要**





（参考）ビザンチン将軍問題

NTT DATA

ビットコインが「ビザンチン将軍問題」を完全に解決しているかに関しては諸説ある＊1が、分散型システムで過去有効な解決を見出せなかった問題に対して、実用的な解を示し、現在に至るまで稼働しているシステムを実現した事は事実。

《日本ブロックチェーン協会が提示したブロックチェーンの定義》

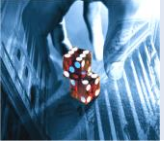
1. 狭義：ビザンチン障害を含む不特定多数のノードを用い、時間の経過と共にその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ
2. 広義：電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ

- 「ビザンチン将軍問題」とは、相互に通信しあうネットワークにおいて、故障または故意によって偽の情報を伝達する可能性がある場合、正しい合意を形成できるかを問う問題、ビザンチン帝国の将軍達が同盟軍を形成、1つの都市（帝国軍）を包囲しているような状況で発生
- 同盟軍は全員一致で攻撃か撤退かを決めなければならないが、残念な事に同盟軍には裏切り者の国があり、どの国かいくつあるかも分からない
- 全同盟国が一堂に会さず、2国間の情報交換のみで、裏切り国以外の同盟国全体で正しく方針を伝達しあう事はできるか？

よく知られた解は「各国が知った情報」の情報を交換する方法で、次の4つのステップを踏む
①まず2国間で情報交換、1階情報として「A国攻撃、B国攻撃、C国撤退…」を各国それぞれが得る、勿論裏切り国からの情報は虚偽の可能性
②次に「1階情報」自体を交換、これにより2階情報として次のマトリクスを各国が獲得
A国から「A国攻撃、B国攻撃、C国撤退…」
B国から「A国攻撃、B国攻撃、C国攻撃…」
…
③各国は、更に2階情報のマトリクスを縦に見て、過半数が同じ方針を示していれば、その国の方針は正しいと判断
A国の判断「A国攻撃、B国攻撃、C国撤退…」
…
I国の判断「A国攻撃、B国攻撃、C国攻撃…」
④最後にこのマトリクスを縦に見ると、裏切り国以外の同盟国分の方針は完全に一致、つまり正しく方針が伝達された事になり、これに基づいて攻撃か撤退か決定すれば良い、但し残念ながら裏切り国数が3分の1以上あると正しい伝達にならない事が証明済み

ビットコインではマイニングにより報酬が与えられる一方で、不正を試みる者はPoWの問題を何倍も解いて正直な参加者達に勝たねばならない
これが極めて困難で、単純に問題を解く方が“お得”な事が、ビットコインのセキュリティを支えている

＊1：ビットコインネットワークに参加する複数のピアを比較的少数のピアが操れば、ビットコインのネットワークを分断し得る（エクリプス攻撃）という説も存在

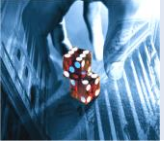


Ⅰ-B コンセンサスアルゴリズム
コンセンサスアルゴリズムの種類と特徴（1/3）

NTT DATA

分散ネットワーク上で各ノードが合意形成をする為のアルゴリズム。
どのようなサービスに適用するかによって適切なコンセンサスアルゴリズムを選択する事が重要。

コンセンサスアルゴリズム	特徴	採用システム	可用性
PoW (Proof of Work)	• ビットコインのP2Pネットワーク上で取り交わされるトランザクションの正当性を、ネットワークの参加者自身が検証・承認する事で、**管理者を介さずに価値の移転を可能**とする為の仕組 • **トランザクションを承認するノードはマイナー（採掘者）**と呼ばれ、**ブロックの生成にはマイニング（採掘）**という単純だが**非常に多くのコンピュータ・リソースを要する**作業が必要となる為、悪意のあるマイナーが意図的に不正なブロックチェーンを伸ばして、これを正当化するためには膨大なコンピュータ・リソースが必要となり、事実上改ざんは不可能	• Bitcoin Core • Ethereum（※詳細的にはPoSへの移行が検討中）	究極的には**1台でも稼動**可能
PoS (Proof of Stake)	• PoWを応用したアルゴリズム、**コインの保有量・保有期間が大きいほどマイニングの難易度を低くする**事でPoWのコンピュータ・リソースの無駄遣いを改善 • 大量コイン保有者が常に有利になる為、彼らがコインを使わなくなる懸念	• mijin	
PoI (Proof of Importance)	• PoW・PoSを応用したコンセンサスアルゴリズム • コイン保有量・保有期間に加え、**直近の頻度の高さでマイニングの難易度を低くする**事でPoSにて想定される大量コインの保有者によるコインのため込みを是正	• NEM	

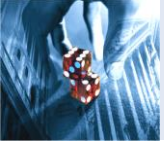


Ⅰ-B コンセンサスアルゴリズム
コンセンサスアルゴリズムの種類と特徴（2/3）

NTT DATA

全ノードの3分の1未満の故障台数にて保証されるアルゴリズム。
PBFT類似の仕組みは先般の3メガの実証実験でも使用。

コンセンサスアルゴリズム	特徴	採用システム	可用性
PBFT (Practical Byzantine Fault Tolerance)	• 特定のノード（以下コアノード）にブロックの作成権限を集中させ、コアノードによる合議制で承認（2/3以上のコアノードが合意することで承認） • コアノードは信頼できる機関により運営される必要があり、PoW、PoS、Polのような「特定の管理者を介さずに合意形成する」という特徴は無いが、迅速確実な価値の転移が可能 • コアノードで障害が発生した場合、ネットワーク全体に障害が波及する懸念	• Hyperledger Fabric	全ノードの3分の1未満の故障台数にて保証（※3分の1ちょうどの場合は不可）
Sieve	• PBFTを拡張したアルゴリズム • 合意形成の前段階で検証を行う「実行結果転送」と、検証された実行結果を集計する「集計結果転送」の2つのフローに分けて処理を行う特徴を持つ • 各ノードの実行結果が異なる可能性を早期に検出したい場合に有効な方法 • 各ノードのいずれかがクライアントになり、リーダーに各ノードへの実行を行うよう命令、リーダーの依頼により各ノードが行った実行結果において一定数合わない場合は中止となり、要求は無視される • 集計結果転送にPBFTが採用される事が多いが、処理手順はPBFTより多くなる	• Hyperledger Fabric （※2016年7月からは非採用）	



