ブロックチェーン概論

JAIECO ブロックチェーン研究会 第 1 回

慶應義塾大学 SFC 研究所 上席所員
斉藤 賢爾
ks91@sfc.wide.ad.jp

かんたんな自己紹介

- 斉藤 賢爾 (さいとう けんじ) (ks91@sfc.wide.ad.jp)
  慶應義塾大学 SFC 研究所 上席所員 (村井純 研究室)
  株式会社ブロックチェーンハブ CSO (Chief Science Officer)
  一般社団法人アカデミーキャンプ 代表理事

- 経歴
  - 1988~1997 年、日立ソフト (現 日立ソリューションズ)
  - 1993 年、コーネル大学より M.Eng 取得 (コンピュータサイエンス)
  - 2006 年、慶應義塾大学より博士号取得 (政策・メディア)

  - 慶應義塾大学 大学院 政策・メディア研究科や SFC 研究所にて 15 年以上にわたり P2P およびデジタル通貨等の研究に従事
  - 福島のこどもたちのための「アカデミーキャンプ」を実施
    ⇒ 私の頭の中ではつながっています

本日の構成

- 1. ブロックチェーンとは何か
- 2. アイスブレーク (簡単なゲーム)
- 3. 基礎技術
- 4. ビットコインブロックチェーンの技術
- 5. 地球規模の OS に向けて

1. ブロックチェーンとは何か

- ブロックチェーンは民主化された「新聞」であり、
- 「空中約束固定装置」
  - 空中に「約束」を固定する

ブロックチェーンとは？

- ブロック (塊) のチェーン (連鎖)
  - ブロック ← 取引 (TX) の集まり
  - 取引 (TX) ← 状態の変化の記述 (例：送金)

- パブリッシングのプラットフォーム (新聞の代わり)
  - "A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post"
  - "To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash, rather than newspaper or Usenet posts"

– Satoshi Nakamoto (2008)

なぜ新聞なのか？

- ビットコインの「問い」
  - 「自分が持っているお金をいつでも自分の好きに送金することを誰にも止めさせない」ためには？

- ビットコインの「答え」
  - デジタルなコインを P2P でやり取りする
    - デジタル署名を用いる (検証可能性の担保)
  - 二重消費 (double spending) を防ぐ必要がある

⇒ 群衆が (出来事の証拠として) 発行する「新聞」に取引の証拠 (ダイジェスト) を載せる

- ブロックチェーンは群衆による群衆のための「公告媒体」

2. アイスブレーク (簡単なゲーム)

- ブロックチェーンを理解するための簡単なゲーム
  - 名刺とデジタルコインを同時に交換します

ゲームのルール

- 指名された人は
  - メモの最初の行に「10 JARECO」と書く
    (JARECO : Japan-America Real Estate COin)
  - メモの次の行に自分の名前をローマ字で書く
  - それがコインとなります

- 全員で
  - 相手を見つけて名刺を交換し、自己紹介します
  - 自分がコインを持っている場合は相手に渡します
    - メモの最下行に、渡す相手の名前をローマ字で書く
    - メモにクリップで自分の名刺を追加する
  - 受け取る人は、1) 最下行に自分の名前があるか 2) その上の行の人の名刺が追加されているか を確認します

