黄金期は過去ではなく未来にある。

ブロックチェーンの課題と未来

慶應義塾大学 SFC 研究所・環境情報学部 / 株式会社ブロックチェーンハブ
斉藤 賢爾

ks91@sfc.wide.ad.jp / ks91@blockchainhub.co.jp

簡単な自己紹介

- 斉藤 賢爾 (さいとう けんじ)
  慶應義塾大学 SFC 研究所 上席所員・環境情報学部 講師 (非常勤)
  株式会社ブロックチェーンハブ CSO (Chief Science Officer)
  一般社団法人ビヨンドブロックチェーン 代表理事
  一般社団法人アカデミーキャンプ 代表理事

- 経歴
  - 1993 年、コーネル大学より工学修士号取得 (コンピュータサイエンス)
  - 2006 年、慶應義塾大学よりデジタル通貨の研究で博士号取得 (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 18 年以上にわたり P2P (Peer-to-Peer) およびデジタル通貨等の研究に従事
  - 2011 年夏より福島のこどもたちのための「アカデミーキャンプ」を仲間らと開催
    - 昨夏は SFC にて アカデミーキャンプ 2018 夏「オッケーグーグル、宿題やっといて！」を実施
    - 先週末は アカデミーキャンプ 2019 冬「乙女のためのオートメーション ～ カワイイは自動化できる！」を実施

  → 私の頭の中ではつながっています (これからの社会のデザインはこどもたちと一緒に)

最近の著書

- 「信用の新世紀 ブロックチェーン後の未来」(2017)
- ジャンル: 短編 SF プロトタイピング + 解説 + 妄想
  - 貨幣経済の衰退から新しい経済社会のメイキングまで
  - 冒頭と末尾が短編 SF (2048 年にタイムスリップ)

- 2048 年の社会は？
  - 根本的な仕組みから自動化されている
  - 「何を実現したいのか」という、
    ひとりひとりの意思が大切である社会
- 「自動化」はひとつの重要なキーワード

- 最も大事なメッセージは
  - 人は「贈与」しか知らない環境で生まれ育つ

ブロックチェーンの真価と社会へのインパクト

- ブロックチェーンという技術について、評価が定まらない面があります
  - ビットコインを実現するために設計された ため、
    同システムにとっては実用的な、いろんな要素が入り込んでしまっています
- 本当に特徴的な部分は何でしょうか？
- それは社会にどのような意味を持つのでしょうか？