Ⅰ-B コンセンサスアルゴリズム
コンセンサスアルゴリズムの種類と特徴（3/3）

NTT DATA

全ノードの2分の1未満の故障台数にて保証されるアルゴリズム。

コンセンサス アルゴリズム	特徴	採用 システム	可用性
Paxos	• 合意形成に特化したアルゴリズムで、PBFTと同様にリーダーを中心として採用する値を決定、**決定条件は過半数のノードの同意が取れている事**で、**同意内容は後で覆る事が無い** • **リーダーが不正をした場合やメンバーが虚偽の申告をした場合は同期が取れなくなる**為、**悪意ある参加者の存在が懸念される環境には適さない**	• Google Chubby	**全ノードの2分の1未満の故障台数にて保証** （※2分の1ちょうどの場合は不可）
Raft	• 一般に実装が非常に難しいとされるPaxosよりも**システム実装を意識したリーダー選出の仕組み** • メンバーが二分された場合、半数に満たない少数のコミュニティは、過半数の承認が得られず、コミットされないままになる • またメンバーが3等分された場合は、どのコミュニティもコミットできない状態が続く特性	• RAMCloud	

（参考）コンセンサスアルゴリズムとブロックの分岐

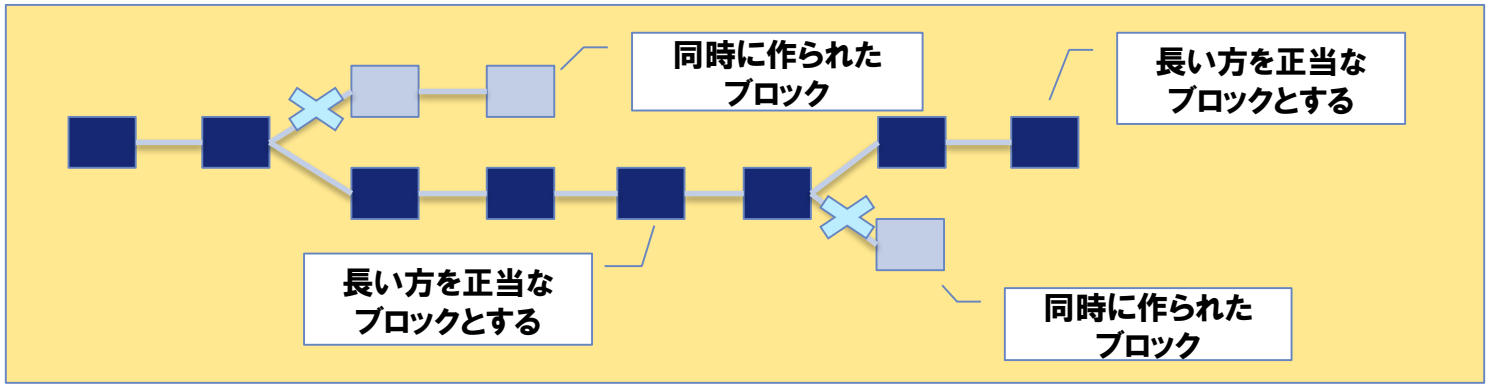
例： PoW（Proof of Work）における分岐問題と対策

- ブロックチェーンでは、同じタイミングでブロックが作成されたり、ネットワークの遅延や断絶によって局所的にブロックが作られる＊1事で、結果的に**同じ番号で異なるブロックが存在する事象**が発生
  → この状態を「**分岐（フォーク）**」と言う

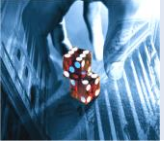
- 次のブロックを作成する参加者は、分岐したチェーンの中から**一番長い枝（ブロックが多い枝）を選び、そこに自分のブロックを加える計算を開始**
  一方、短い方の枝は事実上捨てられ＊2、**短い枝を構成するブロックの参加者は取引が無効**

- Bitcoinの場合、参加者（マイナー）は、**ブロックを作成する（マイニング）事で報酬を得られる仕組み**
  CPUの使用量を証明に使用する事で、少数の悪意あるノードは多数の善意のノードに勝つ事ができない理屈
  CPUを大量に使わせる**インセンティブとして報酬**を設定

- この方法では、**理論的に取引を確定できない（確率論でしかない）**という課題が存在
  従って、ネットワークの遅延等を考慮し、**一定時間待つ事でフォークは解消できるとの前提**に立って運用



＊1：分岐は悪意あるノードよりも、P2Pのネットワークの構造上の理由に寄る所が大きい
＊2：厳密には、かなり遅れて枝が交代する可能性もある為に捨てず、ブロックが遅れて届いた場合でも対応できるようにそのまま残存



Ⅰ-C 参加方法による分類 ブロックチェーンの公開範囲

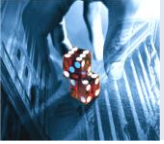
NTT DATA

ブロックチェーン技術は参加に対してオープンなパブリック型のみならず、管理された参画者で構成されるコンソーシアム型や自組織内で構築されるプライベート型が存在。

	パブリック型	コンソーシアム型	プライベート型
特徴	・悪意ある参加者を排除する仕組み（コンセンサス方式等）が必要	・全参加者の身元が明確になっている為、コンセンサスの形成が取り易い	・組織内のルールに基づきコンセンサスを形成する事ができる
ノード参加	不特定多数のノードが参加可能	特定の組織・グループが参加可能	単一の組織・グループが参加可能
ブロックチェーン閲覧	制限なし	制限可能	制限可能
ブロック生成時の難易度設定	高難易度な仕組みが必要	任意	任意
マイニング報酬	必要	任意	任意

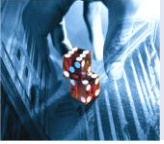
Bitcoinはパブリック型

エンタープライズ利用はコンソーシアム型が有力視



Ⅰ-D ブロックチェーン基盤の種類
基盤の比較

名称	開発元	特徴
Bitcoin Core	Bitcoin Foundation	・ビットコインのリファレンス実装 ・ブロックチェーン技術を最初に適用・普及したプラットフォーム
Ethereum	Ethereum Foundation	・分散型アプリケーション（Dapps）のプラットフォーム ・専用プログラミング言語でコントラクトを記述可能
Hyperledger Fabric	Hyperledger Project	・Linux Foundation主導で開発された金融向け分散型台帳技術基盤 ・パフォーマンスや信頼性向上のため、独自のコンセンサスアルゴリズム（PBFT）やメンバーシップ管理の仕組みを保有
Corda	R3 CEV	・R3コンソーシアム主導で開発された金融業界向けの分散型台帳基盤 ・合意形成に焦点を当てており、参加者全員で全てのデータを共有しない事が特徴 ・2016年11月、Hyperledger Projectに無償で提供された
Chain Open Standard 1	Chain.inc	・1秒足らずで取引完了状態を実現する新しいコンセンサスモデルやブロックチェーンの暗号化など、企業利用を前提とした機能を保有
Eris	Eris Industries	・Ethereumから派生し、パーミッション型のブロックチェーンを志向 ・ブロックチェーンを交換できる特徴を保有
mijin	テックビューロ	・「NEM」の開発者による国産プライベート型ブロックチェーン、参加は許可制 ・トランザクションの高速化を志向 ・コンセンサスアルゴリズムに「Proof of Stake」を採用
Orb1	Orb	・国産、運営主体により権威付けられた「スーパーピア」によって定期的に取引を確定させることで、決済完了性を確保、中央集権と分散型のメリットを融合



