黄金期は過去ではなく未来にある。

ブロックチェーンを超えて — デジタル通貨とトークンエコノミー

慶應義塾大学 SFC 研究所・環境情報学部 / (株) 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 **年間にわたり** 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」を実施**
    - 今夏は 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！」を実施済

  → **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)

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？

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

ョンロジック (何が正しいトランザクションかを決める)

アプリケーション層！

唯一性の合意
例：ナカモト・コンセ

つのトランザクションが投入された場合、
ルが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

設計によっては不要にできる！

存在性の証明
例：作業証明付きハッシ

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

トラストに頼る必要があった！

正当性の保証
例：UTXO 構造とデジ

・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

デジタル署名でできる！

- **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？
    - これはあくまで問いの雛形であり、アプリケーションに応じた問いを立てることが重要
    - 遺言書に限らず、署名後も長期に渡り正当性を担保しなければならない文書の作成・検証を問いにできます
- 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

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

- 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

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

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
  - もちろん貨幣システムにも

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

トークンエコノミー

- **サービスを受ける権利から**
- Politics (**秩序形成**) **の道具へ**

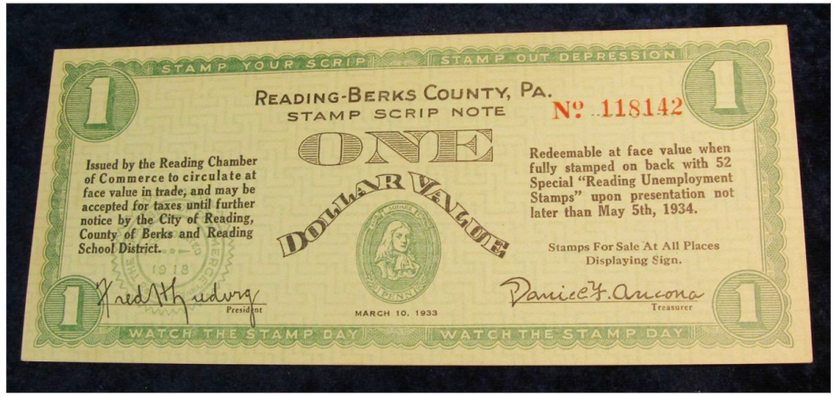
現状はさほど面白い状況ではない...

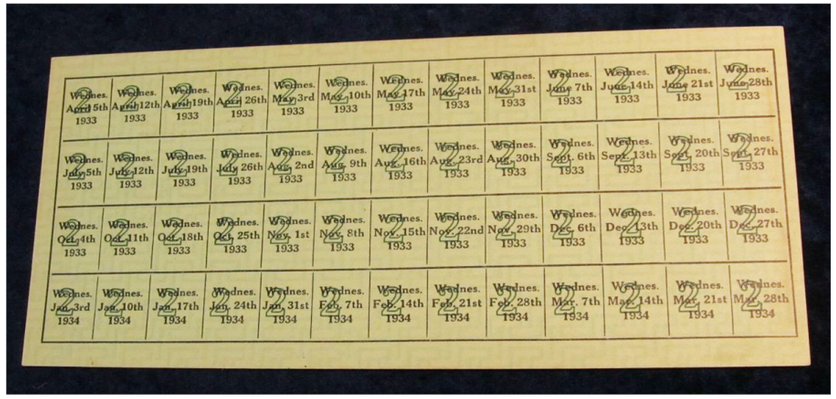
- ICO : Initial Coin Offering
- **これから実施するプロジェクトで使うトークンを先に売りに出して プロジェクトのための資金の調達に充てる**
  - **そのトークンが値上がりする期待をもって人々が買っていく**

- **「ひと山当てたい人が、他の人のひと山当てたいという気持ちを利用して プロジェクトのためのリソースを獲得する」モデルの一般形**
  - 400 年前からある

- **拙著「不思議の国の NEO」で提案したモデル**
- **「貢献したい人が、他の人の貢献したいという気持ちを利用して プロジェクトのためのリソースを獲得する」モデル**
  - **流行らせたい**