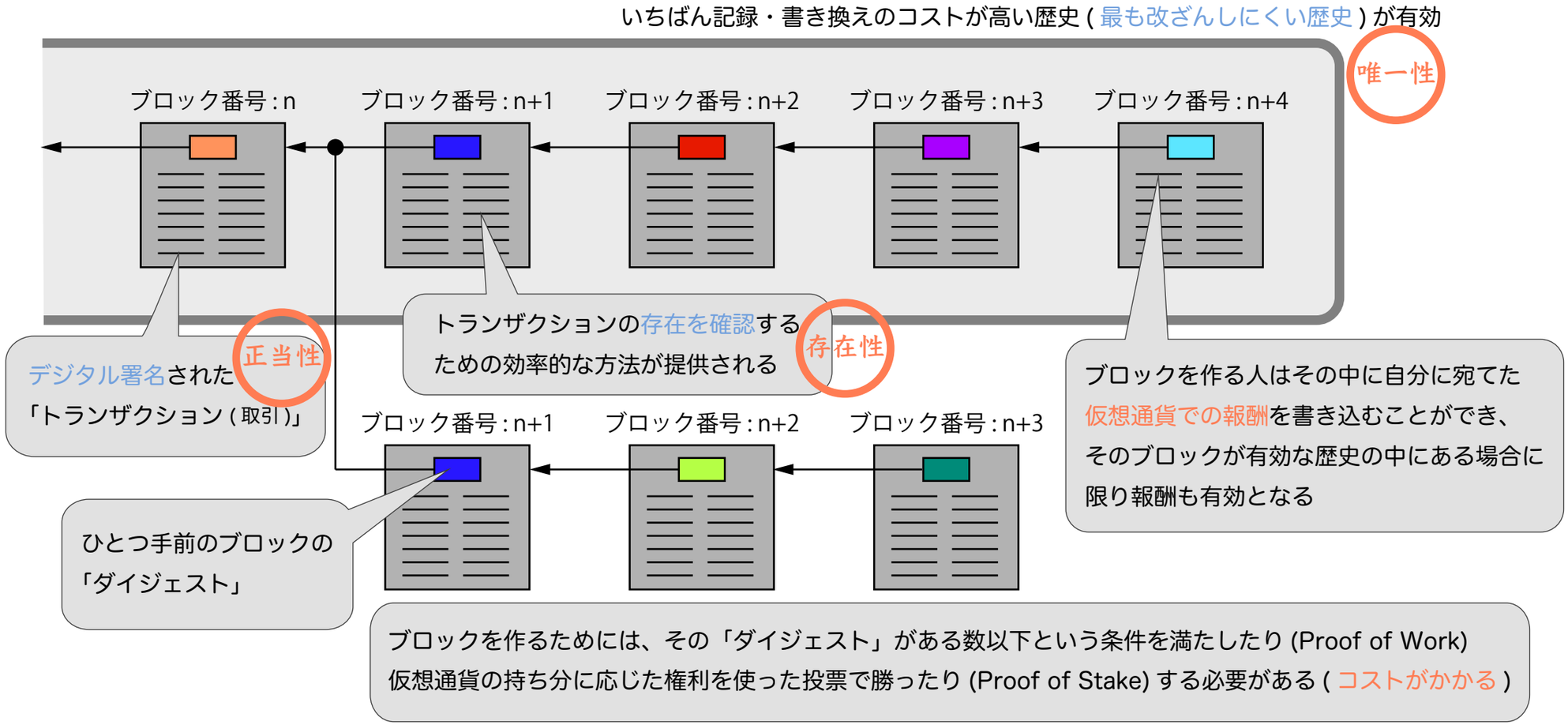
ビットコイン/ブロックチェーンの行く末は？

- 今、ビットコインとそのブロックチェーンについて説明することは、「YouTuber になりたい人に真空管の説明をすること」にも似ています (当社比)

技術の名前	テレビジョン	レッジャー (台帳)
本当にやりたいこと	遠くに映像を送ること	記録が改ざんされていないと証明すること (自分が持っているお金を自由に使うために)
最初の要素技術	ブラウン管 (真空管)	ブロックチェーン
最初のモデル	テレビ	ビットコイン
進化形	YouTube, Skype, etc.	???

- 最初の要素技術・最初のモデルは廃れ . . .
  - 本当にやりたいこと (真価) がより自由にできる方向へ

抽象化されたブロックチェーン (もはや古い？)



- Proof of Work (作業証明) の場合、投入される電力コストは仮想通貨の市場価値と均衡する
- 仮想通貨の コストで守られる記録の仕組みに全員が入ることで非改ざんの証明を行う

ブロックチェーン/台帳技術の機能を分解する

ルールの記述
例：BTC の移転

・アプリケーションロジック (何が正しいトランザクションかを決める)

唯一性の合意
例：ナカモト・コンセンサス

・矛盾するふたつのトランザクションが投入された場合、
(いずれ) 関与する全員が同じ片方を選んで歴史の中に位置づける

存在性の証明
例：作業証明付きハッシュチェーン

・過去にあったトランザクションの証拠を抹消できず、
・かつ、過去になかったトランザクションの証拠を捏造できない

正当性の保証
例：UTXO 構造とデジタル署名

・トランザクションの内容が改ざんできず、
・そのアセットに関する過去のトランザクション列に照らして矛盾がなく、
・かつ、正当なユーザにより投入されていることを保証する

- 例えばアセットを「電源」、トランザクションを「その権利や電力の売買」と置き換えて読んでみてください
- 機能が下から積み上がっています (例はビットコインですが、各層を分離して別々の技術で実現可能)
- 新奇性はどこにあるでしょうか？

ブロックチェーン/台帳技術の機能を分解する

ルールの記述
例：BTC の移動

アプリケーション層！

ョンロジック (何が正しいトランザクションかを決める)

唯一性の合意
例：ナカモト・コンセ

設計によっては不要にできる！

つのトランザクションが投入された場合、
ークル) 関与する全員が同じ片方を選んで歴史の中に位置づける

存在性の証明
例：作業証明付きハッシ

トラストに頼る必要があった！

トランザクションの証拠を抹消できず、
、過去になかったトランザクションの証拠を捏造できない

正当性の保証
例：UTXO 構造とデジ

デジタル署名でできる！

・トランザクションの内容が改ざんできず、
に関する過去のトランザクション列に照らして矛盾がなく、
・かつ、正当なユーザにより投入されていることを保証する

- 例えばアセットを「電源」、トランザクションを「その権利や電力の売買」と置き換えて読んでみてください
- 機能が下から積み上がっています (例はビットコインですが、各層を分離して別々の技術で実現可能)
- 新奇性はどこにあるでしょうか？