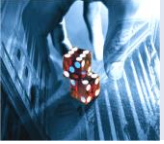
NTT DATA

Ⅰ. ブロックチェーンとは
- A）ブロックチェーンの構成要素
- B）コンセンサスアルゴリズム
- C）参加方法による分類
- D）ブロックチェーン基盤の種類

Ⅱ. ブロックチェーンの関連団体・プレイヤー
- A）代表的なイニシアチブ
- B）業態毎の代表的なプレイヤー

Ⅲ. ブロックチェーンの活用可能性
- A）ブロックチェーンの利点と課題
- B）具体的なUse Case

添付
- A）通貨としてのブロックチェーンにおける各国対応
- B）通貨としてのブロックチェーンにおける日本の関連法規制

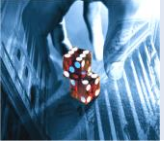


II-A 代表的なイニシアチブ （国内）

NTT DATA

特に2014年設立のJBAをはじめとして、国内もまだ推進団体が乱立。

団体名	設立年月	概要	会員数	主要参加企業
日本ブロックチェーン協会（JBA）	2014年9月	● 仮想通貨及びブロックチェーン技術の健全なビジネス環境と利用者保護体制の整備を進めること目的として設立。活動として、国内での仮想通貨ビジネス振興や、課題解決の自主ガイドラインの制定・施行、ブロックチェーン技術の社会インフラへの応用、政策提言を行っている	計66社 内 賛助会員38社 準賛助会員5社	bitFlyer、Orb、SORAMITSU、Microsoft、GMOインターネットグループ、デロイトトーマツ、IBM、他
ブロックチェーン推進協会（BCCC）	2016年4月	● ブロックチェーンに携わる企業・個人が参加。ブロックチェーンの普及啓発と適用領域の拡大を推進 ● 技術領域の資金調達支援によりブロックチェーン技術の進化に寄与することを目的とする ● 海外のブロックチェーン団体と連携し、国内への情報連携や情報発信を行っている。	計80社	インフォテリア、さくらインターネット、アイリッジ、ビットキャッシュ、Microsoft、GMOインターネットグループ、PwCあらた監査法人、他
ブロックチェーン研究会	2015年12月	● 国内金融機関がブロックチェーン技術の礎を築くことに貢献すると共に、欧米金融機関に比肩する水準まで技術レベルを高めていくことを最終目標として設立。金融システムに対するブロックチェーン技術の活用可能範囲の特定及び、実用化に向けた方向性を定めることを研究会の目的としている ● 2016年11月に国内の銀行間振込業務の実証実験報告を発表	計4社	みずほフィナンシャルグループ、三井住友銀行、三菱UFJフィナンシャルグループ、デロイト トーマツ グループ
国内外為替の一元化検討に関するコンソーシアム	2016年10月	● SBIホールディングスと、子会社のSBI Ripple Asiaが事務局を務める地域金融機関やインターネット銀行を中心としたコンソーシアム ● 国内外為替に必要となる業務について、技術・運用両面で協議を行う ● 2017年3月実証実験実施のうち、商用利用に向けた検証を予定	計42行	りそな銀行、七十七銀行、千葉銀行、横浜銀行、第四銀行、池田泉州銀行、西日本シティ銀行、琉球銀行、新生銀行、セブン銀行、ソニー銀行、他



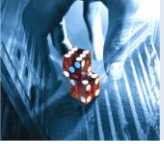
II-A 代表的なイニシアチブ （海外）

NTT DATA

国際的には、R3 Consortiumと、Hyperledger Projectの2強が中心。

団体名	設立年月	概要	会員数	主要参加企業
R3 Consortium	2015年 9月	● ニューヨークのベンチャーR3 CEV社が中心となり、銀行を中心とする金融業における新技術のインフラ作りや法規制への対応等を研究する為に設立 ● 主要発表、実績 2016年1月：Ethereumプラットフォーム検証 2016年3月：債券発行・取引・配当に関する実証実験 2016年7月：みずほFG・SBIホールディングスがR3にて実証実験を共同開催する旨発表 2016年11月：KYCに関する実証実験 2016年4月：独自のブロックチェーン・プラットフォーム「Corda」を発表したが、2016年11月に、Hyperledger ProjectへCordaを無償で提供すると発表	計77社／機関	Barclays、BBVA、J.P. Morgan、Citi、UBS、Bank of America、Deutsche Bank、HSBC、BNY Mellon、中国外貨取引センター、三菱UFJフィナンシャルグループ、三井住友銀行、みずほ銀行、SBIホールディングス、野村ホールディングス、トヨタフィナンシャルサービス、他 ※ゴールドマン・サックス、モルガン・スタンレー、バンコ・サンタンデール、等は脱退表明（2016年11月）
Hyperledger Project	2016年 2月	● Linux Foundationが中心となり、金融業のみならず製造業、不動産契約、IoT、ライセンス管理、エネルギー取引等、様々な業態の要件に対応する事を狙いとし、各分野における業績や知見を共有する事で、堅牢な取引を可能とするシステム構築を目指している ● 主要発表、実績 2016年06月：みずほFG、仮想通貨等検証計画発表 2016年08月：日本取引所グループ　実証実験実施 2016年09月：UBS、貿易金融に関する実証実 2016年11月：R3 Cordaの無償提供受領	計107社	Accenture、ConsenSys、Cisco、IBM、Intel、ABN AMRO、ANZ Bank、BNY Mellon、J.P. Morgan、Wells Fargo、SWIFT、Airbus、富士通、日立製作所、NEC、NTTデータ、R3CEV、他
Global Payments Steering Group (GPSG)	2016年 9月	● Rippleのブロックチェーン・ソリューションを採用し、国際送金の標準仕様を策定することを目的として、北米、欧州、オーストラリアの金融機関によって設立 ● 議長は、Ripple社のアドバイザーDonald Donahue氏	計6社	Bank of America Merrill Lynch、Santander、UniCredit、Standard Chartered,、Westpac Banking Corp、Royal Bank of Canada

＊1：その他SwiftのGPII（Global Payments Innovation Initiative）内におけるブロックチェーンの検討や、Chain、ISO（国際標準化機構）における「ブロックチェーンと電子分散台帳技術に係る専門委員会」等も存在