1930年代 – スタンプ紙幣

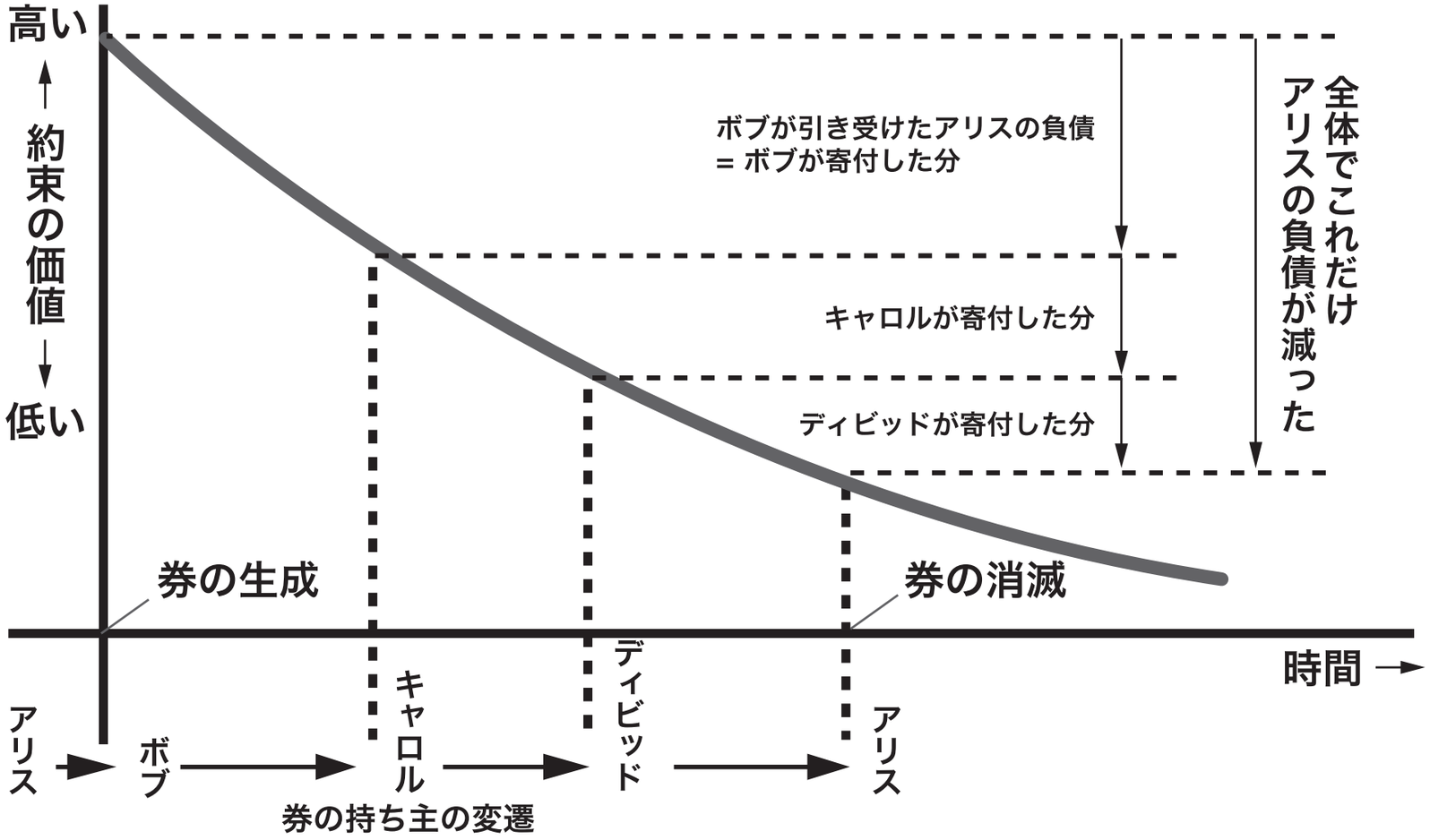




- オーストリアの街ヴェルグル (Wörgl) 等にて 1930 年代に実施
  - 大恐慌時代
- 地方政府が発行する「労働証明書」
  - 公共事業のための支払いに使用
- 毎月とか毎週、裏側に有料のスタンプを貼らなければ無効
  - 事実上、価値が減っていく貨幣
- すさまじいスピードで流通し、景気を回復した
- 中央銀行との裁判に負けて中止に追いやられた
- 今ならデジタルで、より直接的に実現可能