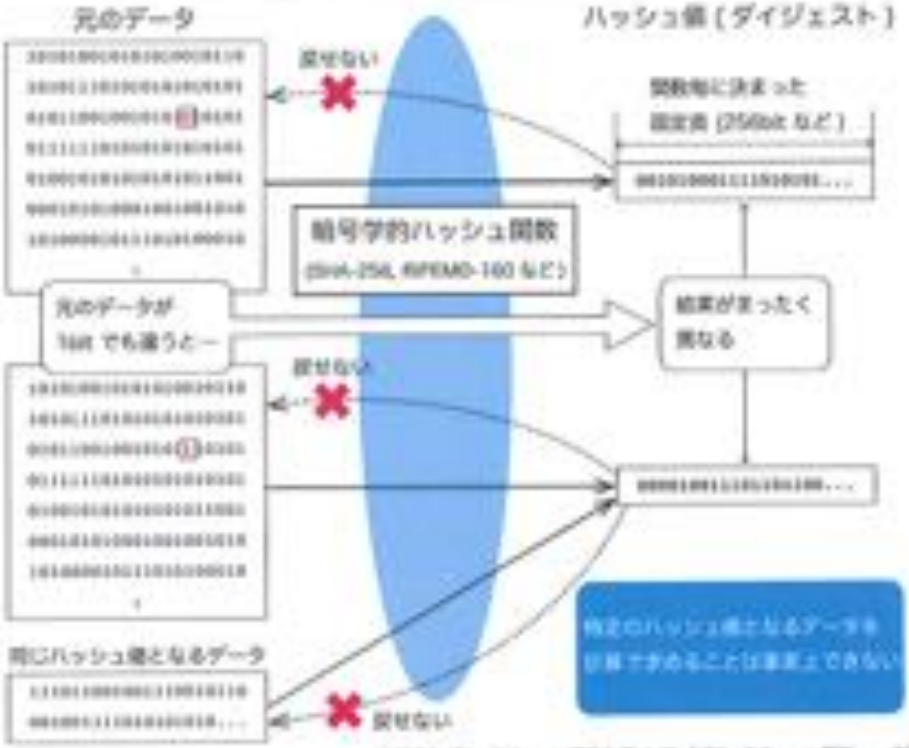
完璧にできましたか？

- 何かがうまくいかなかった場合
  - どうすればうまくいくようにできますか？

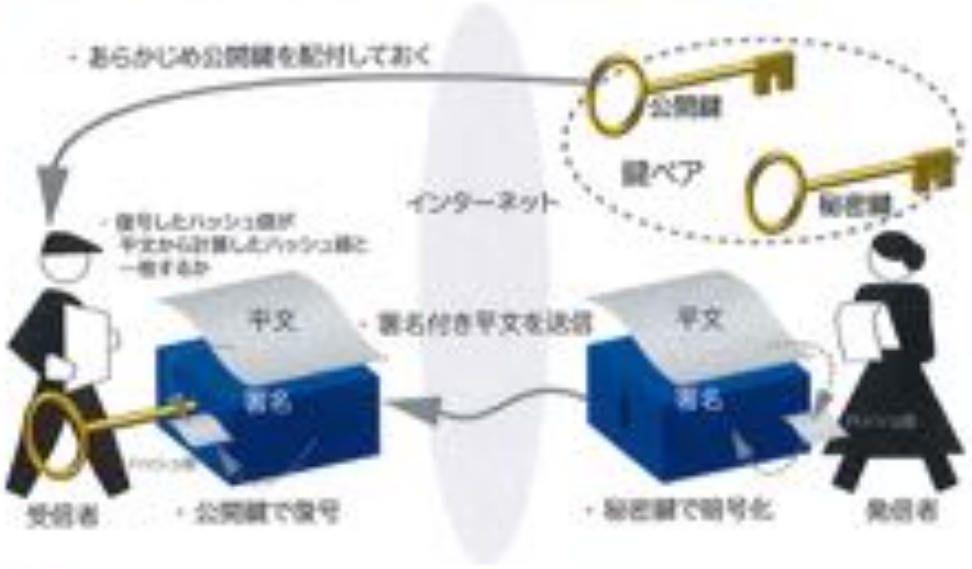
3. 基礎技術

- 暗号学的ハッシュ関数
- デジタル署名

暗号学的ハッシュ関数



デジタル署名

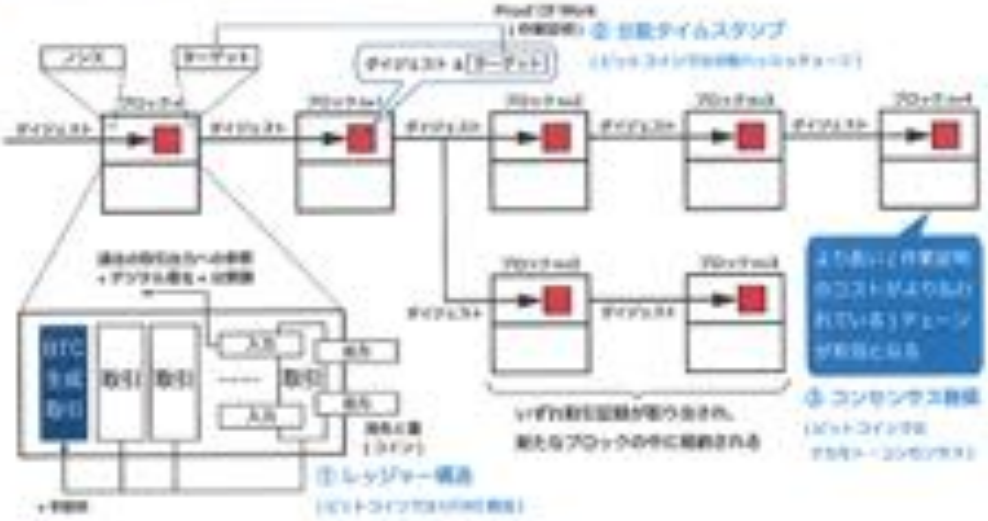


- 本人が送ったものであり改竄されていないことが証明できる
- RSA, DSA, ECDSA (楕円曲線 DSA) 等 (上の例は RSA)
- ビットコインでは取引はデジタル署名されるが、狭義の PKI は用いない

4. ビットコインブロックチェーンの技術