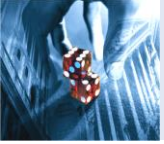


II-B 業態毎の代表的なプレイヤー

NTT DATA

ブロックチェーン業界におけるプレイヤーは、提供者、利用者、評価／推進者と多岐に渡る。

		国内	海外
提供者	ブロックチェーンサービス事業者	• テックビューロ • Orb • ソラミツ • bitFlyer • カレンシーポート • コンセンサスベイス • bitbank • Gaiax、他	• R3 CEV • Ripple • Kraken • CARDANO Labo • Chain • Acronis • Smart Contract • BITNATION、他
	SIer	• NTTデータ • 富士通 • 日立製作所 • NEC、他	• IBM • Microsoft • Cisco • Samsung • Tata • Intel、他
	コンサルティング会社	• NTTD経営研究所 • 野村総合研究所 • ISID • ベイカレント、他	• Accenture • Deloitte • IBM • PwC、他
利用者	金融機関	• 三菱UFJ FG • 三井住友 FG • みずほ FG • 三井住友信託銀行 • SBIホールディングス • オリックス • 大和証券グループ • 野村ホールディングス • 日本取引所グループ • 山陰合同銀行 • 静岡銀行 • 横浜銀行、他	• J.P. Morgan • Wells Fargo • Bank of America • Goldman Sachs • Banco Santander • OCBC • ANZ • ICICI Bank • Nasdaq • SWIFT • Visa • MasterCard、他
	その他事業者	• オートバックスセブン • 凸版印刷、他	• Walmart (US) • Everledger (UK)、他
第三者評価／推進者	政府、自治体	• 金融庁 • 経済産業省 • 日銀 • 自民党、他	• MAS • エストニア政府 • Royal Mint（イギリス王立造幣局）、他
	法律／会計事務所	• 森・濱田松本法律事務所 • 創法律事務所 • 西村あさひ法律事務所、他	• Selachii LLP (UK) • Deloitte Touche Tohmatsu • KPMG、他
	大学	• 早稲田大学 • 東京大学 • 慶応大学 • 会津大学、他	• Holberton School (US) • Blockchain University (US)、他



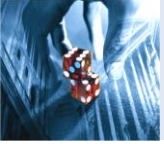
NTT DATA

Ⅰ. ブロックチェーンとは
- A）ブロックチェーンの構成要素
- B）コンセンサスアルゴリズム
- C）参加方法による分類
- D）ブロックチェーン基盤の種類

Ⅱ. ブロックチェーンの関連団体・プレイヤー
- A）代表的なイニシアチブ
- B）業態毎の代表的なプレイヤー

Ⅲ. ブロックチェーンの活用可能性
- A）ブロックチェーンの利点と課題
- B）具体的なUse Case

添付
- A）通貨としてのブロックチェーンにおける各国対応
- B）通貨としてのブロックチェーンにおける日本の関連法規制

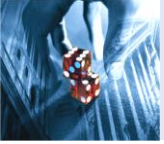


Ⅲ-A ブロックチェーンの利点と課題
ブロックチェーン技術の利点

NTT DATA

無条件な利点に関しては2つ、残り3つは現状課題を有するが利点として活用できる可能性。

①データの 透明性・トレーサビリティ	• 参加者全員が**同一の情報を共有可能** • 取引の実行順を管理しており**追跡が容易**
②関係者間の直接的な 情報の共有・管理	• 対等なコンピュータ（参加者）が**仲介者を介さずに取引を実行**可能
③改ざんが困難な仕組み ／記録の不可逆性	• 分散環境で高い**改ざん耐性**を実現、**記録の変更が困難** 【課題あり】 ✓ 改ざんが困難かつ不可逆であるゆえ、何らかの原因で**正しくない情報がブロックチェーンに書き込まれてしまった場合の運用対処**は重要な観点
④実質的な ゼロ・ダウンタイム	• 分断耐性に優れ、単一障害点が無いため、**可用性が高い** 【課題あり】 ✓ ブロックチェーンの信頼性は参加者が担保する仕組みの為、**合意形成に必要な台数（＝信頼性を保証するレベル）に満たない場合、システムを停止する選択肢**も必要
⑤コスト低減の 可能性	• 柔軟性の高いシステム構築が可能で、**コスト低減**につながる可能性 【課題あり】 ✓ ブロックチェーンによる開発・運用コストの定義は、**既存システムの置き換えと新規ビジネス適用とでは考え方が全く異なる、また機能要件が多いシステムは低減効果少**



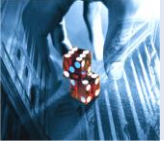
Ⅲ-A ブロックチェーンの利点と課題
ブロックチェーン技術の課題

NTT DATA

前頁に加えて、現状更に6個の課題（論点）があると言われている。

⑥権限管理・暗号化	• 悪意ある参加者に対する配慮は、コンソーシアム型、プライベート型でも必要 秘匿化・権限は既に各所で検討されているが、機密情報や個人情報の取り扱いには 課題が多い
⑦性能・リアルタイム性	• P2Pネットワーク上で、単一の情報を転送を繰り返しながら共有するため、レスポンス タイムやスループットを一定以上上げる事は非常に困難＊1 リアルタイム性を求められる領域での適用は難しいとされている
⑧データ同期の タイムラグ	• すべてのノードで一斉に同期が行われないため、データの受信時刻、処理時刻情報 などがノード間で異なると、業務に支障を来たす場合がある。（例：金融取引では、 電文処理日時がノードごとに異なると、取引が検索できない事態が懸念される）
⑨ファイナリティの確保	• 採用するコンセンサスアルゴリズムによっては、どの取引が有効または無効になったか が判断しにくく、ファイナリティが確保できない（例：PoWなど） • 一方、ファイナリティを確保できるPBFTなどのコンセンサス・アルゴリズムは、ノード数を 増やすとスループットが低下する性質がある
⑩システム 運用・ガバナンス	• 一度ブロックチェーン上に配置したプログラムは変更できない前提に対して、後日 追加、更新プログラムをどのようにリリースするか。悪意ある参加者によって、合意 形成を操作される懸念（PoWの51%問題＊2など）へのガバナンス対策が必要
⑪スケーラビリティ、 リソースの全体最適化	• 時間の経過と共に、取引件数の累積によって、ブロック情報は必然的に肥大化 ノードによっては、ハードディスク容量や実行時間の増加が将来懸念される＊3 • ビットコインでは、マイニングに消費される電力として、推計で約14,700米ドル/日 相当の電力消費したとの報道もあり＊4、また別途マイニング報酬＊4も存在

＊1：ビットコインの処理能力は1秒間に最大7取引（＝60万件/日、楽天銀行＝56万件/日とほぼ同件数）、BitFury社の論文によれば実際にはこれよりも小さい値だと言われている
＊2：ビットコインでは土地代や電気料が安価な中国の参加者が大挙してマイニングに参加し、ビットコインのマイナーの過半数を占める結果になった
＊3：ビットコインでは現時点でブロックチェーン情報が70-80GBに及び、今後確実に増大（3か月で1GB程度）する事からHD容量の圧迫や初回実行時間の増加が懸念されている
＊4：マイニング業者大手のBitFury社ではマイニングセンター設立に1億ドル/拠点物資金を投入しているという記事もアリ　＊4：現在のレート換算で680億円/年程度



