金融情報学研究会(Sig-Fin)　講演用資料

台頭する‘2つの新技術’と金融市場
-ブロックチェーンと分散台帳技術-

2017年9月

日本取引所グループ
フィンテックラボ
山藤　敦史

全てはビットコインから始まった

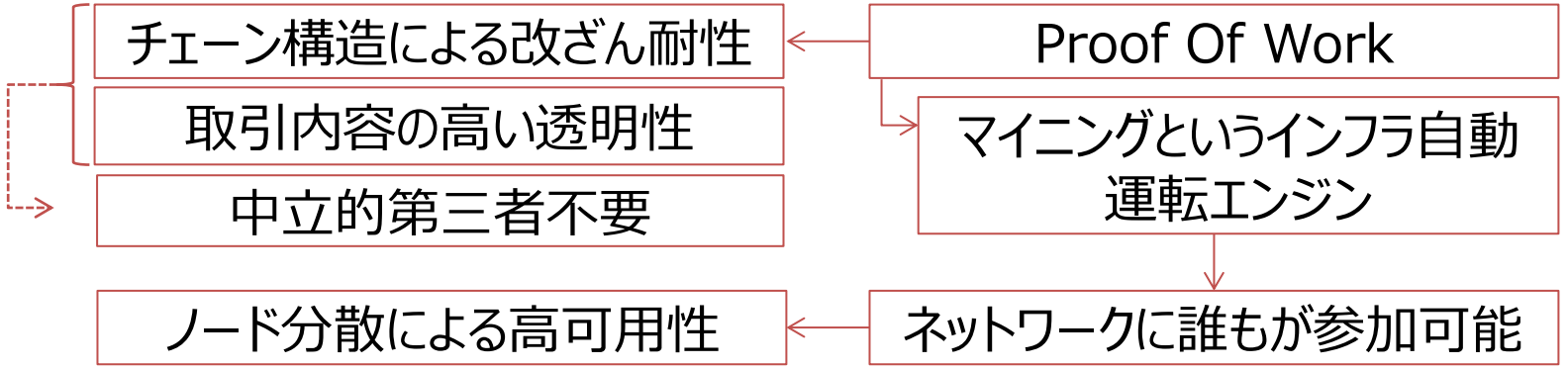
2008年	• 「Bitcoin: A Peer-to-Peer Electronic Cash System」という論文が暗号通貨について議論するメーリングリストに投稿。ちなみに投稿者のサトシ・ナカモトが本当は誰なのかは現在でも議論になっている。
2009年	• 有志が集まってプログラミングし最初のビットコインが発行
2010年	• メーリングリストに投稿された、「ビットコイン1万枚とピザを交換しないか」という冗談に、別の参加者が応じたのが最初の取引

- ✓ **価値を信じる人が一定数いればそれは通貨になり得る**
- ✓ **そこに中央集権的な存在は不要で、ビットコインを支える仕組みや技術への信用があれば良い**

- ✓ **その革新性が人を惹きつけ、コミュニティが拡大**
- ✓ **熱狂が生み出す多くのイノベーション**

ビットコインの技術要素の概要

- ビットコインは複数の要素で組み合わされており、個々の要素技術や考え方は既存のものも多いが、バランスよくデザインされた要素の組み合わせに価値
- 技術的な評価とともに、インセンティブ設計も含めたビジネスモデルとして評価をする必要がある

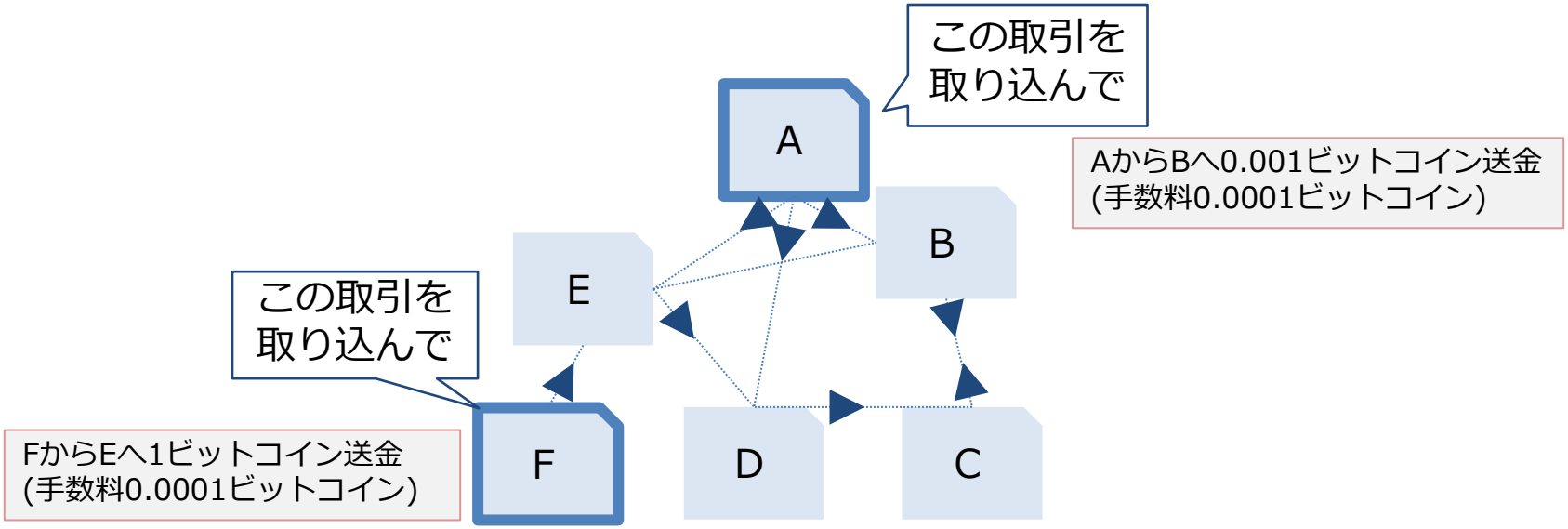


ビットコインブロックチェーンの処理手順(1/4)

①取引発生

取引のブロックチェーンへの記録を依頼する場合は、必要な情報（誰から誰へビットコインを送金したいのか、手数料を幾ら払うのか）をパブリックネットワーク上に送信

(※単純化のため、ウォレットや交換所等の処理を1つのノードにまとめて表現)

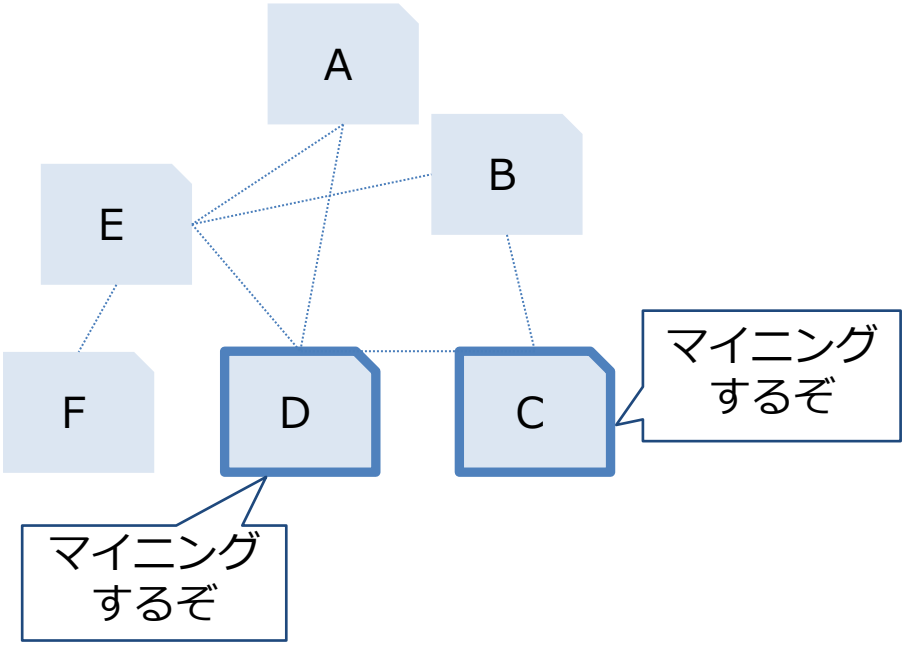


ビットコインブロックチェーンの処理手順(2/4)

②マイニング競争

ビットコインは約10分に1回の間隔で12.5ビットコイン(※2017年9月現在で約550万円相当)が発行。これを手にできるのは、大量の繰り返し計算でしか求められない正解に「最初に」辿り着いた者のみ。(PoW：Proof of Work)

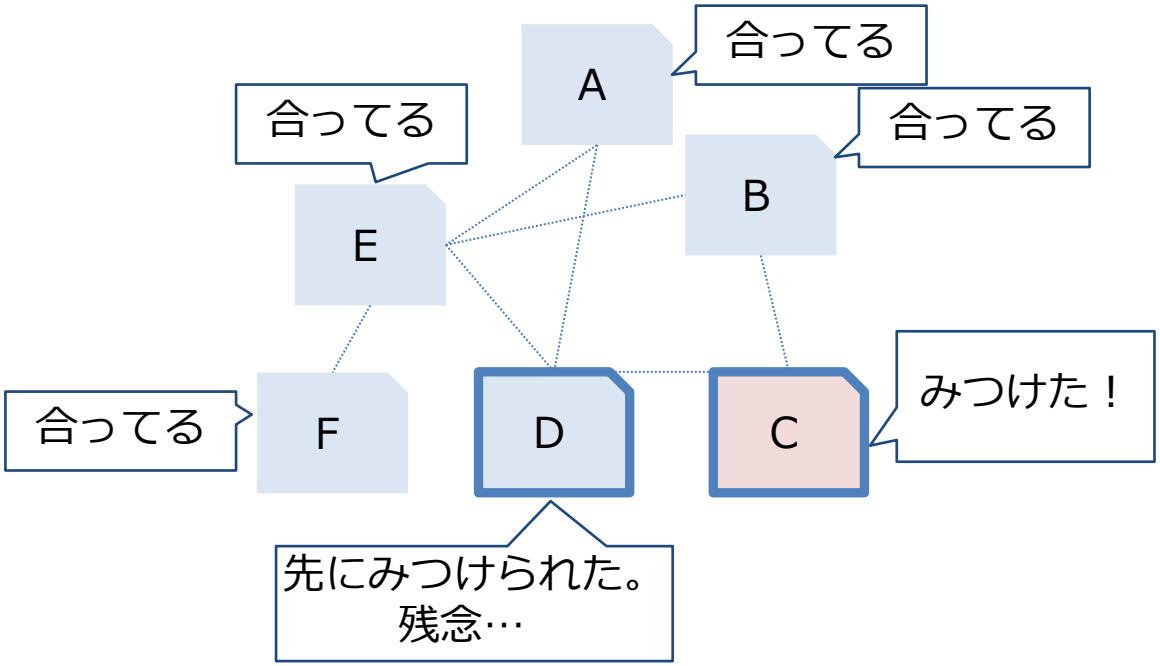
正解の算出にあたって①で発生した取引も(任意で)取り込んで計算され、その際の手数料も報酬。