- 維持される構造
- 技術の階層構造
- 作業証明
- 技術の課題

ブロックチェーンの概要 (ビットコインの場合)



- 1. 各マイナーは、過去 10 分ほどの間に収集した取引データをブロックに格納し、マイニング (くじ引き) を行う
- 2. 成功したらネットワーク内にブロードキャストする
- 3. 各マイナーは、それをチェーンの新しい末尾と認めるなら、その後ろにブロックを繋げるべく 1 に戻る

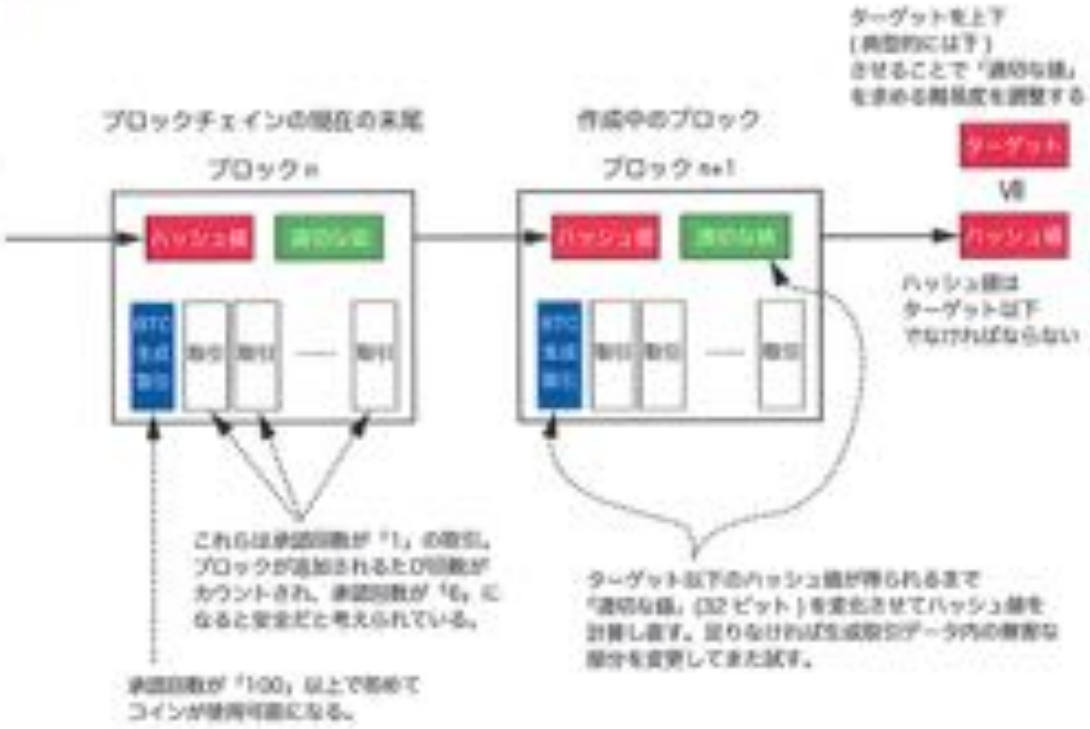
ブロックチェーンを理解する

- ブロックチェーンは、インターネットの End-to-End の哲学を、
  アセット (資産) の制御において現実化する (ことを試みる)
  「空中約束固定装置」