III-B 具体的なUse Case
適用可能性が見込まれる領域

NTT DATA

モノの移動や記録が必要で、あまりリアルタイム性が求められない領域は適用可能性

赤字：次ページ以降にて具体的な「実用化に向けた取組」を記載

金融

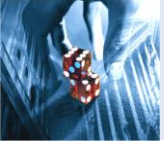
1. 仮想通貨（地域通貨、社内通貨、等）
2. 電子マネー プラットフォーム
3. Payment プラットフォーム
4. Clearing／Settlement プラットフォーム
5. 国内／外国送金
6. 為替、両替
7. 資金調達（クラウドファンディング）
8. Core banking／共同化 プラットフォーム
9. 証券 プラットフォーム
   （株式・デリバティブ取引、証券決済、等）
10. 電子記録債権、貿易金融
11. 保振決済照合
12. 債権管理
13. 融資契約管理
14. KYC、AML
15. 保険
16. 金融機関社内インフラシステム
    （情報系、チャネル系、その他業務系）

等

金融以外

1. 所有権登記・登録（不動産／動産、自動車、等）
2. 無形財産使用権管理
   （音楽・映画等のデジタル製品のコピー防止、
   その他知的財産、ライセンス、等）
3. 利用権管理（レンタル、シェアリング、等）
4. 貴金属、美術品、等の管理（盗難、鑑定書）
5. 診療、犯罪、裁判、等の途上／過去履歴管理
6. 取引記録、取引ライフサイクル管理
7. 自治体（予算と執行、公約）
8. 工程管理、IoTの実行管理
9. 商品販売・予約（中古市場、P2P、等）
10. 投票
11. 税
12. IDカード
13. ポイント、マイレージ
14. 保証書
15. 災対センター

等

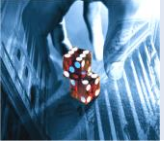


Ⅲ-B 具体的なUse Case 実用化に向けた取組（1/4）

NTT DATA

実用まで至っているものは無いが、送金に関する各金融機関の関心は高い。

		国内	海外
金融	1. 仮想通貨	**実験・PoC** • 三菱東京UFJ銀行（仮想通貨 MUFGコイン） • みずほ銀行（仮想通貨 みずほマネー） • 飛騨信用組合（地域仮想通貨）	**実験・PoC** • Citi（仮想通貨 Citiコイン） • BNY Mellon（仮想通貨） **調査・検討** • UBS（仮想通貨） • 中国人民銀行（仮想通貨） • ゴールドマンサックス（仮想通貨SETLcoin×Wallet）
	3. Payment プラットフォーム		**実験・PoC** • 三菱東京UFJ銀行@シンガポール（小切手電子化）
	5. 国内／外国送金	**実運用** • リクルート（米Align Commerce Corporation）（※リクルートストラテジックパートナーズが運営する合同会社RSPファンド6号を通じての出資） **実験・PoC** • みずほFG、SBIホールディングス（国際送金） • みずほFG、三井住友銀行、MUFG（国内送金） **調査・検討** • 三菱東京UFJ銀行（国際送金） • 横浜銀行、住信SBIネット銀行、りそな銀行、等（国内送金） • ふくおかFG×ハウインターナショナル（国内送金）	**実験・PoC** • Santander UK（国際送金） • Visa×Chain B2B Connect（国際送金） • Wells Fargo、ANZ（国際送金） • Standard Chartered（国際送金） • OCBC（国際送金） • ATB Financial Canada（国際送金） **調査・検討** • Bank of America（国際送金） • J.P. Morgan（国際送金） • Banco Santander（ユーロ圏送金） • SEB（国際送金） • KB Korea（国際送金） • SWIFT（国際送金）
	7.資金調達（クラウドファンディング）		**実運用** • Slock.it（The DAO クラウドファンディング）

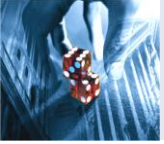


III-B 具体的なUse Case
実用化に向けた取組（2/4）

NTT DATA

証券分野での取組も盛んに行われている一方、勘定系・ACH等の検討は限定的。

		国内	海外
金融	8. Core Banking／共同化プラットフォーム	**実験・PoC** • 住信SBIネット銀行（勘定系システム）	**実験・PoC** • BC Finance Myanmar（融資・貯蓄基幹システム） **調査・検討** • SWIFT（研究レポート）
	9. 証券プラットフォーム	**実験・PoC** • 日本取引所グループ×日本IBM×野村総研（ポストレード業務） • みずほ銀行（証券クロスボーダー取引） **調査・検討** • 三井住友信託銀行（有価証券管理） • 東京証券取引所、大阪証券取引所、日本証券クリアリング機構（証券取引）	**実運用** • Nasdaq（未公開株式取引システム「Nasdaq Link」） • Overstock（有価証券授受システム） **実験・PoC** • BNP Paribas（ポストトレード業務） • ヤンゴン証券取引所（証券決済業務） **調査・検討** • Nasdaq（株主投票） • Royal Mint（UK）（金トレード商品） • UBS（スマート債券プラットフォーム）
	10. 電子記録債権、貿易金融	**調査・検討** • 全国銀行協会（※検討会にて適用可能性全体） **実験・PoC** • オリックス＆銀行、静岡銀行（貿易金融取引） • MUFG×Chain（約束手形）	**実験・PoC** • Barclays（貿易金融取引） • UBS（貿易金融取引） • Bank of America & HSBC＋IDA（貿易金融取引） • DBS、Standard Chartered（貿易金融取引）
	12. 債権管理	**調査・検討** • 三井住友信託銀行（債権流動化業務）	**実験・PoC** • R3（債権発行・取引・配当システム）
	13. 融資契約管理	**実験・PoC** • みずほ銀行（シンジケートローン）	**実験・PoC** • South African Reserve（シンジケートローン）

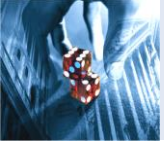


III-B 具体的なUse Case 実用化に向けた取組（3/4）

NTT DATA

非金融分野では一部政府主導にて実用化に至っている事例も存在。

		国内	海外
金融	14. KYC、AML	調査・検討 • 楽天証券×ソラミツ（KYC）	実験・PoC • R3（KYC） • ING Bank（認証）
	16. 金融機関社内インフラシステム	調査・検討 • 三菱東京UFJ銀行（契約管理（※詳細領域不明）） • 三井住友銀行（ブロックチェーン研究（※詳細領域不明））	実験・PoC • J.P. Morgan（社内ネットワーク） • ING Bank（セキュリティ向上目的の実証実験（※詳細領域不明）） 調査・検討 • Kasikornbank Thailand（銀行システム） • USAA（バックオフィス業務効率化）
金融以外	1. 所有権登記・登録		実験・PoC • スウェーデン政府（不動産・土地登記） 調査・検討 • 香港政府（土地所有権管理）
	3. 利用権管理	実験・PoC • AMBITION（不動産賃貸の権利の発行・流通管理）	実験・PoC • ロイズ×セーフシェア（車や部屋の賃貸履歴管理）
	4. 貴金属、美術品、等の管理		実運用 イギリス Everledger社（ダイヤモンド鑑定・所有者・保険情報を管理）
	5. 診療、犯罪、裁判、等の途上/過去履歴管理		実運用 • エストニア政府（医療データ管理） • エストニア政府（外国人ID「e-resident」） • フィリップス×Tierion（健康状態記録）