ビットコインブロックチェーンの処理手順(3/4)

③結果の確認

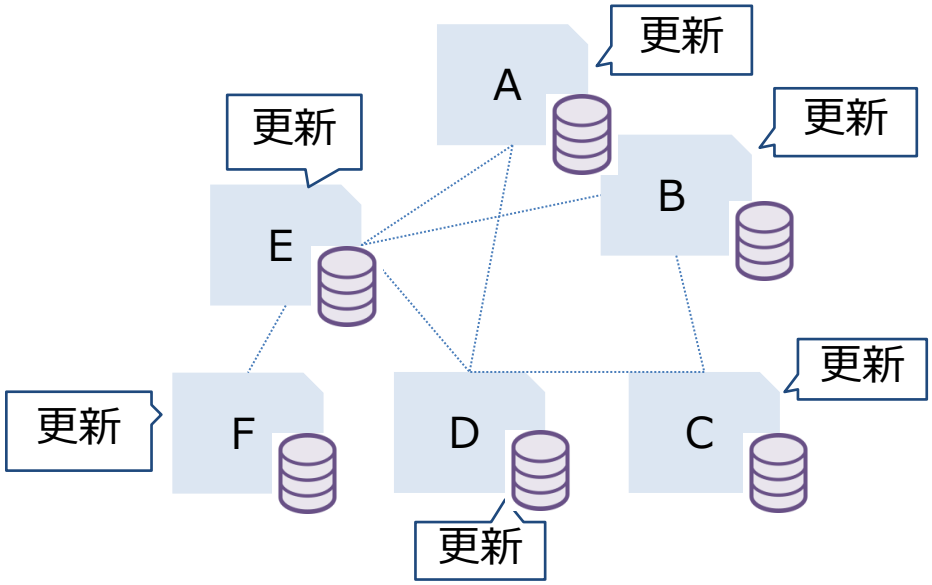
下記例の「C」は、取り込み対象となる取引と発見したナンスを各ノードに伝え、各ノードは正解である事を確認。マイニングで用いられるハッシュ計算は一方向性を持つため簡単に確認する事ができる（ナンスからハッシュ値を求める事は簡単だが、ハッシュ値からナンスを求めるのは繰り返し計算が必要）。



ビットコインブロックチェーンの処理手順(4/4)

④ブロックチェーンへの書き込み

　正解を確認した各ノードは、自分の持っているブロックチェーンに新たなブロックを追記。これで各ノードに分散しているブロックチェーンが同期。



Proof of Work

【問題】
最初のX桁が全て0となるような値(ナンス)を探せ

①前ブロックハッシュ
②今回取り込む取引のダイジェスト値(マークルルート)
③ナンス

暗号学的ハッシュ関数 (SHA256)

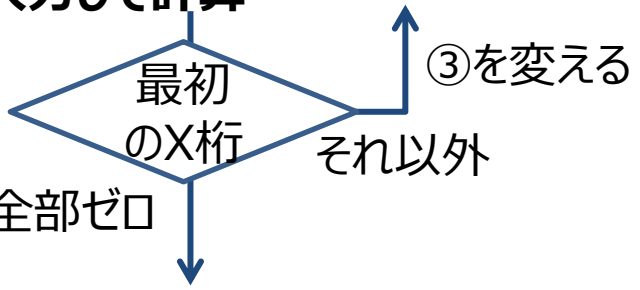
00000000000000006ecee94daaa034bbd026cad52a9d3c6a5b7972716e5d566

解き方

①②は固定(※)で、③に適当な初期値を設定

↓

ハッシュ関数に①②③を入力して計算



この時の③が正解のナンス

- **繰り返し計算でしか正解が導けない作業を課す事で、ブロックの生成の権利を競わせる仕組み**
- **大量の計算を高速で行えるかどうかのマイニングパワー勝負**

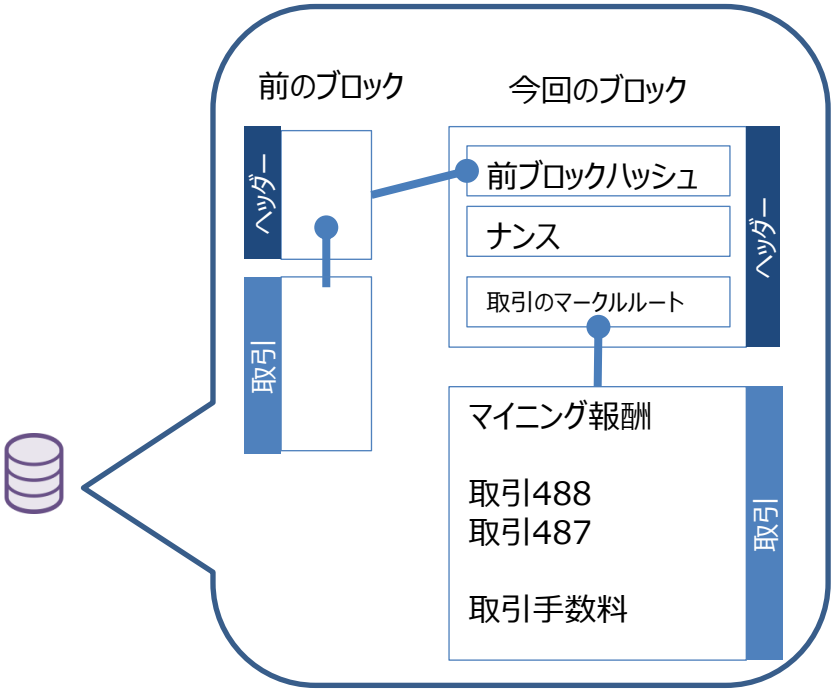
※どの取引をブロックに取り込むかはマイナーによって異なる可能性

なぜ改ざん不可能と言われるのか？

ブロックのチェーン構造とマイニング競争

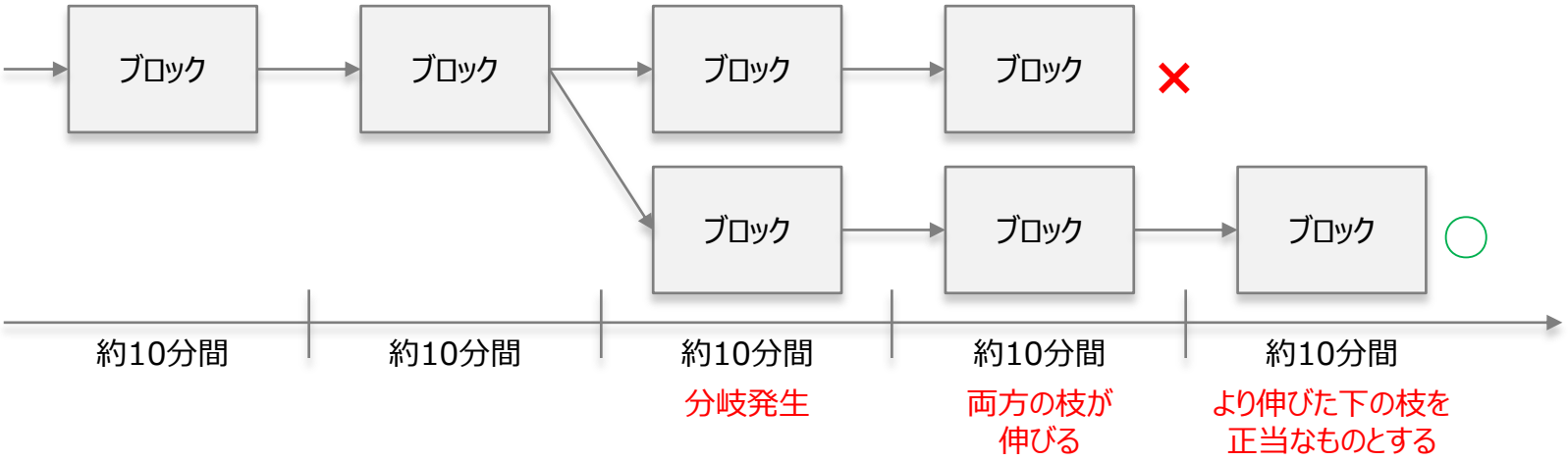
　マイニングは、前ブロックハッシュを含めてナンスを求める必要があるため、自分の望むように過去を改ざんしようと思うと、それ以降の取引のナンスを全て再計算してみつける必要がある。

　世界中で行われるマイニング競争に連続して勝利し続ける事は難しいため、ブロックが積み上がれば、改ざんは実質不可能と言われる。



どうやって‘一番’を決めるのか？

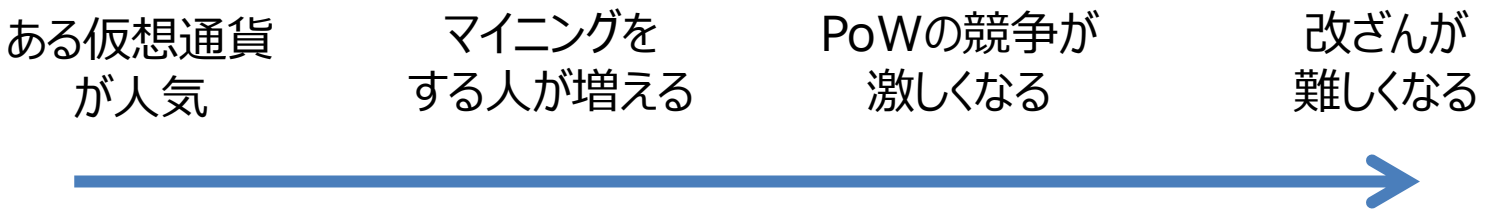
- 世界中でマイニング競争が繰り広げられるため、別々のマイナーが同じタイミングで正解を見つけ出す事もある
- その場合、どちらが先だったという判定をするのではなく、「より長く伸びたブロックチェーンが正しい」というルールが適用される