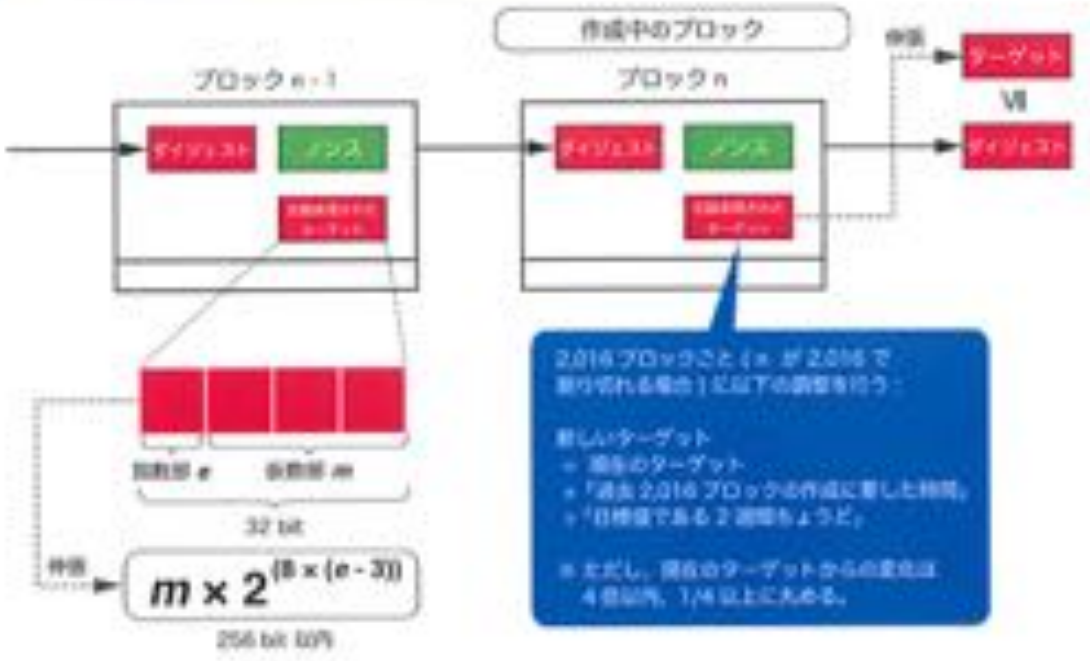
Proof of Work とは？

- 計算コストを投入したことの証明
  - 作業は困難だが、その結果の検証は容易
- それにより、スパムや不正行為を抑止するというが...
- 例 : Hashcash (1997)
  - メールヘッダに SHA-1 ハッシュ値の最初の 20 ビット (当時) が 0 になるような乱数を用いたスタンプを載せる
    - 1 通のメールの送信準備に 1 秒ほどかかる
    - 受信側での確認は一瞬で、スタンプが無効ならスパムと扱う
- ハッシュ値/ダイジェストを用いる場合の一般化
  - あるターゲット以下になるようなダイジェストとなるデータを見つけよ
  - ハッシュ値も数なので大小を比較できる

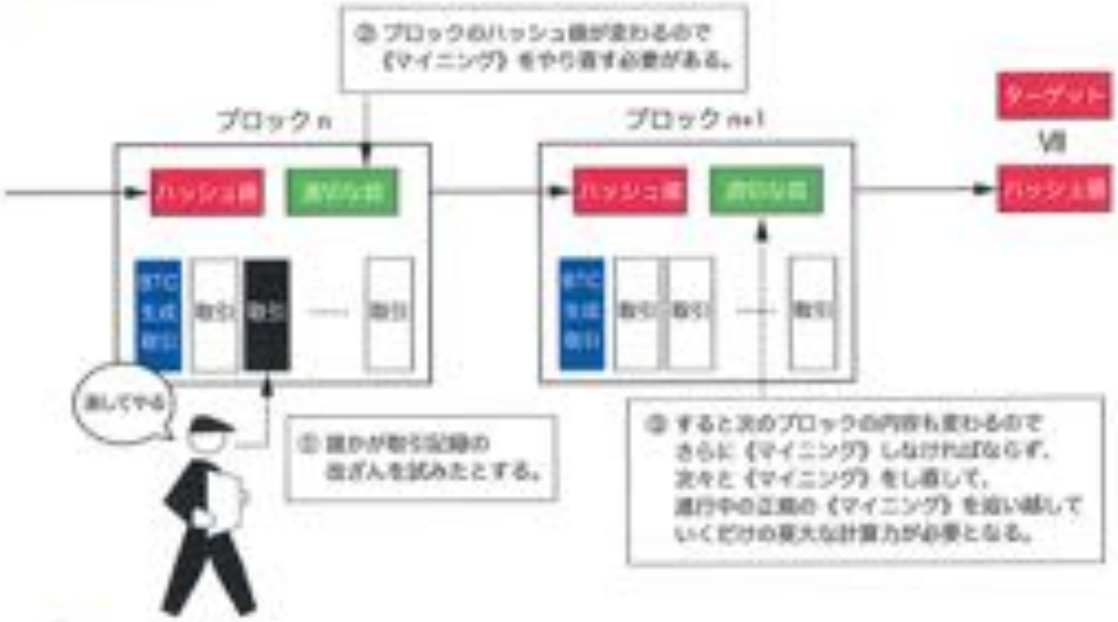
マイニング (ビットコインの場合)