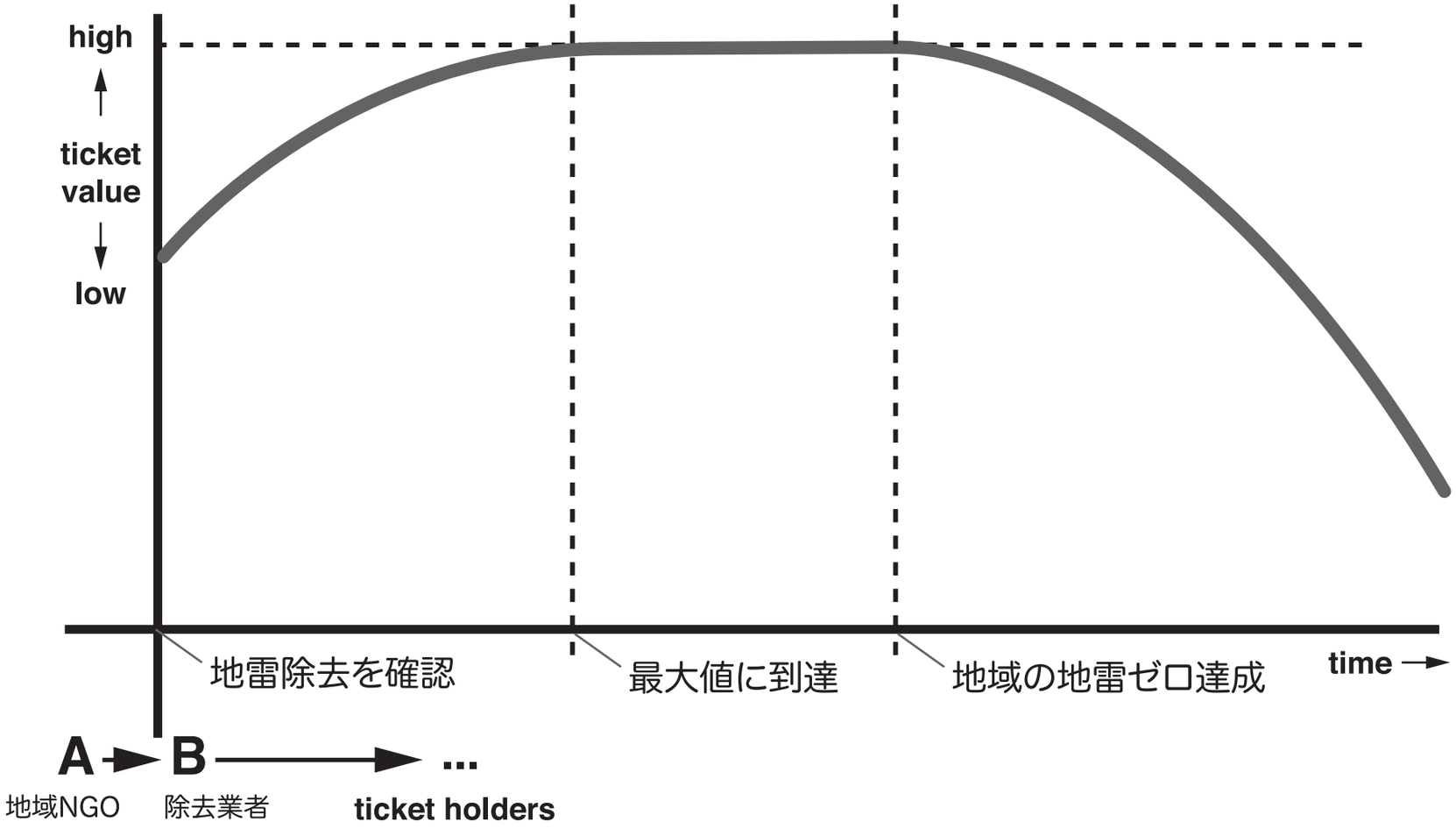
- http://www.icollector.com/

貢献のためのトークンシステム



- 善意にもとづくようでいて . . .
- 本質的に手数料ゼロ (溜め込まない場合) の支払い手段が作れる

地雷除去デジタル通貨の増減価モデル



- なるべく多くの貨幣を最大値にすべくこぞって除去し、完全に除去するまで続けるのが最適な戦略となる
- 増減価により人の行動を制御できる (むしろ行政ツールなのかも知れません)

Politics の道具としてのトークン

- 【政治 (politics)】
  - 諸権力・諸集団の間に生じる利害の対立などの調整・秩序形成

- 減価する貨幣を用いるデザインは、おそらくあらゆる廃棄物処理に適用可能
  - スペースデブリ、CO_2、海洋廃棄物、...
  - 従来の政治が成し遂げられなかったことを可能にするという期待

- 多くの「実現したいこと」に対して同じ仕組みが用いられるとすれば...
  - 「**投票行為としての消費**」の概念が拡張される
    - 「実現したいこと」が共感を得られるなら貨幣を発行できる
    - 生産や流通の自動化の恩恵もあり、私たちが生きていくためのコストは下がり続け、
    - 従来の意味での貨幣は衰退し、私たちはそもそも「消費者」であることを止めていく ...
  - トークンを選ぶことを通して politics が行われる
    - 私たちひとりひとりが、何に参与するのかを主体的に決める

まとめに代えて — 想定される社会的変化

- 私たちが常用している貨幣に対してデジタル化が引き起こす変化
  - → 銀行《の・ようなもの》は自分で立てられる
  - → 銀行マネーを使う行為が著しく面倒くさくなる
  - → 過去に銀行マネーがそうだったよりも遥かに身近で多用される
  - → トークンは (心理) コストと無縁 (希少ではない)

- 「**サービスを受ける権利の表現**」としてのトークンは、やがて
- 「Politics (**秩序形成**) **の道具**」に変化すると考えられます

- その大きな変化を見据えた上で、
  目前の課題を解決するための設計から始める必要があります