- このため、瞬間を切り取ってみると複数の状態が併存しながら、長期的に一つの状態に安定していくという性質を持つ
- 金融取引のファイナリティに相当する概念が瞬間的には不安定である事が、後述の分散台帳技術の台頭に繋がっている側面もある

インセンティブモデルが支える改ざん耐性

- PoWによる改ざん耐性は技術だけの問題ではない



- 人気がない仮想通貨では？
- 人気があり過ぎると？

‘信用‘の意味の変化

アドレス毎の取引履歴は誰でも確認する事ができる

＋

履歴は誰にも改ざんできない

＝

- あるビットコインアドレスの所有者が、「○○枚のビットコインを所有している」と主張した場合、誰もが公開履歴によってその正当性を確認できる
- **公証人のような第三者による証明が不要**

⇒ **‘非中央集権性’を支える重要なポイント**

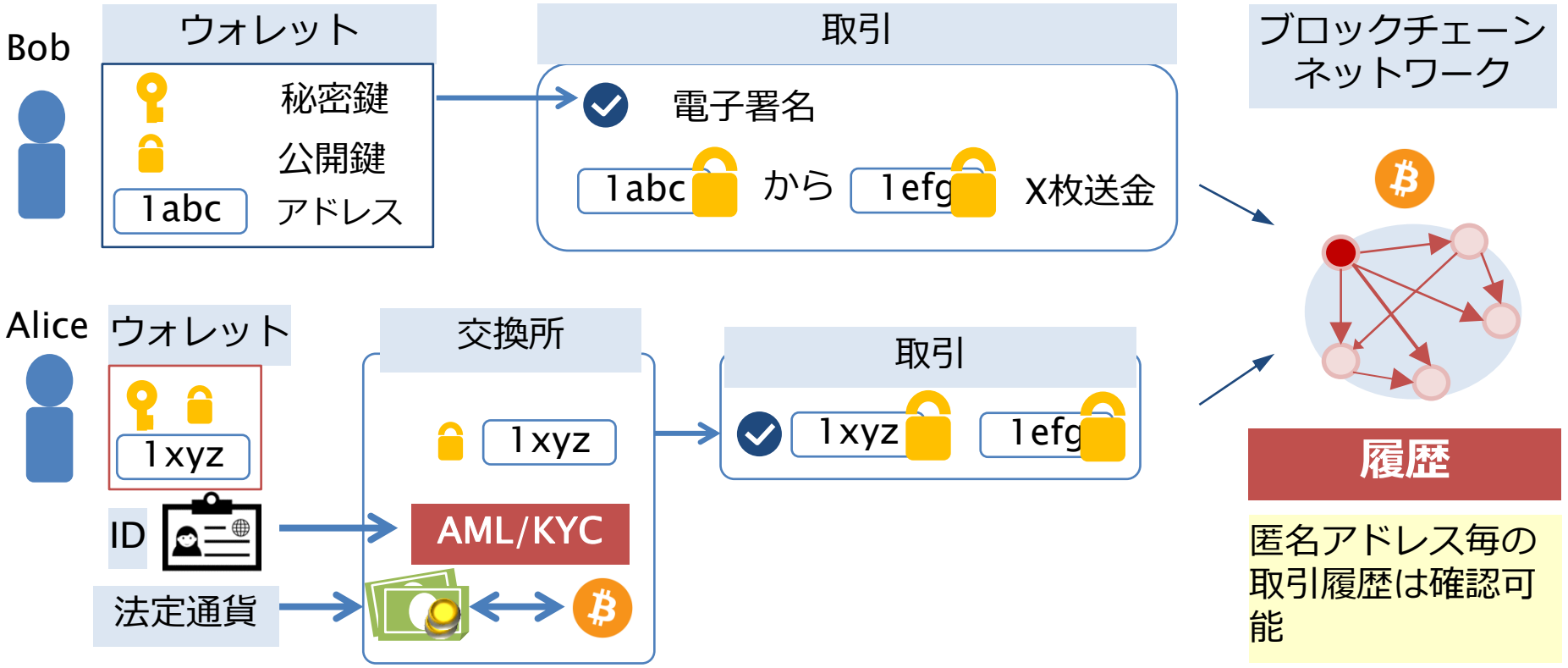
⇒ **権威への信用か、自律的なシステムへの信用か**

セキュリティとは何を指すのか？

- 個人の匿名情報が守られる？
- ハッキングなどで仮想通貨が盗まれない？
- 改ざん耐性？
- 人によって知りたいポイントが違う

匿名性

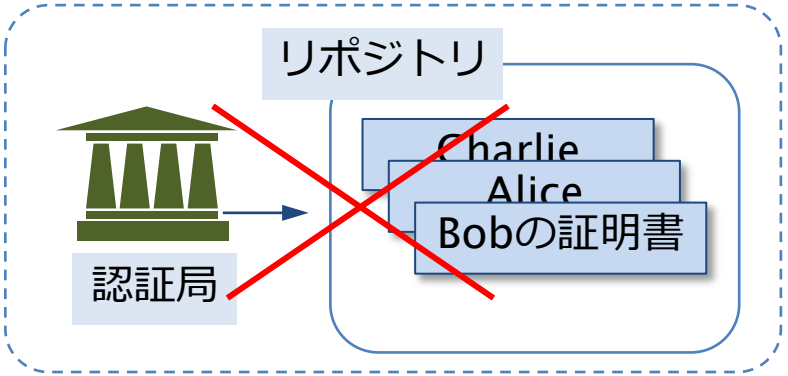
匿名性　アドレスと個人を紐付けるのはネットワークの履歴からは困難だが…

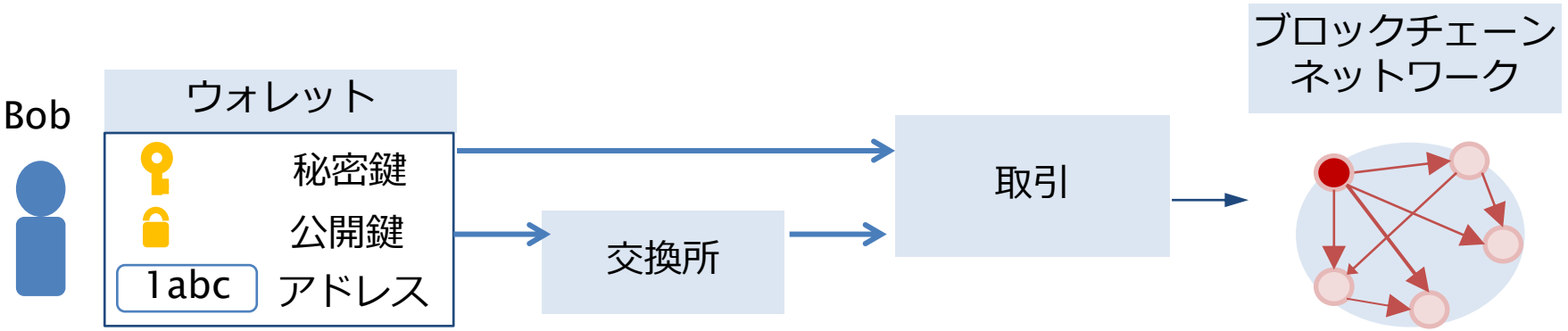