ターゲットの調整 (ビットコインの場合)



POWによる保護



- 取引はデジタル署名されていて内容は元々改ざんできないが、消される可能性がある
- Proof Of Work (作業証明) を課すことで改ざんを抑止する . . . というが

過去2年間のハッシュレートの推移

現実 *vs.* ブロックチェーン

- 思考実験
  - ビットコインで支払うと、上空を飛ぶドローンが運んできた缶ジュースを落としてくれるというサービスを作るとする
  - ドローンはいつ缶ジュースを落とせばよいのか？
- 実時間で進行する現実と、ブロックチェーンの動作はかけ離れている
  - しかしビジネスの主体はリスクをとって応用していける

5. 地球規模のOSに向けて

- 人類史に残る変化のはじまり

ところで、

人類史に残る会社とは？

- 仮に聞いてみたい
- 人類史に残る会社の例は？

人類史に残る会社とは？

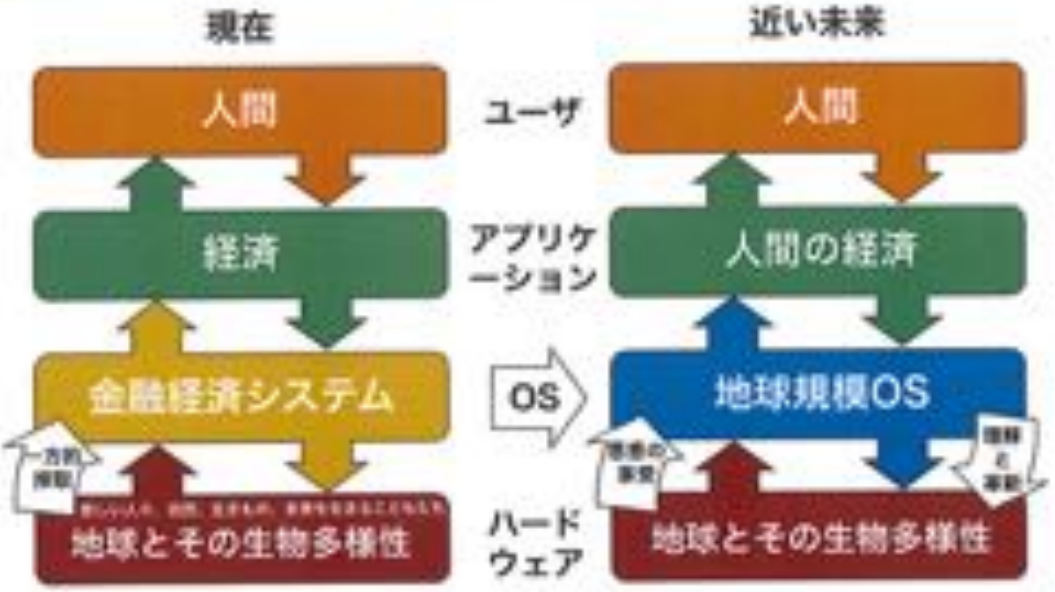
- 例：
  - イギリス東インド会社 (1600)
    - 初の株式会社のひとつ
  - 海援隊 (1865)
    - 近代的な株式会社に類似した組織
- 現在、人類史に残っているのは、現在の会社の仕組みの起点となる会社
- 次に人類史に残る会社は？
  - 近代的な株式会社を終焉させる