ブロックチェーンの真価は？

- 過去に位置づけられたデジタル署名を、何の権威にも依らずに正しいまたは正しくないと証明できるようにする → 過去に署名されたデータの 存在性の証明
  - 例題 $_1$：デジタル化された遺言書の署名が本人のものであり、内容が改ざんされていないことを証明せよ　ただし、
    - 一般に本人の死後は秘密鍵が秘密に保たれている保証がない
    - 相続人と公証人 (遺言書を保存しその正当性を保証する誰か) は共謀するかも

↑ 誰かがブロックチェーンだと言って売り込んで来たものが、
採用に値するかどうかをテストするために使える問い

  - 例題 $_2$：デジタル通貨の二重消費を検出せよ (消費を特定の過去に揺るがなく位置づけよ)
    (検出した上で互いに矛盾する取引のどちらを採用するかは実は別の問題)

→ 暗号技術の危殆化や仮想通貨暴落による停止の可能性まで考慮すると、
ビットコイン等のブロックチェーンでも解けていない問題

「遺言書テスト」

- あなたのブロックチェーンでは「遺言書」を作れますか？
  - 本人が 生前に署名した ままのかたちで遺言書が保存されていることを
  - 保存しているシステムを信用せずに (なぜなら共謀の可能性があるから)
  - 利害関係のあるすべての相続人に対して証明できますか？
    - 「内部で改ざんされていないことの証明」と「デジタル署名の事後 (永年) 証明」
    - これはあくまで問いの雛形であり、遺言書に限らず、アプリケーションに応じた具体的な問いを立てることが重要
- 多くのいわゆるプライベート/コンソーシアムの台帳技術は (少なくとも素のままでは)
  このテストに合格できないはずです
  - かといってパブリックなものは外因により停止してしまい、動かしたい人々の意思だけでは継続できない恐れがあります
    - 外因：暗号技術の危殆化や仮想通貨の暴落

BBc-1 は「遺言書テスト」に合格する技術として設計し、その参照ソフトウェアを提供します

- 今までの話に、よく言われる「分散」「共有」や「非中央集権」が入っていないが？
  ⇒　「遺言書テスト」に合格するためには、「中央」にトラストは置けません
  - 中央に位置づけられてきた機能の内部で改ざんが行われてないことの「証明」を、外部で行えることが重要
    - 改ざんを (侵入者にとって)「難しくする」だけでは不十分
  - その他、解きたい問題を解くのに必要な要素技術は、ブロックチェーン以前から存在しているのでは？
    - 例：可用性・耐障害性のための複製&分散合意技術、自律性のための P2P, etc.
    - ブロックチェーンについて騒がれている部分の多くは単に「分散システムの性質」
    - 必要に応じて既存の技術を適用できる

合格を阻む課題 (いろいろあるのですが重要なものを抜粋して)

- ブロックチェーンや台帳技術の技術的課題
  - パブリックに動いている技術 (狭義のブロックチェーンなど / 《新聞モデル》) は
    - 規模・多様性の大きさによるコストで守られている

      (多様性についてはそうでもないという現実)

      → コストをかければ破壊でき、そのコストは (巨大だが) 見積もれる
    - 勝手に動いているため、使いたいだけ持続するという保証が無い

  - プライベートに動かす技術 (プライベートレッジャーなど / 《社内報モデル》) は
    - 規模・多様性が小さいので守られていない (証明機能がない)

      (内部の者によって改ざんできてしまう)

      → 解決策はあると考えています (BBc-1 を開発・検証中)

      (プライベートレッジャーを連携させて存在の証拠を持ち合います)

- 記録と実体に関する本質的な課題
  - 技術だけでは解決できない領域を含む (公開鍵は本人のもの？)