III-B 具体的なUse Case
実用化に向けた取組（4/4）

NTT DATA

		国内	海外
金融以外	6. 取引記録、取引ライフサイクル管理	実験・PoC • オープンイノベーションラボ他（有機農産品情報管理）	実運用 • 南アフリカ（スマートメーター） 実験・PoC • アメリカ Walmart社（中国から輸入する食品の管理）
	7. 自治体	実験・PoC • 凸版印刷（自治体向けサービス） • 東京大学 会津大学 国際大学ｸﾞﾛｰﾊﾞﾙｺﾐｭﾆｹｰｼｮﾝｾﾝﾀｰ（会津地域ブロックチェーン活用実験）	
	8. 工程管理 IoTの実行管理	調査・検討 • 経済産業省（IoT分野に広げるための調査研究）	調査・検討 • IBM & SAMSUNG "ADEPT"（IoTのデータ管理にブロックチェーン活用を研究） • マン島（IoTへの応用を試験） • Philips社（ヘルスケア領域での活用検討） • ディズニー"Dragonchain"（待ち時間／行列監視等）
	9. 商品販売・予約	実験・PoC • オートバックスセブン（中古カー用品のC2C売買）	実験・PoC • オーストラリア Webjet社（ホテル予約・支払管理）
	12. ID		実運用 • アメリカ Holberton School（学生の成績情報管理）
	13. ポイント、マイレージ	実験・PoC • 静岡銀行　マネックスグループ（クーポン・ポイントウォレット「NeCoban」） • 三菱東京UFJ銀行　カブドットコム証券（大手町エリアポイントウォレット「OOIRI」）	
	14. 保証書		実運用 • 中国 Factom社（電子文書の公証管理）

III-B 具体的なUse Case
（参考）貿易金融をテーマにした実証実験

NTT DATA

現状、電子通知でも数日要していたL/C取引を、最短数分で情報閲覧可能にまで短縮。

★:BC基盤提供者

発表	• 2016年7月（2月22日より共同研究を開始）
活動進展度	調査・検討 ／ **実証実験・POC** ／ 実運用
対象ビジネス	• 貿易金融
参加プレイヤー	• オリックス • オリックス銀行 • 静岡銀行 ★NTTデータ • NTTドコモ・ベンチャーズ
基盤、アルゴリズム	• 非公開 • 非公開
実験概要	■ 信用状注（Letter of Credit：L/C）の取引について国内初BC技術を適用したプロトタイプシステムの検証を完了 • 貿易取引は輸送時間を要し、商品引渡と代金決済のタイムラグが発生 • 関係者も多く取引が複雑な為、輸出／輸入者のリスク回避の為、銀行が信用状を発行、郵送やEメール等で事務手続き実施 • 輸出者が信用状の発行依頼の段階で情報が共有される事で、信用状の誤りが発生した場合も早期に検知が可能、修正手続きも迅速 • 今後、インボイス、船荷証券などの船積書類をBC上で同時共有する事で貿易金融業務全般でBC技術のメリットが享受できる可能性

ORIX　ORIX オリックス銀行　静岡銀行

図1. 従来型システムの処理の流れ

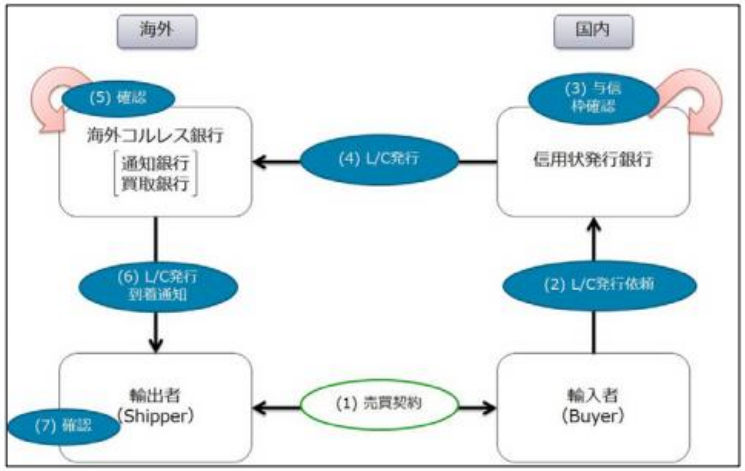
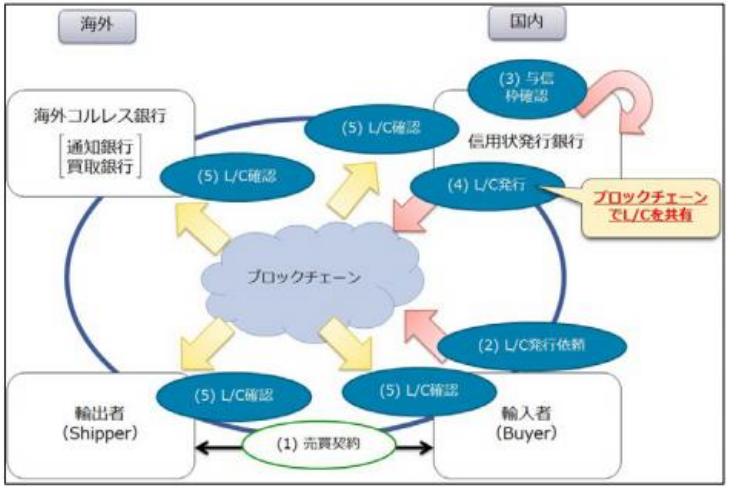