個人が交換所を通して売買すればアドレスとの紐付けが可能

無くしたら、盗まれたら？

- ビットコインは公開鍵暗号技術を用いているが、基盤を利用しているわけではない
- 認証局も失効手続きもない





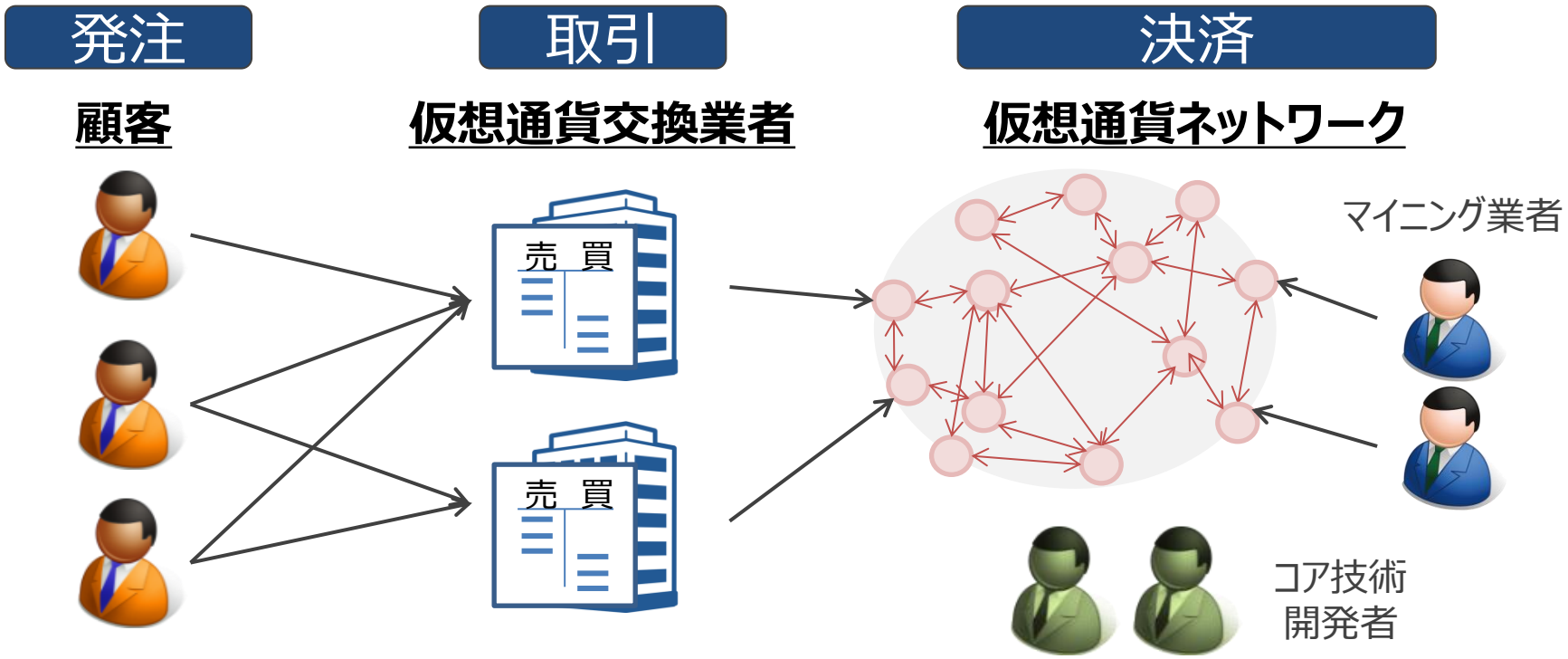
秘密鍵を無くした ⇒ ほぼ永久に亡くなったまま

秘密鍵を盗まれた ⇒ 秘密鍵の所有者＝ビットコインの所有者

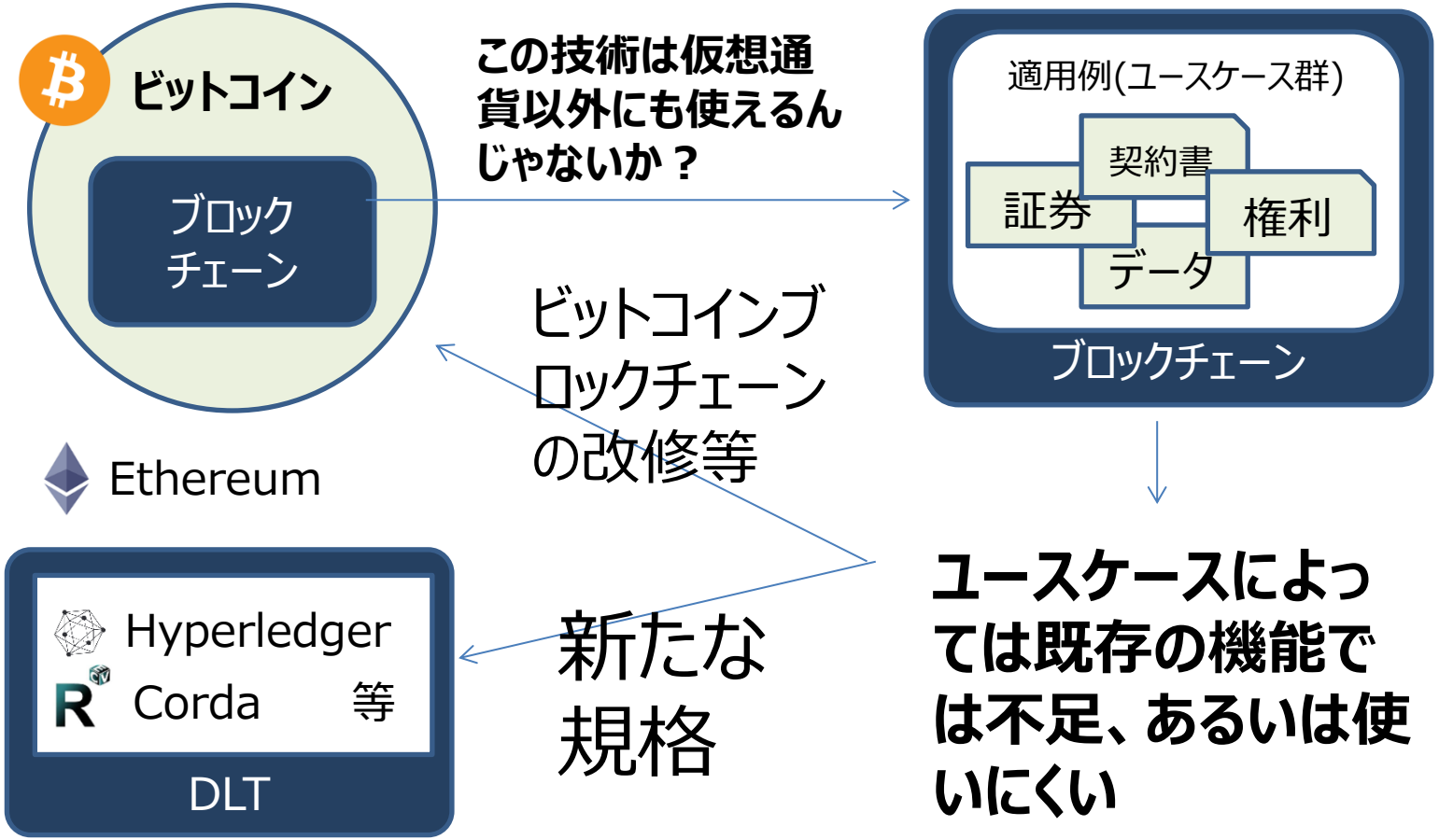
盗難･紛失への耐性は物理的な紙幣やコインに近い

証券取引の視点からみた仮想通貨市場

- 仮想通貨交換業者　→ **「証券会社」に近い**役割
  各業者の「板」が独立しておりSORもない
- 仮想通貨ネットワーク　→ グローバルに統一された**決済インフラ**

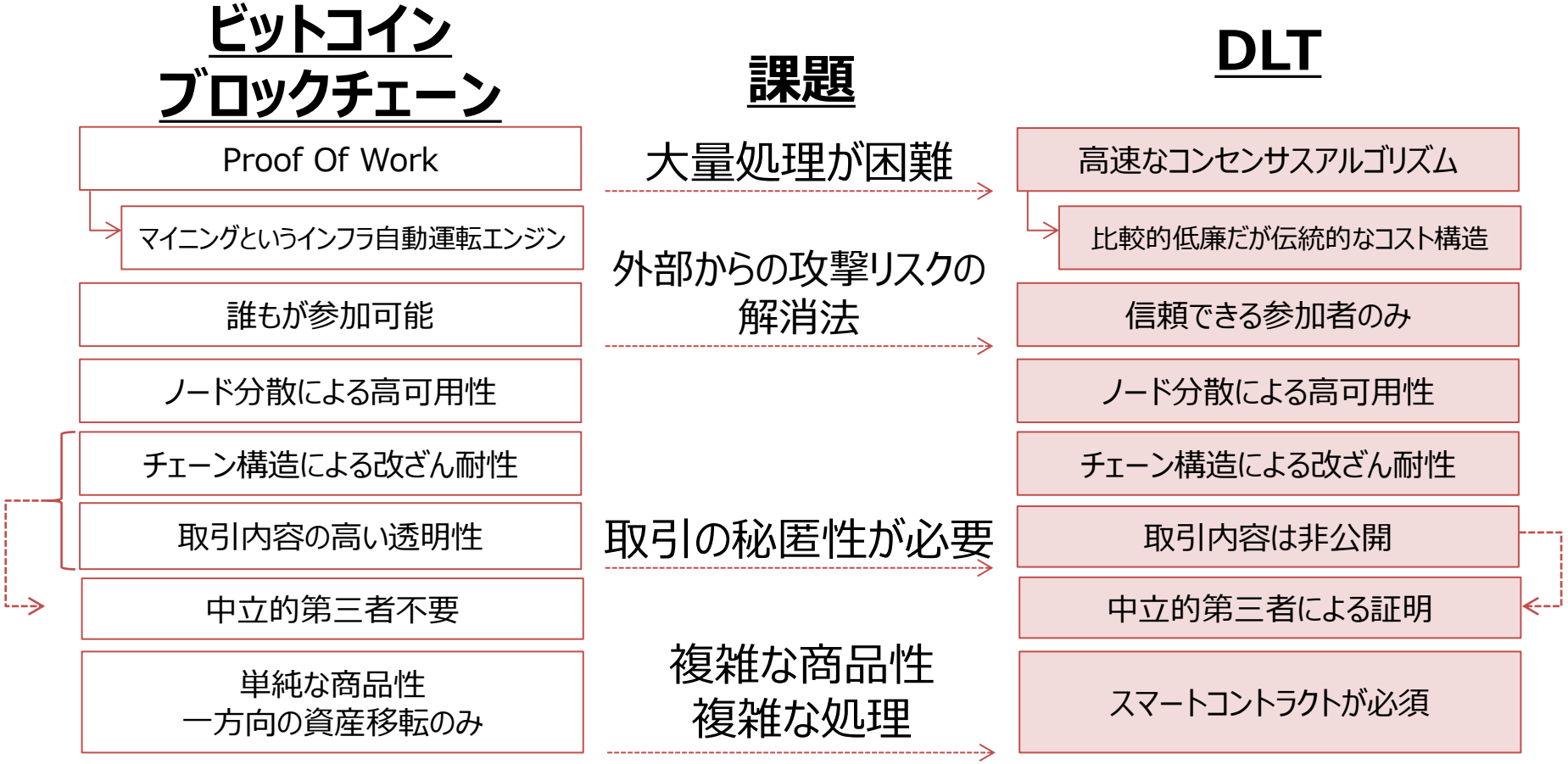


ブロックチェーンの変容



金融市場への適用

- ビットコインブロックチェーンの特徴の幾つかを修正した規格が発生
- オリジナルと区別するため、分散型台帳(DLT)と呼ばれる事が多い

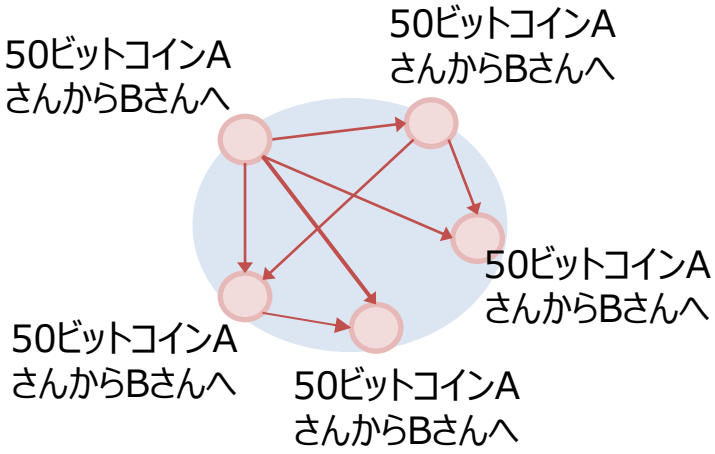


スマートコントラクト

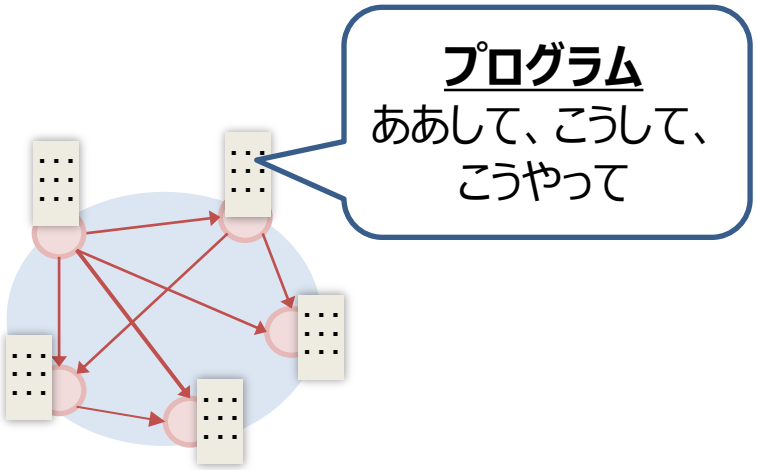
- AからBへ仮想通貨へ移転させることができるなら、もっと複雑な情報も移転させられるはず