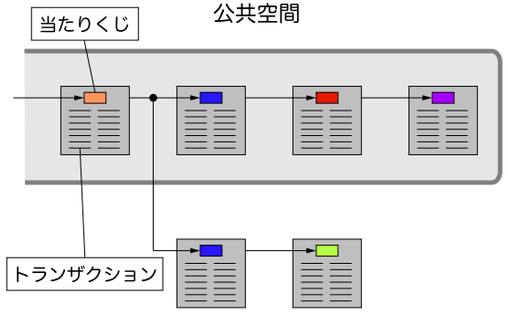
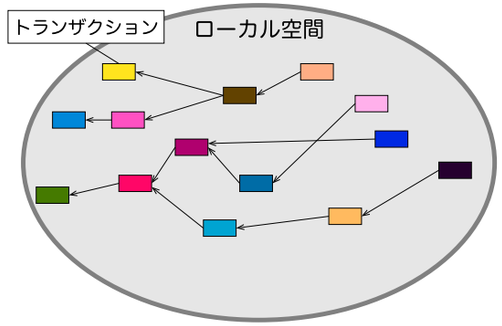
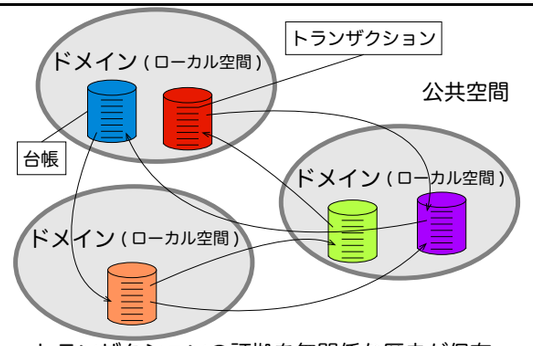
(合格すれば) 例えば文書を公正に保全できるが...

- 文書の保全は社会における共通理解の固定化

- 文書は社会の礎である (例：法文)
- 文書は自動化の要でもある (例：契約書とその自動的な執行)
  - そもそもコンピュータのプログラムコードも文書である
    ↑ いわゆる「スマートコントラクト」の真価
    - 実行されているプログラムコードの真正性を担保する
    - P2P で動くコードに対してそれをする (例：Ethereum) のはむしろ特殊例では？

- デジタルな文書の管理のシステムに社会の信用を預けられるか、ということが、
- 多くのブロックチェーン《と・呼ばれるようなもの》でできるかも知れない
  問題解決の基礎となる
  - 「自動化」は重要なキーワード

ブロックチェーン/台帳技術の比較

プラットフォーム	Bitcoin, Ethereum 等	プライベート DLT 一般	BBc-1
メタファー	(民主的) 新聞モデル	社内報モデル	古文書 (参考文献) モデル
存在性の証明方法 (抹消・捏造不可)	作業証明 (仮想通貨の コストで守る)	ない (遺言書テスト不合格) (内部無矛盾性)	コンテキスト証明 (研究中) (外部性で守る)
唯一性の合意方法 (矛盾の解消)	ナカモトコンセンサス (最大コストの歴史を選択)	冗長化された第三者 による分散合意	(冗長化された) 関係者 による (分散) 合意
イメージ	 ・作成時と同じだけくじを引かないと改変できない ・最もくじが引かれた歴史を有効とする	 ・トランザクションの関係と順序をローカルに表現 ・証明にはならない	 ・トランザクションの証拠を無関係な歴史が保有 ・どれかの台帳を無矛盾に書き換えても証拠が残る

- Ethereum はデポジットに応じた投票権による分散合意に舵を切ろうとしている (やはり仮想通貨のコストで守ろうとしている)
- 仮想通貨のコストで守ると、それを超える価値を扱えない

レッジャー (台帳) を応用する

- レッジャー？
  - 記録が正しく保全・アクセスできるようにデジタル拡張された台帳・帳簿です
  - 例えば「メール」と聞いても私たちはすでに「郵便物」は想起しません
    - そのデジタル拡張のことだと誰もが思います

小さく見える技術が社会を大きく変える

- IP (Internet Protocol) (インターネットの基礎となる通信規約)
  - 真価：IP アドレスで示された端点から端点へのパケットの到達性を提供する
  - 巻き起こした変化：
    - 郵便に代わるもの、電話に代わるもの、出版に代わるもの、テレビに代わるもの などを生み出し、それぞれがその前身よりも遥かに軽やかに使えることで、人々のコミュニケーションを革新的に変えた

- レッジャー/ブロックチェーン (IP 上のアプリケーション)
  - 真価：過去に位置づけられたデジタル署名を、何の権威にも依らずに正しいまたは正しくないと証明できるようにする
  - 巻き起こすだろう変化：
    - 記録の公正性のレベルを押し上げ、支払いを、会計を、登記を、契約を、そして行政・立法・司法をも含む社会基盤を遥かに軽やかにする変化をもたらす？