DAC/DAO

- Distributed/Decentralized Autonomous Corporation/Organization
- 自律分散組織 - 経営が自動化された組織
- 例 : ビットコイン
  - ユーザを株主、コインを株式、採掘者たちを従業員と考えれば...
  - そのプログラムコードは、株式の移転を業とするその組織の経営の仕方を記述していると見なすこともできる

- 一般化して考えると「法」のあり方が変わっていく
- ソフトウェアには、もともとそういう力がある

地球規模 OS (2007)



- 複数主体による地球上の資源の利用を調整する

基盤としての地球規模 OS

- 金融・貨幣経済システムを時代遅れにする
- 決済システムを内包
- プログラミング言語と環境を内包

- 人的資源を含む地球上の資源の会計システム
- 新たな「法」を定義できる
- 人々が業を起こすための基盤
  - 営利組織も、政府も、NPO/NGO も利用できる

- 現在の金融・貨幣経済システムを時代遅れにする
- 決済システムを内包
- プログラミング言語と環境を内包

これは...！

イーサリアム(Ethereum)

- Vitalik Buterin, "Ethereum White Paper: A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM"
- ブロックチェーン技術を応用
- そこにプログラミング言語を載せる
- スマートコントラクトのための分散アプリケーション基盤
  - スマートコントラクト：
    デジタルに表現される資産を予め定められたルールに従って自動的に移転させる仕組み
- 現在の金融・貨幣経済システムを時代遅れにする？

地球規模OSのための応用問題

- ヒッチハイク問題
  - 走行中の自動車の空席は近傍の人間が共有できる資源である
  - 歩行者と運転手がランデヴーし、目的地へのヒッチハイクを可能にするようにネットワークをプログラムせよ

Uber

現在の視点から見たゴール

- Uber のような企業をプログラムとして記述・実行できるような環境を整え、提供する
  - Uber はすでに多くの部分が自動化されている
- それにより
  - 誰もが公益性に主体的に関与するためのコスト・敷居を下げる
    - ビジネスは結局は公益性に関わる
  - 地球上の限られた資源を有効に活用し、持続的に生きられる文明への変化に寄与する

ここまでのまとめに代えて

技術的な課題の整理

- ブロックチェーンの技術の 3 層を評価する
  - 1. デジタル署名によるデータ構造 (レッジャー構造)
    - 誰もが制御を持て、自己充足構造で誰もが検証可能
    - ⇒ 有益 (ただし秘匿性は苦手)
  - 2. ハッシュチェーンによるブロックの連鎖 (分散タイムスタンプ)
    - 相対時刻を定義する、証明の基盤
    - ⇒ 想定されていたほど強固ではない
  - 3. ナカモト・コンセンサス (コンセンサス構築)
    - TX の確定に向けたトライアル
    - ⇒ 現実と同期して動く上で問題がある
- しかしそれが可能にするとされる世界にはインパクトがある
- 課題の解決と課題が解決されたことを前提とする応用の探究を同時に進める必要がある

ご質問や議論を

ブロックチェーンの応用

JAPECO ブロックチェーン研究会 第 2 回

慶應義塾大学 SFC 研究所 上席所員
斉藤 賢爾
ka918afc.vide.ad.jp

本日の構成

- 1. 取り沙汰される応用とユースケース
- 2. 実際の応用事例
- 3. 応用のための新しいプラットフォーム
- 4. ブロックチェーンの応用を問う

1. 取り沙汰される応用とユースケース

- 取り沙汰される応用
- 現在までの実際の応用
- デジタル領域でのユースケース

取り沙汰される応用 *(Hyperledger での整理)*

- 金融アセット (資産)
  - 直接アクセス (仲介不要)、合意された実時間内の決済、ビジネスルールの記述、秘匿性の制御
- 企業行動 (特に財務上の意思決定)
  - 株式分割、減資・併合、株式移転・交換、合併、第三者割当増資等の実時間での実行と秘匿性の制御
- サプライチェーン
  - 材料のトレースバックや生産・貯蔵から販売までの記録と検索
- マスターデータ管理
  - 権限を持つ者のみが更新でき、指定された検証者がそれを承認する
- シェアリングエコノミーと IoT
  - 信用が必ずしも確立していない状況下でのスマートシティ/タウン、交通、ヘルスケア/フィットネス、リテール、建築、教育等 (暗黙的に実時間)