図2. ブロックチェーン技術を活用した処理の流れ



Ⅲ-B 具体的なUse Case
（参考）国内銀行間振込業務をテーマにした実証実験

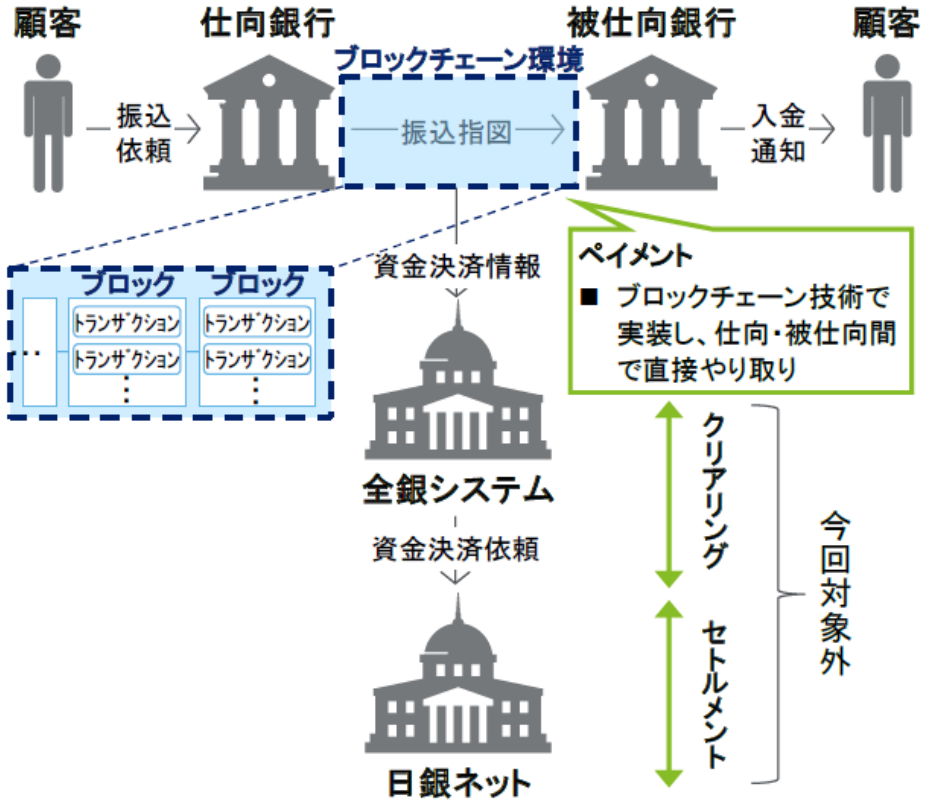
スループット、改ざん耐性、データ完全性で一定の効果を確認。

★:BC基盤提供者

発表	• 2016年11月（2015年12月に研究会設立）
活動進展度	調査・検討 ／ **実証実験・POC** ／ 実運用
対象ビジネス	• 国内振込
参加プレイヤー	• みずほ FG • 三井住友銀行 • 三菱UFJ FG • デロイトトーマツグループ ★ bitFlyer
基盤、アルゴリズム	• 非公開（Hyperledger？） • PBFT類似の独自
実験概要	■ **全銀システムが対応するペイメント業務**をBC技術で実現 • 144行が参加する前提で環境構築をした大規模な国内送金の実証実験 • 1拠点のスループット（データ処理量）は、**1,500件/秒で全銀システムのピーク時処理能力1,388件/秒を達成** • BCの分岐が発生しない仕組みで行った為、51%攻撃による改ざん攻撃を排除可能 • また全体で一貫した原簿の共有が可能な為、データ完全性上も問題が無い • 今後、**可用性レスポンスタイム、拡張性、保守性、セキュリティ等において更なる確認・改善**が必要

MIZUHO みずほフィナンシャルグループ　三井住友銀行 SMBC　MUFG

実証実験における対象範囲



Ⅲ-B 具体的なUse Case
（参考）国内銀行間振込業務をテーマにした実証実験

サンタンデールはリップル基盤の中で、IOUを利用者間でやり取りする事で間接的に送金を実現。

★:BC基盤提供者

発表	• 2016年6月（2015年中頃からUse Case選定）
活動進展度	調査・検討 ／ 実証実験・PoC ／ 実運用
対象ビジネス	• 国際送金
参加プレイヤー	• Santander U.K.（Banco Santander英国法人）　★ripple
基盤、アルゴリズム	• Ripple　• RPCA
実験概要	■ BC技術による国際送金アプリを約6,000名の行員へ解放、GBP/USD/EURにて10GBP～10,000GBP迄の送金が可能 • 上位50位以内の銀行のうち15行がRippleと提携（スタンダードチャータード、NAB、MHFG、BMOフィナンシャル・グループ、サイアム商業銀行、上海華瑞銀行、ウニクレディト、UBS、RBC、ウエストパック銀行、ライゼバンク、CIBC、ナショナル・バンク・オブ・アブダビ、ATBフィナンシャル、フィドール銀行、等） • 現在EUR21カ国、USDアメリカに数秒で送金可 • 送金アプリはApple Payに連動 • 2016年11月にBanco Santander、ripple、ゴールドマン・サックスらがR3コンソーシアムを脱退

Santander

Santander Becomes First U.K. Bank to Introduce Blockchain Technology for International Payments

Jun 01, 2016　03:45 PM　by Giulio Prisco

Santander U.K. has announced its introduction of blockchain technology for international payments through a new app that is currently being rolled out as a staff pilot. The bank plans to make the application, which is only available on Apple's iOS, available to consumers after it completes the pilot program. The announcement makes Santander the first bank in the U.K. to use blockchain for international payments.

Ⅲ-B 具体的なUse Case
（参考）行政サービスの電子化への実装

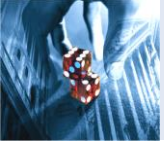
エストニア政府はガードタイム社と共にブロックチェーンを活用した電子政府実現を果たし始めている。

★:BC基盤提供者

発表	• 2015年12月
活動進展度	調査・検討 ／ 実証実験・PoC ／ 実運用
対象ビジネス	• 非居住者カード、医療記録、等
参加プレイヤー	• エストニア政府 ★ガードタイム
基盤、アルゴリズム	• KSI（Keyless Signature Infrastructure）
実験概要	■ 国民ID、X－Road（既存のレガシーシステム同士を結ぶ相互連携ネットワーク）へのKSI導入にて、公証サービスを提供開始 • 130万人のエストニア国民の生涯の健康・医療データの記録管理にブロックチェーンの利用試験を開始 • 加えて、e-Residencyと呼ばれる非居住者向けIDカードの管理にブロックチェーンを活用 • 今後更に、不動産情報の登録、公文書のアーカイブ、等にuse caseを広げて、ブロックチェーンの電子政府化への貢献を促進予定