- 移転のための条件をプログラムコードに書き込むことができれば、より複雑な処理もできるはず

単純な仮想通貨の処理



スマートコントラクトの処理



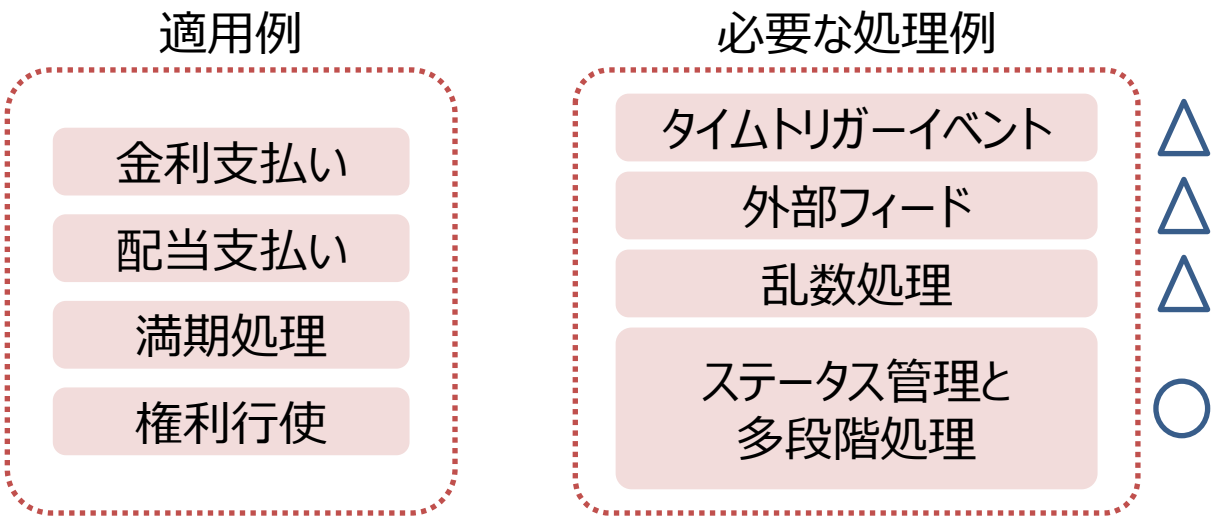
スマートコントラクトへの期待と課題

メリット

- 一連の処理の自動実行により圧倒的な処理の効率化
- 自動履行される契約　→　信頼性確認負担の軽減
- ブロックチェーンネットワークに乗せる事による高可用性
- 24時間365日のサービスも可能

課題

- 非決定的処理（下記例）への課題
- アプリの事前審査や、障害発生時の緊急時対応



情報秘匿への要件

- 証券市場では取引履歴の公開を好まない投資家も多い

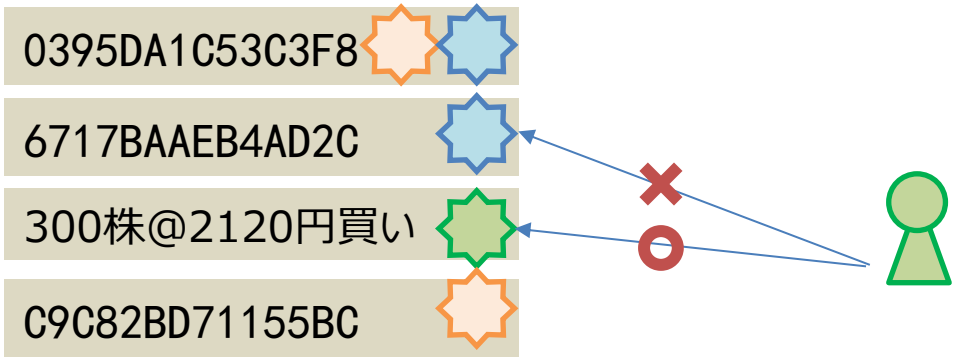
匿名アドレス　1Nn3pe5i7RDqUtbL1BZPxTVoeJLvqo1qfv

300株@2140円買い
400株@2130円買い
300株@2120円買い
8000株@2100円買い

取引戦略

大口ポジション

- 投資家属性の匿名性だけでなく取引情報の暗号化とアクセスコントロールが必要



ちょっと待った！

- 仮想通貨の非中央集権性を支える要素の一つがなくなる

❌アドレス毎の取引履歴は誰でも確認する事ができる

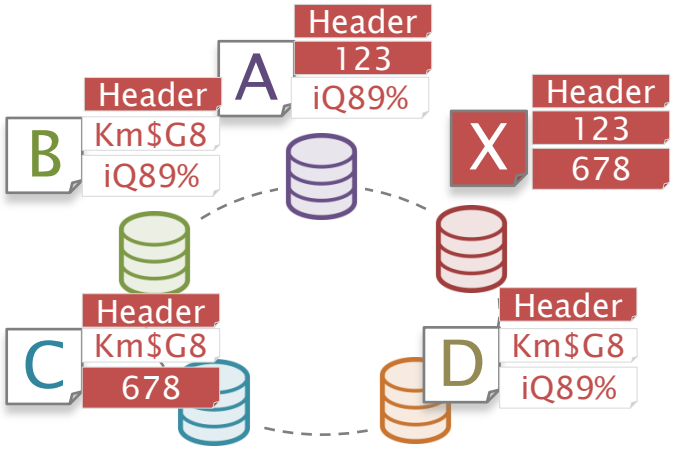
＋

履歴は誰にも改ざんできない

- 「情報は公開されていませんが、私は○○証券を○○株持っています」という主張の正当性は誰も判断できない
- **第三者による証明が必要となってしまう**

情報秘匿へ最近のアプローチ

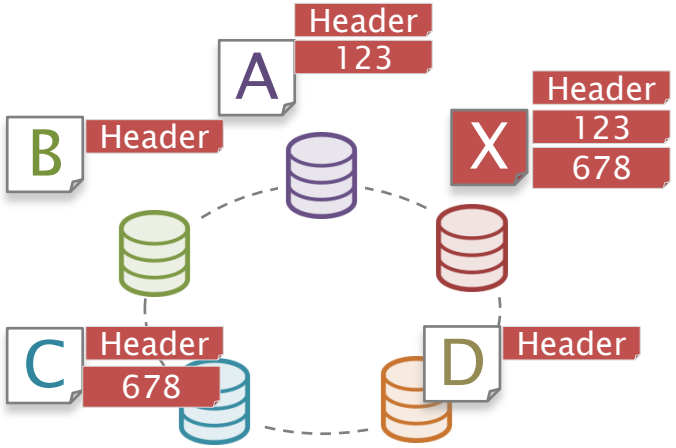
暗号化した上で全データ共有



- 合意形成の処理過程で復号
  ⇒再暗号化
- データが他社ノードに蓄積

⇒データ共有範囲を限定したい

共有範囲の限定

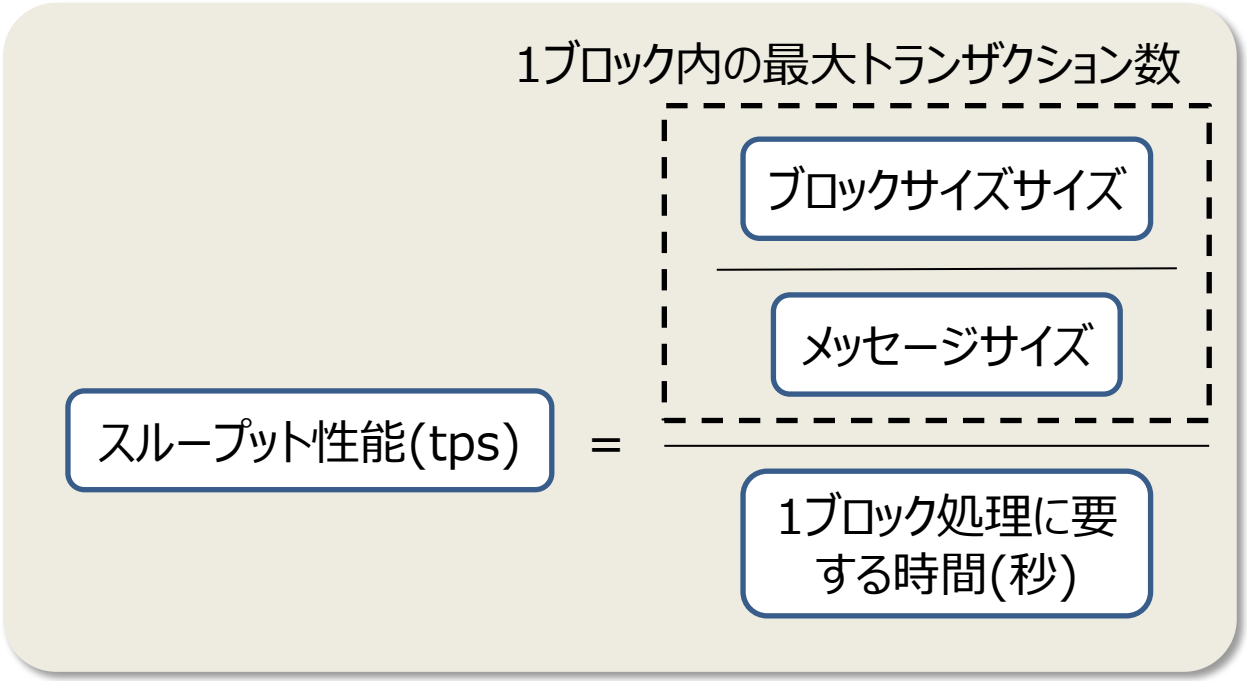


- 関係者間でのみ合意形成処理
  and/or
- 関係者ノードにのみデータ蓄積

- （後述のスループットにも影響）

スループット向上への課題

PoW型の処理におけるスループットの定義



- Bitcoin cashへのハードフォーク
- SegWit
- 短縮すると各回の競争は減少してしまう

Payment Channel, Lightning network
→ Off-chainでのネッティング・エスクロー型処理導入による高速化
→ 理論的には大幅な改善の可能性