- 赤字はビットコインブロックチェーンが苦手とする部分
  - 解きたい問題の中に、現状、解けていない問題がある

現在までの実際の応用

- 通貨・送金
  - 例：ビットコイン、...
  - 銀行ネットワークをバイパスする送金
    - これだけでも巨大なインパクト
- 存在証明
  - 例：Proof of Existence
    - ブロックチェーンに任意のダイジェストを埋め込む
  - 存在していたこと、改ざんされていないことの証明
    - 元々の設計用途の応用の範疇（「新聞」の代わり）
- ネームサービス
  - 例：ネームコイン
    - 名前と実体の対応づけを空中に固定する
  - デジタル空間の中だけで完結する

ユースケース (Chain OS での例示)

- アセットの発行
  - 例. 銀行への USD の振込に基づいて (紐づいて) ブロックチェーン上に USD を発行する
- 支払い
  - ビットコインのように送金する
- 同時執行
  - デジタルアセットの移転に対するデジタルコインでの支払いを 1 トランザクションでアトミックに実行する
- オーダーブック (板)
  - 例：1EUR あたり 1.13USD または 0.79GBP で 10,000EUR を売る
- 担保付きローン
  - デジタルアセットを担保として利息付きで USD を貸し出す
- オークション
  - 最低価格を指定してデジタルアセットをオークションで売り出す

2. 実際の応用事例

- Abra – 送金界の Uber – as is 応用事例
- Proof of Existence – 存在証明 – 用途外応用事例

Abra

- 送金界の Uber
  - https://www.goabra.com
- 近所の個人や店舗等を利用して現金を入出金
  - Abra は送金業だが、自分ではお金を預からない
  - cf. Uber はタクシー業だが、自分では車両を持たない
  - cf. Airbnb はホテル業だが、自分では宿泊施設を持たない
- システム内での送金は無料

Abra とは

- P2P 送金ネットワーク
- モバイルアプリに入金
  (テラーまたはデビットカード経由)
- アプリから送金 (無料)
- テラー (teller) から出金
- テラー → 人間 ATM → すなわち ATM
  - 誰もが金銭出納係になれる
- ビットコインをバックエンドとして利用
  - BTC に交換して送金

手数料

- Abra はテラーが大体 1.5% の手数料を設定することを推奨
- Abra は取引当たり 0.25% の手数料を設定
- テラーが手数料を取らなければ、Abra も取らない
  (by CEO)

バックエンド

- BTC を移転 (USD 価格を 3 日間固定)
  - ヘッジコストは Abra の手数料に含まれる
  - 固定価格失効に関する UI は将来整備 (昨秋の時点)
- ヘッジコントラクトは当初はサーバに格納
  - スマートコントラクトに移行

- "Don't lose your phone!" (秘密鍵の在処は？)
  - Abra はユーザのお金を預からない
  - マルチシグは検討したが最初のバージョンでは使っていない

- 本来、カラードコインで実装できるという印象

Proof of Existence (存在証明)

- 個人が開設してしまった公証サービス
  - https://proofofexistence.com
- ある時点で文書が存在していたことを証明
- 文書自体を公開することなく所持していることを証明
- 改ざんがあれば検出

Proof of Existence (存在証明)

- 指定された文書のダイジェストをビットコイン ブロックチェーンに埋め込む (出力スクリプト部分に)
  - OP_RETURN の後ろに
    - OP_RETURN = その時点でスクリプト実行を失敗と見なす
    - ⇒ 誰も受け取れない宛先 (burn = 消 (焼) 失) として利用される
  - 0x444f4350524f4f46 ('DOCPROOF') に続いて
  - 文書の SHA-256 ダイジェストを埋め込む
- Bitcoin blockchain explorer 等で探してみてください
  - 毎日のように利用されています
- 手数料は 5 mBTC (0.005 BTC)

3. 応用のための新しいプラットフォーム

- 要求の整理
- Hyperledger Fabric
- Chain OS
- R3 Corda

要求

- さまざまなアセットの表現と管理
- プライベートなトランザクション、秘匿された契約
- アイデンティティと監査可能性
- 即時性とファイナリティ
- スケーラビリティと相互運用性
- ポータビリティ (さまざまな環境への適用・適応性)