guardtime

Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents

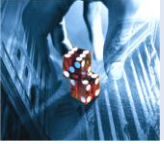


I. ブロックチェーンとは
- A）ブロックチェーンの構成要素
- B）コンセンサスアルゴリズム
- C）参加方法による分類
- D）ブロックチェーン基盤の種類

II. ブロックチェーンの関連団体・プレイヤー
- A）代表的なイニシアチブ
- B）業態毎の代表的なプレイヤー

III. ブロックチェーンの活用可能性
- A）ブロックチェーンの利点と課題
- B）具体的なUse Case

添付
- A）通貨としてのブロックチェーンにおける各国対応
- B）通貨としてのブロックチェーンにおける日本の関連法規制



添付-A
通貨としてのブロックチェーンにおける各国対応

NTT DATA

各国の対応は様々。ただ比較的先進国は仮想通貨容認、無課税措置の方針が多い。

		政府／中央銀行の規制状況		民間サービスの状況	
容認	ドイツ	2013年8月	ビットコインを「プライベートマネー」と見なして課税対策	2013年10月	ビットコイン取引所"Kraken"がドイツのオンライン金融機関Fidor銀行と専属パートナーシップ
	カナダ	2013年11月	ビットコインと交換した物・サービスの価値のカナダドル相当を収入とみなして課税対象	2013年10月	バンクーバーにATMを世界で始めて設置
	ノルウェー	2013年12月	ビットコインを資産として扱い、資産譲渡益を課税対象		
	シンガポール	2014年1月	売買に対しては物品税7%を課税、ただし中央銀行は通貨と認めずに利用に対して注意喚起	2014年2月	ATMの設置あり
	スウェーデン	2014年1月	税法上の扱いを美術品と同じにする方針		
黙認	アメリカ	2014年2月	FRBイエレン議長　ビットコインについて「FRBは監督もしくは規制する権限を持たない」と発言	2013年2月	Appleがビットコインアプリ"Blockchain"をStoreから削除
				2014年2月	ATMの設置有り
	イギリス	2014年3月	仮想通貨が法定通貨と交換される場合は無税、仮想通貨で販売される場合、付加価値税の課税対象	2014年1月	世界初の保証付ビットコイン保管サービスが登場。保険取引所ロイズ保険引受
警告	インド	2013年12月	インド中央銀行がビットコインを含むデジタル通貨の利用リスクを警告も、規制の計画はないと発表	2013年12月	最大手の取引所が閉鎖、その後、他の取引所も追随
	香港	2014年1月	「詐欺やマネーロンダリング等の不正行為にビットコインを利用することは法律のもと禁止」と警告	2014年	ATMの設置有り
				2014年	ビットコインを販売する現実の店舗が開業
	キプロス	2014年2月	中央銀行による警鐘		
違法／禁止	タイ	2014年2月	中央銀行：バーツと交換される限りにおいて、ビットコイン取引は適法、ただ外貨との交換は禁止と発表		
	ブラジル	2013年10月	ビットコインを含む電子マネーによるオンライン決済にガイドラインを設け、事実上ビットコインを禁止		
	中国	2013年12月	中国人民銀行、国内の金融機関にビットコインの取扱を禁止する通達を指示 また公的金融機関による扱いに制限	2013年12月	検索サイト"百度（バイドゥ）"がビットコインの支払受付を停止
				2013年12月	最大手の取引所"BTC China"が新規デポジット受入を停止
	ロシア	2014年2月	ロシア検察総長室「法律はルーブルを唯一の公式通貨と定めており、ビットコインは違法」と表明		

添付-B
通貨としてのブロックチェーンにおける日本の関連法規制

NTT DATA

仮想通貨に対する改正資金決済法
（2016年5月25日成立、6月4日公布、1年以内に施行予定）

①仮想通貨の定義（第2条の5）

- 不特定多数間での物品購入・サービス提供の決済・売買・交換に利用できる「財産的価値」で、情報処理システムによって移転可能なものと定義（つまり法定通貨ではないが、決済手段の一つと解釈）

②仮想通貨交換業に係る登録制の導入（第63条の2）

- 仮想通貨交換業を定義し（第2条の7）、仮想通貨交換業者に資本要件・財産的基礎等を満たした上で、内閣総理大臣の登録を義務付け

③仮想通貨交換業者に対する業務規制（第63条関係）

- 仮想通貨交換業者は利用者への取引内容や手数料等の情報提供、システムの安全管理や利用者財産と自己資産の分別管理を行い、定期的にその状況について公認会計士又は監査法人の監査を受ける事が求められている（第63条の11）

④仮想通貨交換業者に対する監督（第63条関係）

- 仮想通貨交換業者は、帳簿書類・報告書の作成、監査報告書を添付した報告書の提出、立入検査、業務改善命令等の監督規制を受ける事
- これに伴い、マネーロンダリング対策としての犯罪収益移転防止法の義務を負う「特定事業者」に仮想通貨交換事業者を追加（第2条）、同法に規定される口座開設時の本人確認義務（第4条）、疑わしい取引の当局への届出義務（第8条）等が適用

仮想通貨の悪用阻止へ
テロ資金対策、規制法成立

ビットコインなどの仮想通貨を規制する改正資金決済法が25日、参院本会議で可決、成立した。公布後1年以内に施行する。仮想通貨への法規制は初めてで、テロ資金や資金洗浄への悪用防止のほか利用者の保護を図る狙いだ。

26日に開幕する主要国首脳会議（伊勢志摩サミット）でもテロ資金対策は主要課題の一つとなっており、具体的な議論が行われる。開催前に法案を成立させたことで、日本のテロ資金対策に対する強い姿勢を示した格好だ。

改正資金決済法は、仮想通貨が事実上の通貨としての機能を持っていると認めた上で、金融庁が監督官庁となり、現金と仮想通貨を交換する取引所に登録制を導入する。

テロ組織に悪用されるのを防ぐため、口座開設時に顧客の本人確認義務や取引記録の保存、不審取引の通報などの義務を課す。金融庁には取引所を検査し、業務改善命令などの行政処分を出す権限を与える。

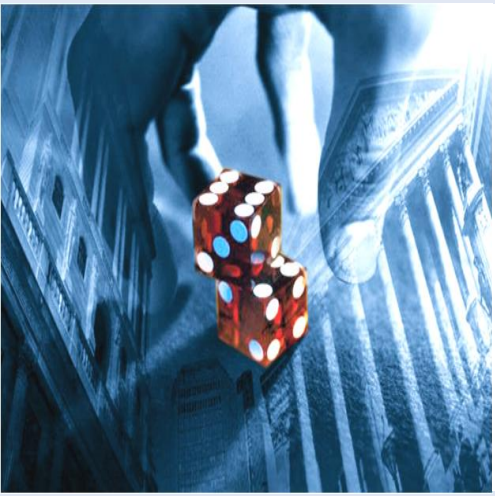
また参院本会議では、金融とITを融合した新たな金融サービス「フィンテック」の普及を促すため、銀行持ち株会社がIT企業を買収できるようにする改正銀行法も成立した。

ビットコインなどインターネット上で流通する仮想通貨を購入する際にかかる消費税が2017年7月からなくなる。利用者はこれまでより消費税分だけ実質的に安く買える利点がある。

ビットコインなどの仮想通貨は専門の取引所を通じて買える。円やドルなどで購入でき、銀行振り込みやクレジットカード決済で支払うケースが多い。現在は購入時に8%の消費税がかかり、利用者は取引所の手数料と一緒に支払っている。

（2016/12/8 自民党・公明党による平成29年度税制改正大綱で発表）

■ 仮想通貨購入は消費税ゼロ



ご清聴ありがとうございました！

【お問い合わせ先】
㈱NTTデータ経営研究所
グローバル金融ビジネスユニット
両角　真樹 Masaki Morozumi
080-7809-4467
morozumim@keieiken.co.jp