劇的なスループット向上への挑戦

スループット性能
(tps)

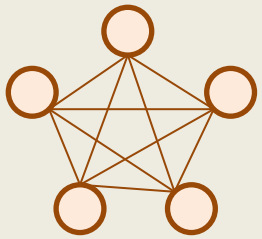
ビットコイン　**約7tps**

大手カード、大手決済システム等　**数千～数万tps**

大幅な乖離

- PoW系ではないコンセンサスアルゴリズムの試行

例：PBFT(Practical Byzantine Fault Tolerance)



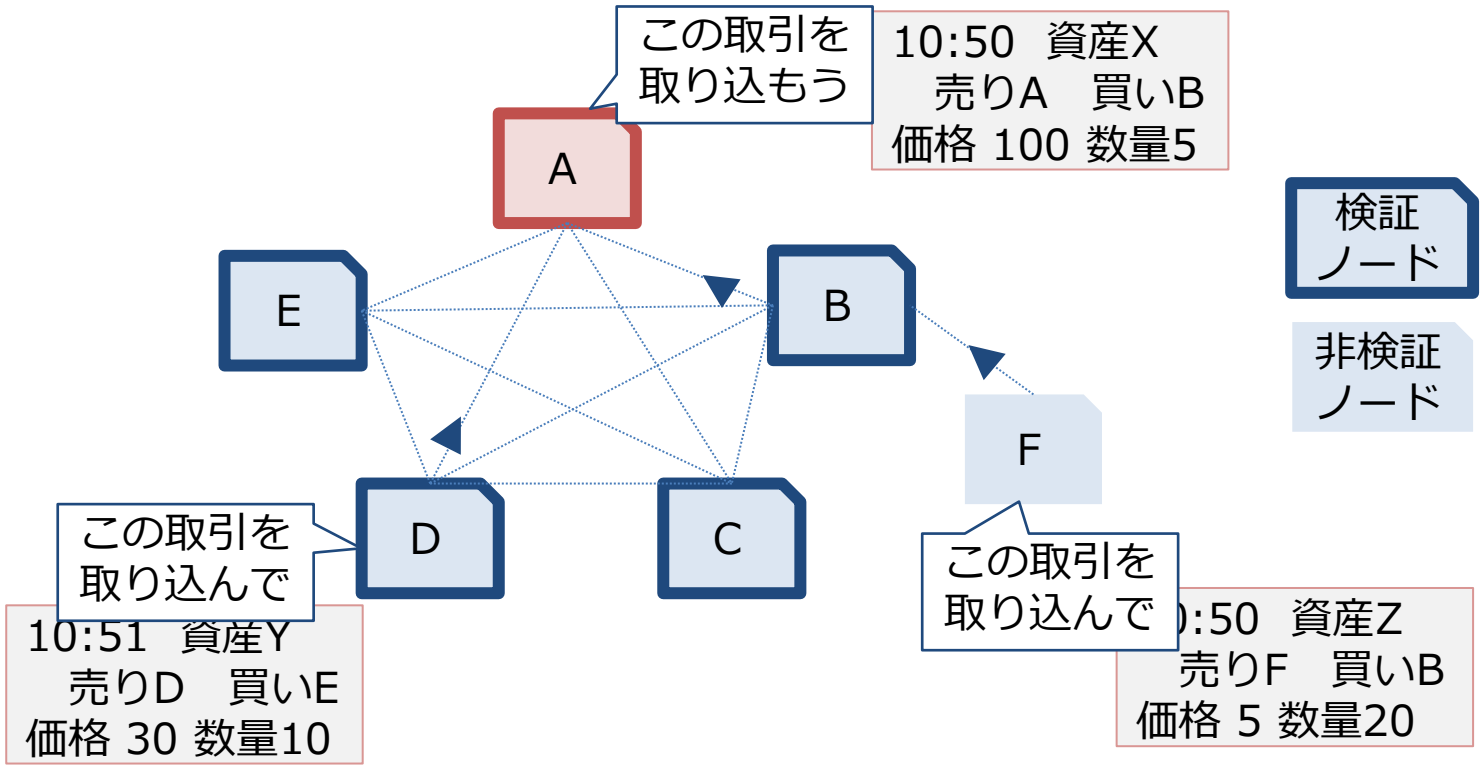
- PoWのような計算競争がない
- 全ノードの一定数(3分の2以上)がトランザクションを認証する事で合意形成とする
- 相対的に高速な処理が可能
- 認証処理に参加できるノードは事前承認制

BFT系の処理手順(1/5)

①取引発生

各検証ノードはネットワーク内に発生した取引をリーダーノード(※)に投げる。非検証ノードはいずれかの検証ノードを通じて情報を流す。

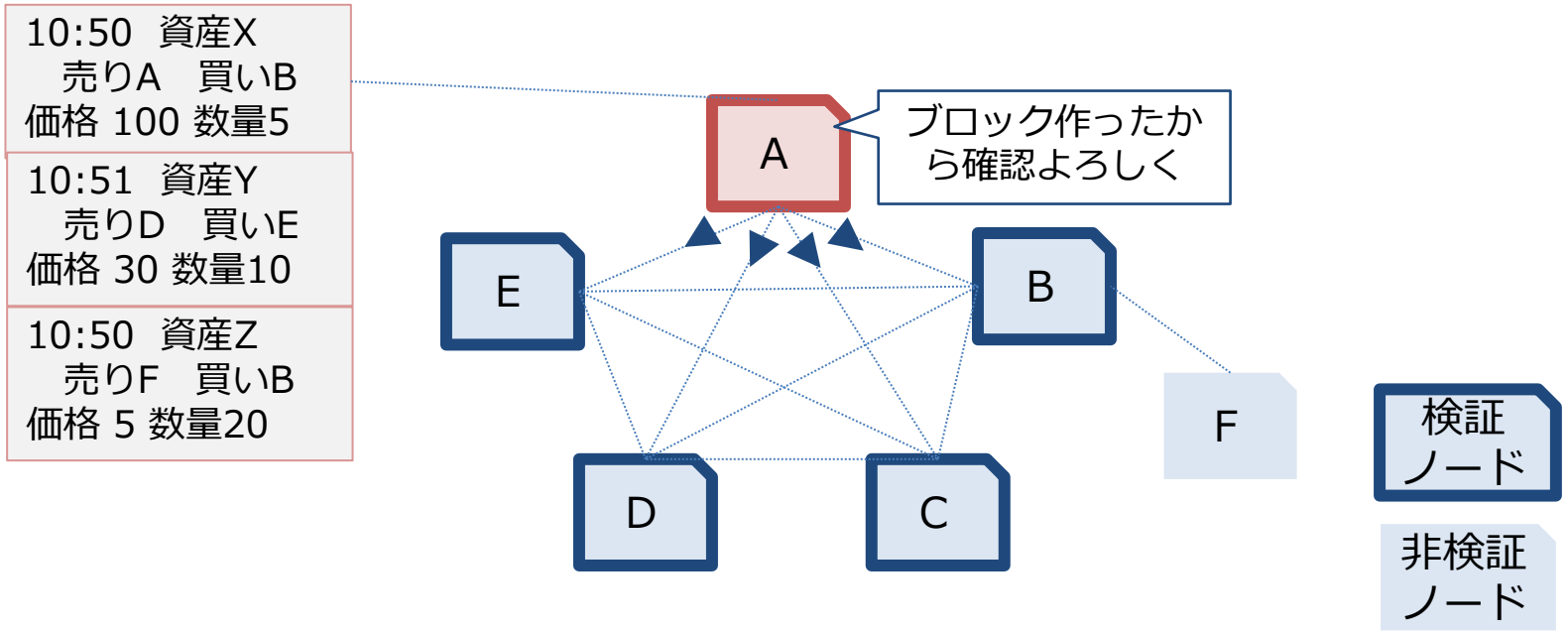
※リーダーノードを固定する方式やラウンドロビンで決定する方法等がある



BFT系の処理手順(2/5)

②リーダーノードによるブロック生成と配布

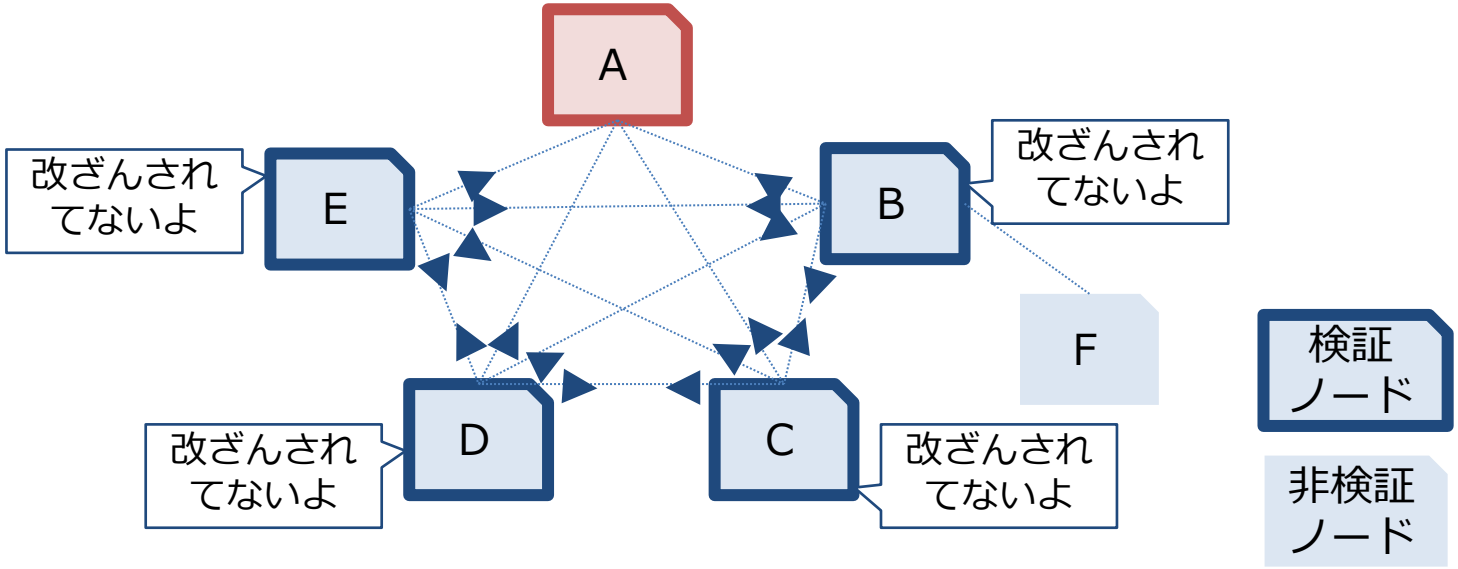
リーダーノードは受け取った情報をブロック化し、他の検証ノードに対し検証依頼



BFT系の処理手順(3/5)