想定される社会的変化

- デジタル拡張が引き起こす一般的変化が帳簿や台帳にも起きる
- 例：郵便 ⇒ メールや LINE などのメッセージングの場合
  - 郵便は公共性が高く「三十四丁目の奇蹟」や「投票所入場券」の例を出すまでもなく本人の証明にも関わる

  → 郵便局みたいなものは自分で立てられる

  → 手紙を郵便で送るという行為が著しく面倒くさくなり、
  一方、メールやメッセージングは過去に郵便がそうだったよりも
  遥かに人々にとって身近で多用される (同居する家族の間ですら使われる)

- (公的な) 台帳・帳簿 ⇒ レッジャーの場合

  → 公証役場や法務局、監査機関みたいなものは自分で立てられる

  → 従来の公証サービスを使う行為が著しく面倒くさくなる

  → 過去に公証サービスがそうだったよりも遥かに身近で多用される
  - 例えば映画のチケットや、レストランの予約、あるいは会議室の予約にすら使われても全然おかしくない
  - 「従量制」のうちは、そういう大きな変化は起きない

何に使えるのか

- 権限を表現できる
  - 特に公共財について、使用権・所有権などのマネジメントに
    - 貨幣は公共財なので、最初に応用された とも言える
    - 電源・電力は、広い意味で公共財
- 存在を証明できる
  - 公証に (例えば遺言書のデジタル化が初めて可能になる)
  - サプライチェーンのマネジメントに (記録と実体の一致には要注意)
- 銀行・金融機関を解体できる . . .
  - 銀行ネットワークをバイパスする送金
- 自由に貨幣媒体を設計できる (いわゆる「トークンエコノミー」の世界)
  - 新しい貨幣がたくさん出てくると煩雑になるが . . .
    - 貨幣が見えなくなり、その利用に関わる複雑なオペレーションは各自に専属するソフトウェアエージェントがやってくれることを前提に

サイボーグ社会

- サイボーグ (cyborg) = サイバネティック (cybernetic) な組織体 (organism)
- 社会が新しい目や耳、手や足をもつ
  - 例 $_1$：どこにいても「藤沢市付近に雨雲が近づいています」と知れる ← 今ココ
  - 例 $_2$：実際に家の洗濯物をロボットが取り込んで畳む

- いろんなことが自動化される ⇒ 貨幣が不要な社会？
  - (1) 労働の対価としての貨幣というときの「労働」の変化
  - (2)「欲望の二重の一致」が自動化されたり「交換」自体が不要になる

⇒ しかし、その新たな目や耳を通して知られた内容は正しいか？

- そして制御の判断は正しいか？公正か？バイアスは無いか？
  - 「自動化されている仕組みをどう信頼できるか」← レッジャーの出番

電力システム等のインフラでは

- まさにサイバネティックなシステムとして
  - センシング
    - 電力制御の根拠となるデータは正当か
    - センサがデジタル署名するだけでは不十分 (「遺言書テスト」)(以下同様)
  - 判断・制御
    - 判断・制御の自動システムは正当に学習しているか
  - アクチュエーション
    - 送られたコマンドは正当か
  - 以上の経過をトレースし検証できるか
- 持続可能な (SDGs 的な) 社会インフラに向けて
  - グリーン電力証書 (証明書)
  - グリーン電力証券 (電力により償還される債権)
- 他

まとめに代えて

- ここ数年、製造業においてある種の問題が継続的に浮上しています
  - 「品質不正」の問題です
  - 品質の維持に関わるデータやソフトウェア等の改ざんが相次いでいます

- レッジャーは、こうした改ざんを検出可能にするかも知れません
  - 不正を抑止するようにシステムを構成できるという期待

- しかし、そもそもの問題は現代の経済社会における企業の「利益目標」の重視とその倒錯した優先順位への盲従があるのでは？
  - レッジャーが関わるかどうかは別として、
  - デジタルテクノロジーの発展と受容が経済社会に与えるインパクトは、新たな貨幣媒体の創造や キャッシュレス や シェアリングエコノミー の台頭といった現象からも垣間見られるように、
  - 根本的なところで貨幣にもとづく社会構造自体を変化させていく可能性があります

⇒ 拙著「信用の新世紀」の冒頭の SF につづく