- エンドが制御をもてる (非中央集権、分散)
  - 空中に約束を固定する

Hyperledger

- https://www.hyperledger.org
- Fabric : IBM と DAH によるコードを統合
- Sawtooth Lake : Intel
- Iroha : ソラミツ
- Hyperledger Whitepaper (WG page)

目的

- 既存のブロックチェーンの課題を解決する新たな構造
  - スケーラビリティ
  - 秘匿/プライベートなトランザクション
  - 軽量、モジュラー、拡張性
    - 実際に軽量にできているかは疑問
    - サブセッティングが必要では？
- 既知のユースケースを超えた将来の応用への適応性の確保

アーキテクチャ *(Fabric)*

(from Hyperledger Whitepaper)

- 論理構造であり、実際のプロセスや仮想マシン等の構成ではありません
- スマートコントラクトのライフサイクルの管理という概念は大きな特徴

Chain Open Standard

- http://chain.com/os/
- Nasdaq Linq での実績
- 課題抽出 → プロトタイピング → 一般化 → 課題抽出のサイクルを回す
- 最も従来のブロックチェーンからの変化が小さい

目的

- 実際のユースケースに基づく要求を満たす
  - ネイティブアセット
  - 許可制、選択的プライバシー、監査可能性
  - 即時性とファイナリティ
  - スマートコントラクト
  - スケーラビリティと相互運用性
  - コンプライアンス

アーキテクチャ (Chain Core)

- コミュニケーション層
  - HTTP+JSON API, RPC サービス, ロードバランサ
- サービス層
  - アセット発行、アカウント管理、ブロック生成、ブロックへの署名
  - 検証とコンセンサス、スマートコントラクト実行
- ストレージ層
  - ブロックチェーンとアカウントデータの保存

特徴

- アセット
  - 任意のアセット定義とアセット識別子
- スマートコントラクト
  - すべての取引をスマートコントラクトとして実行
- プライバシー
  - ワンタイムアドレス、ゼロ知識証明、暗号化メタデータ
- メタデータ
  - トランザクション構造のどの部分に対しても詳細に注記可能
- データモデル
  - いわゆる UTXO 構造
- コンセンサス
  - SBFT : Simplified Byzantine Fault Tolerance
  - 説明だけでは本当に BFT か分からない

R3 Corda

- Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services
- http://r3cev.com/s/corda-introductory-whitepaper-final.pdf

目的

- 金融機関間の金融協定を管理する
  - 業界標準のツールで作られた共通の仕組みでそれを行う
  - 相互運用性、インクリメンタルな展開、秘匿性
- Corda の問題：
  「私が見ているものはあなたが見ているものと一致しており、我々はどちらもそのことを知っていて、かつ監査にも同じものが見えていると知っている」
- ビットコインの問題とは異なる問題を解いている、という認識からの発想
  - ビットコインの問題：自分のお金を自分が使うことを誰にも止められないようにしたい

アーキテクチャの特徴

- システムレベルではなく、商取引レベルでのコンセンサス
  - 多様なコンセンサス機構をサポート
    - 当事者+監査の完全合意が必要なのであって、コンセンサス機構は唯一では？
    - 当事者ノードを分散化した際に各々のパーティでは必要
  - データはシステムワイドにコピーされない
- 第三者ではなく当事者によるトランザクションの検証
- CAP 定理のトレードオフにもとづく設計上の選択肢
  - 従来のブロックチェーンでは可用性のために一貫性が犠牲になっている
  - 逆に一貫性のために可用性を犠牲にする等
- 明示的な監査用ノード
- 「自然言語で書かれた法律関係書類」と『スマートコントラクトのコード』の紐づけ
- ネイティブ通貨は持たない

4. ブロックチェーンの応用を問う

- 「空中約束固定装置」の応用を問う
- ここまでのまとめ

応用を問う

- 「約束」は人間社会の基礎だから、
- もし空中に約束を固定できるなら . . . 何が起きる？

- 政府・公共
- 財産・所有
- 決済・送金
- 共有・貸与
- 医療・健康
- 環境・制御
  ⋮

- それぞれの具体的可能性から見えてくる要求がある

まとめ

- どのような「問い」に答えるかで技術は変わる
  - 解きたい「問い」のためではない技術を採用することはナンセンス
  - 一方で「問い」は社会的・技術的な状況によっても変わってくる

- 応用を考えること = 「問い」を発すること

ご質問や議論を