③各検証ノードによるトランザクションの正当性の検証

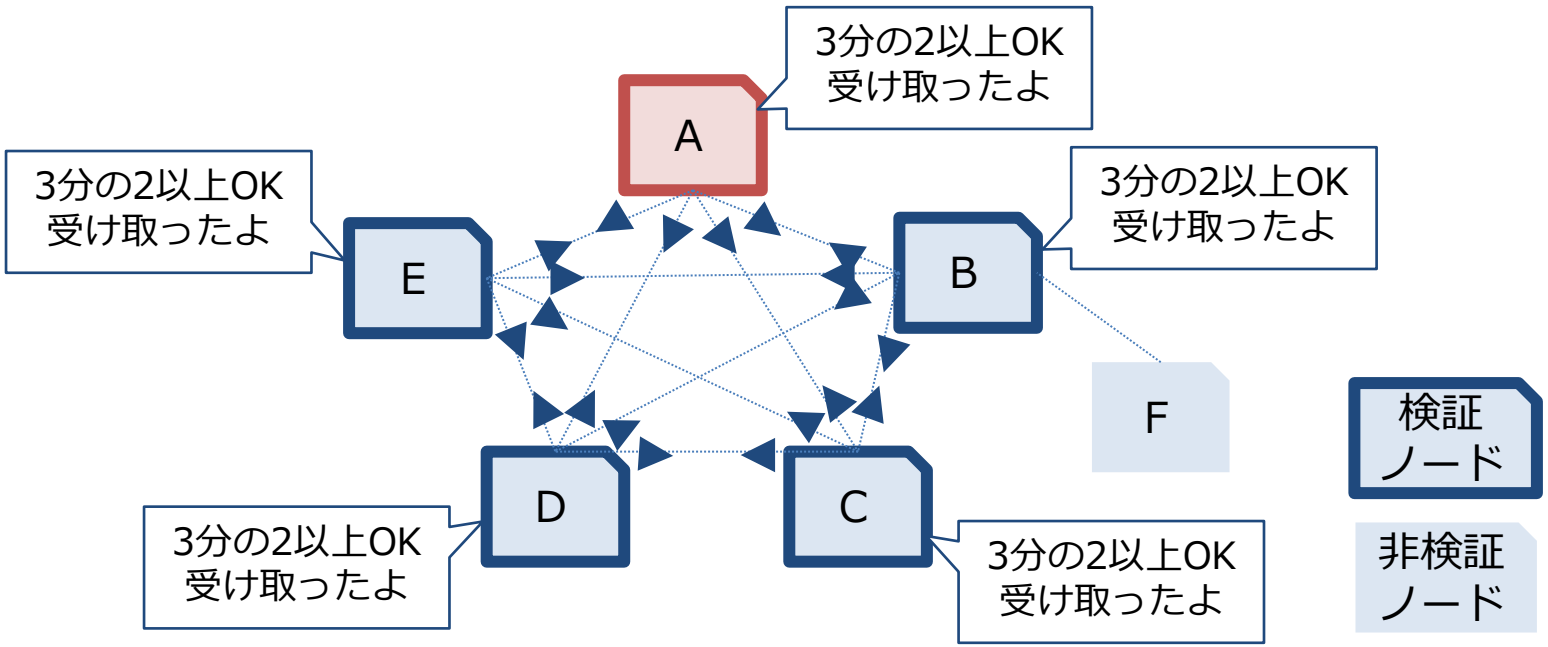
検証ノードはリーダーから送信されてきた取引についている電子署名を確認し改ざんされていないことを確認



BFT系の処理手順(4/5)

④必要な数の検証ノードが合意している事を確認

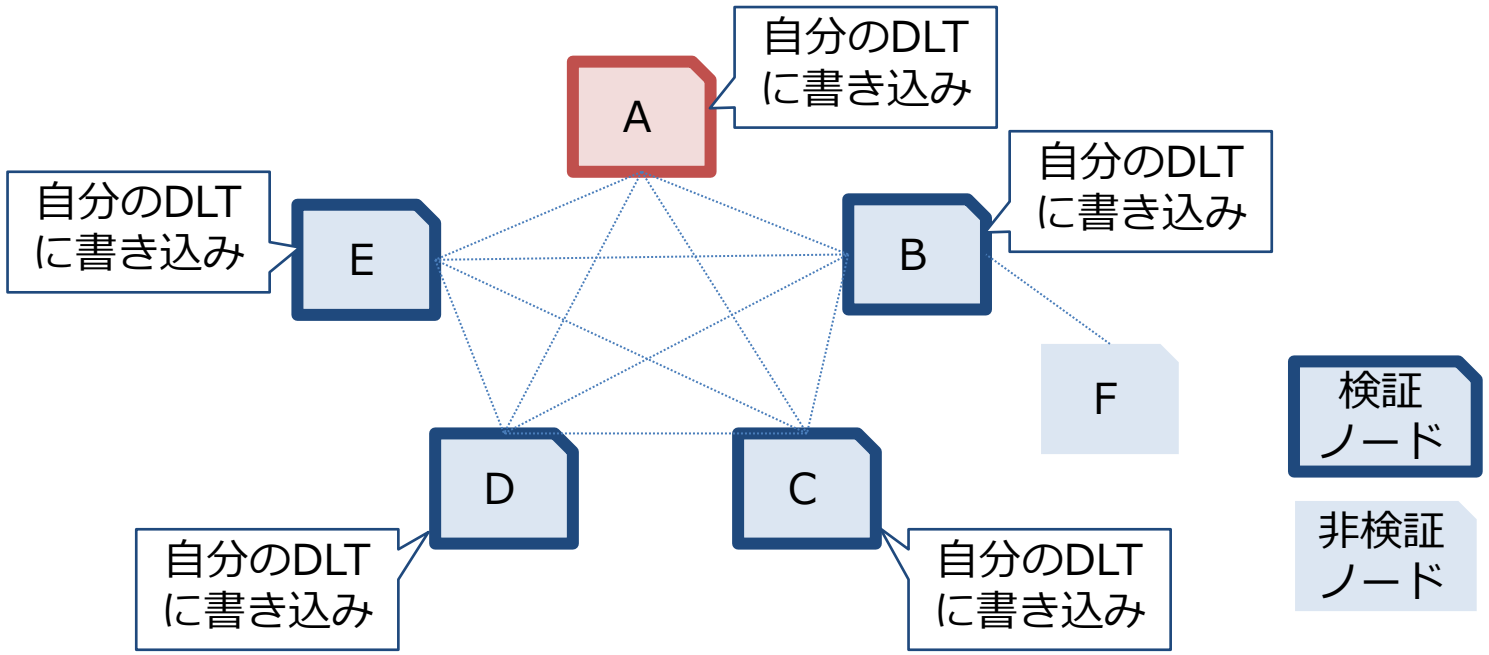
全体の3分の2以上の検証ノードから取引の正当性を確認したメッセージ(③)を受け取った検証ノードは準備完了のメッセージを送信



BFT系のコンセンサス(5/5)

⑤ブロック書き込み

リーダーノードから②で受けとったブロックを自分のDLTに書き込む
非検証ノードはデータを持たないので、書き込み処理を行うのは検証ノードのみ



処理の複雑性とともに生じるボトルネック

BFT型合意形成の流れ

暗号化/複合 → 情報配布 → 合意形成 → スマートコントラクト実行 → 順序決定 → ブロック作成 → DB記録

※アルゴリズムによって各プロセスの有無、処理順、回数は異なる

- スマートコントラクト実行に時間がかかる
- 暗号化/複合処理に時間がかかる
- 情報配布範囲が広いためノード数増加によりパフォーマンス劣化
- シリアル実行を要する処理が含まれるため並列実行による高速化困難

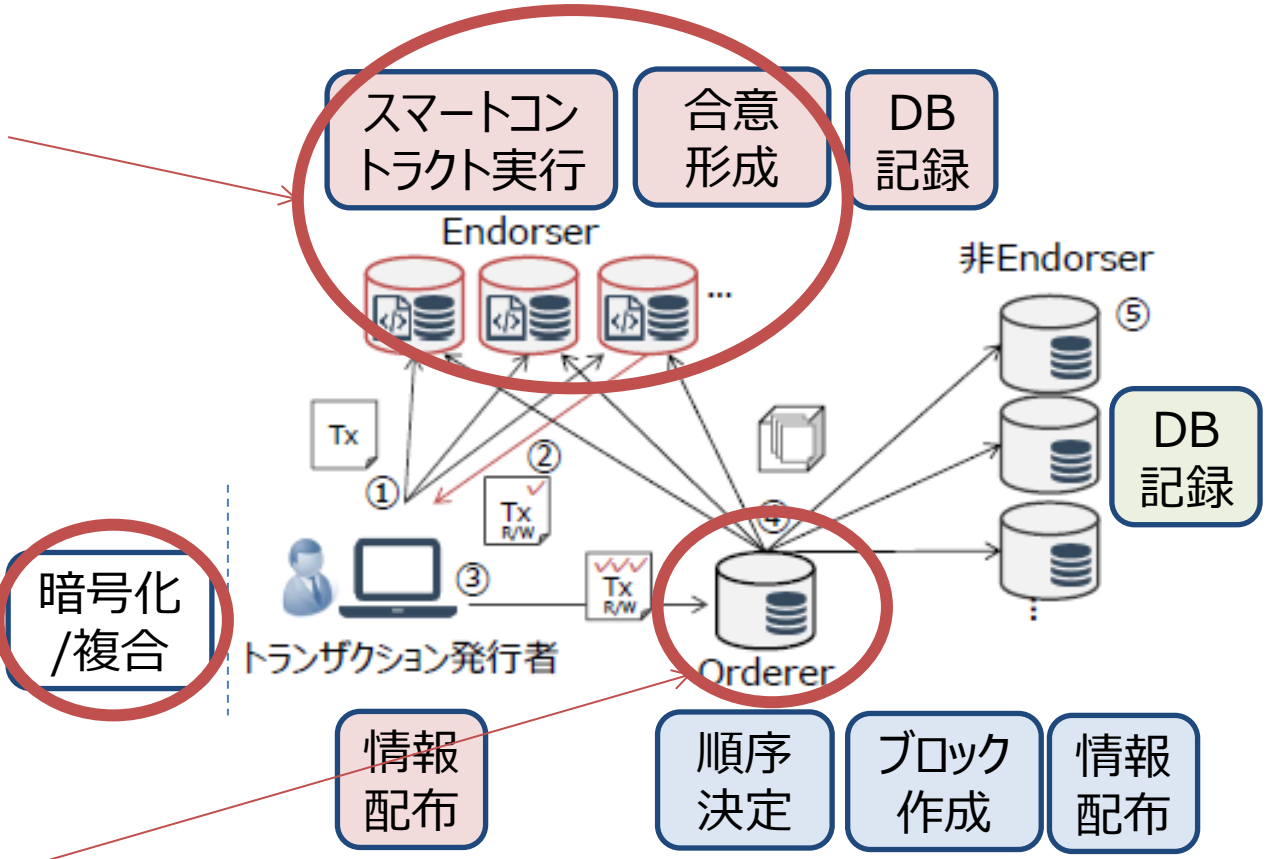
本気の業務要件を想定するとまだボトルネックがある

現時点でのボトルネック解消案

実行処理の分割と合意形成範囲の限定によるシリアル処理の極小化

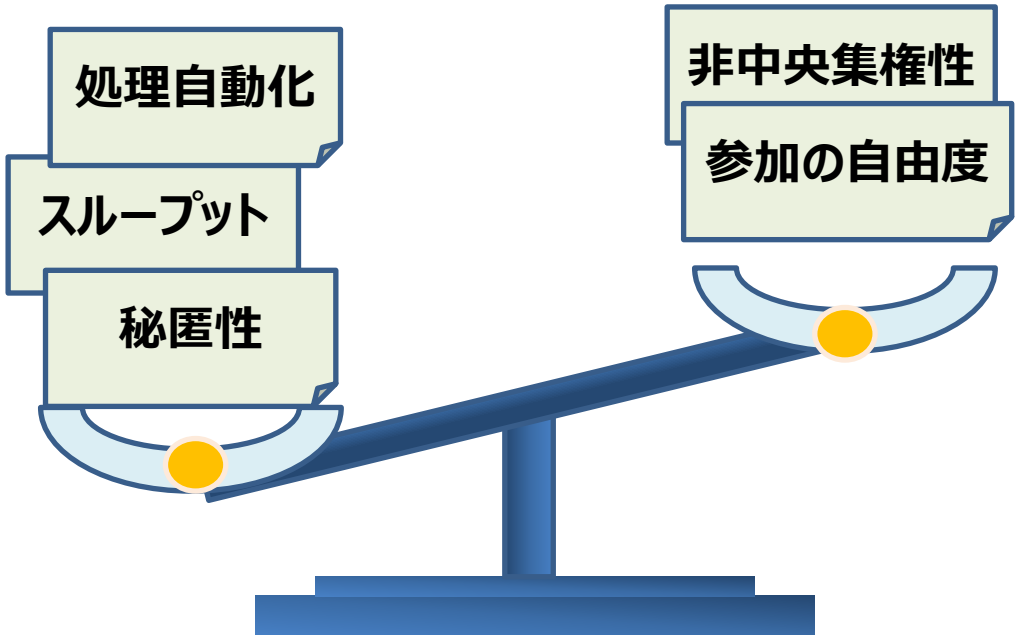
一部処理のOff-chain化

ノード間通信の減少によるトラフィックの抑制



正しい改善の方向性なのか？

- ブロックチェーン/DLTは複数の要素の組み合わせであり、利用者が最も成し遂げたい事に応じて、バランスが変化する事は自然
- 現時点では、技術の利用者としての金融機関は、「情報共有の効率化」と「処理の自動化」に魅力を感じており、結果として分散台帳技術(DLT)がオリジナルのブロックチェーンのコンセプトから乖離している
- 仮想通貨とは全く違うアプローチで、金融の効率化を実現しようとする挑戦



分散台帳技術でないと実現できないのか？

- 分散台帳技術は魔法の杖ではなく、既存技術で実現できる事も多い
- 一方で、既存技術だけで、十分に情報共有の効率化や処理の自動化が達成できてきたとは言い難い

- 業界全体で新たな金融サービスのデザインにチャレンジできるのは新規技術の特権

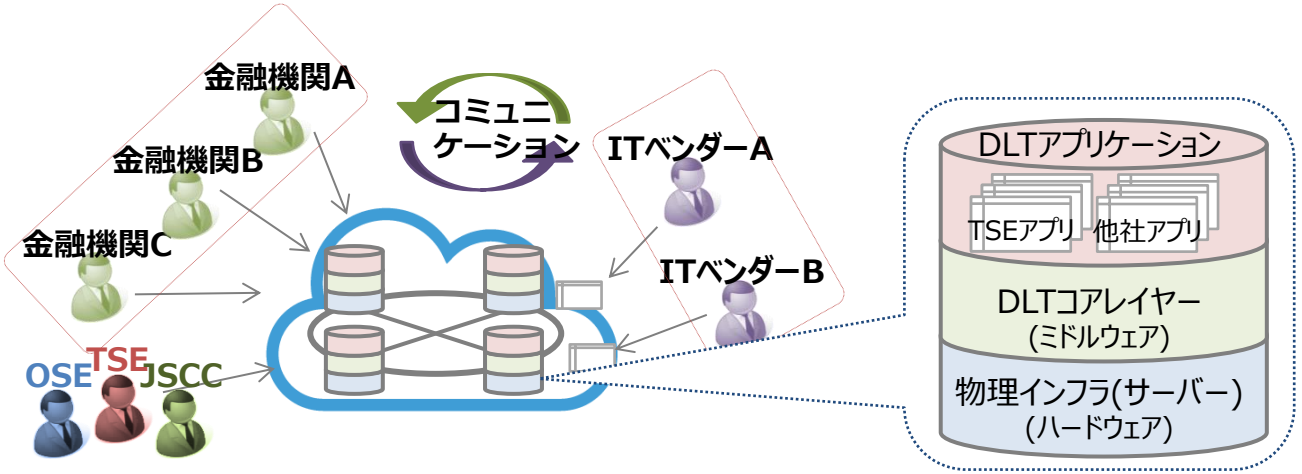
- **分散台帳技術(DLT)の特徴**
  - **サービスの集合体としてのパッケージシステムである**
    - スマートコントラクト（アプリ）、合意形成のための通信プロトコル、データベース等
  - **単独企業ではなく複数企業で基盤共有**

業界連携型実証実験

- 新規技術の探求は、関心があったとしても、人も予算も必要で、単独社で進めるには相当なパワーが必要
- 少しずつ負担をシェアし合えば、もっと効率的に進められるはず
- ブロックチェーン/DLTは、分散ネットワーク上で動くという技術的特性もあり、連携しないと期待される効率化の効果も小さくなる

⇒ 業界連携型の実証実験を開始。金融機関33社+金融庁、日銀、証券業協会
⇒ TSE提供アプリ on Hyperledger fabric V1.0
⇒ 金融機関・ベンダーから2件のプロジェクトが提案され進行中
⇒ JPX Working paper　2本、デモアプリの動画がHPにて公開中

http://www.jpx.co.jp/corporate/research-study/dlt/index.html



手放した方がリターンが大きい

なぜ情報をオープンにするのか？

- 新規分野なので知見を溜め込む事に意味がなさそう
- 理解に誤りがあるかもしれないので指摘を受けたい
- 自分達が苦労した情報不足を解決しないのは社会全体で無駄
- 課題を放置しても解決しない。技術者を信じて課題を発信する。ユーザー企業からのRFI、RFPの発信が必要
- 国内外で情報を囲い込む状況を何とかしたい。これでは技術が発展しない。

▶

- 結果、国内外から想定以上のフィードバック
- 情報収集、理解の確認に多大な効果
- オープンに進めた方が結局早いしスケールする

未来の金融サービスとは？

- 金融の民主化
- 圧倒的な効率化
- 分散アプリケーションの集合としての金融システム
- 資金と証券とプロセスの一体化

(参考文献)

- ‘金融市場インフラに対する分散型台帳技術の適用可能性について’, 2016, JPX Working Paper Vol15
- ‘金融市場における分散型台帳技術の活用に係る検討の動向’, 2017, JPX Working Paper Vol20
- ‘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報告’, 2017, 全国銀行協会
- ‘Embracing disruption’, 2016, DTCC White paper
- ‘The Distributed Ledger Technology Applied to Securities Markets’, 2016, ESMA
- ‘Payment systems: Liquidity saving mechanisms in a distributed ledger environment’, 2017, 日本銀行・ECB
- ‘ブロックチェーンは本当に世界を変えるのか（全14回・ITPro2016年7月～翌2月）’, 2016, 松尾真一郎他
- ‘ビットコインとブロックチェーン：暗号通貨を支える技術(Mastering bitcoin日本語訳)’, 2016, アンドレアス・M・アントノプロス(著), 今井崇也・鳩貝淳一郎(訳)
- ‘いちばんやさしいブロックチェーンの教本’, 2017, 杉井靖典

- 上記の資料を参考にさせて頂きましたが、本文中のあり得べき誤りは全て著者の理解不足によるものです

【本資料に関する注意事項】

- 本資料は情報提供のみを目的としたものであり、投資勧誘や特定の証券会社との取引を推奨することを目的として作成されたものではありません。
- 万一、本資料に基づき被った損害があった場合にも、（株）日本取引所グループは責任を負いかねます。
- 本資料で提供している情報は万全を期していますが、その情報の完全性を保証しているものではありません。
- 本資料に記載されている内容は将来予告なしに内容が変更される可能性があります。内容等について、過去の情報は実績であり、将来の成果を予想するものではありません。
- 本資料のいかなる部分も一切の権利は（株）日本取引所グループに属しており、電子的または機械的な方法を問わず、いかなる目的であれ無断で複製、または転送等はできません。
- 資料には、講演者の個人的意見も含まれておりますので、全てが（株）日本取引所グループの公式見解ではありません。