Indivisible or Divisible?

不動産テクノロジーとしてのブロックチェーンとその技術的・政策的課題

慶應義塾大学 SFC 研究所 上席所員
斉藤 賢爾

ks91@sfc.wide.ad.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 (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 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 17 年以上にわたり P2P 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

  → 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?)

ブロックチェーンは何を提供する技術か

- 1) 内容も存在も誰にも否定できない記録を保存・維持する
  - 「記録」の例：不動産登記、賃貸契約、代金や賃料の支払い、etc.
- 2) その確かさを誰でも確認できる
- 3) 以上のことを誰にも止めさせない

⇒ あたかも空中に記録を固定できる

⇒ 二重の課題がある

- そのことは本当に実現できているのか？
- そのことが実現できたら不動産を表現して取引できるのか？
  - ヒント：「記録」の「正しさ」についてはここでは述べていない

ブロックチェーンとは何か

- 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？
    - (中央) 銀行マネーへの不信

- 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 (検証可能性と内容の否認不可能性の担保)
  - 二重消費 (double spending) を防ぐ必要がある (存在の否認不可能性を担保したい)

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

- ブロックチェーンは、あたかも「空中に約束を固定する」
  - 「約束」の形式をもつ記録を固定できる → 貨幣は「約束」であり、公共財
  - (広い意味の) 公共財を公正に扱うことができるという期待 (完全ではない)

ビーカー / 新聞モデルの世界 (1)

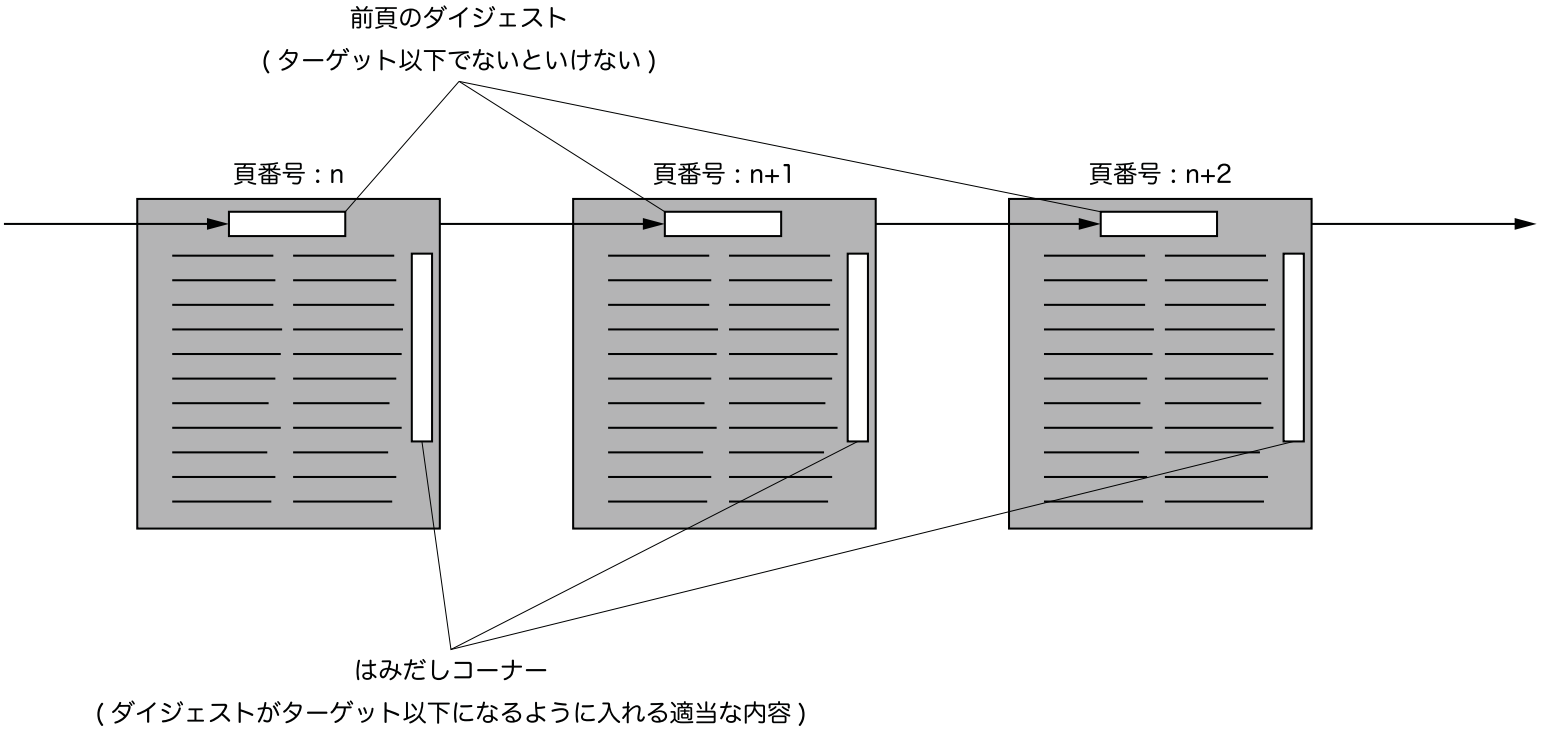
- ビットコインとブロックチェーンを物理モデルで説明します
- 2,100 万 cm^3 の、人類にとって無価値な液体がある
  - タンクに入っている
- 1 億分の 1cm^3 まで計量できるビーカーを各自がいくつでも持てる
  - 公共空間に置かれる
  - ビーカーには鍵付きの蓋がついている
- 平均 10 分おきに選ばれた人だけが、自分のビーカーに今なら 12.5cm^3 くみ出せる
  - 特殊なくじ引きで選ぶ
  - 当たりくじは、各自の箱の中にあり、それぞれが全力でくじを引きまくる
    ⇒ 速く引けた方が有利
    ⇒ 「システムが停まらない (ライブネス)」性質を満たせる

ビーカー / 新聞モデルの世界 (2)

- ビーカー間で比較的自由に液体をやり取りできる (正当性の保証)
  - ビーカーの蓋は本人にしか開けられない
  - 一度開けたら、他の (複数の) ビーカーに注ぎ切る
- 先の「選ばれた人」は、やり取りを「監査」し、新聞の紙面をつくって記録を残す「追記人」でもある (存在の証明)
  - やり取りのおこぼれ (手数料) ももらえる
- 同じページ番号が被ったら、ページ列の長い方の履歴が有効 (唯一性の合意)
- ときどき、液体の入ったビーカーを割ってしまう人がいる
  (というか、ビーカーの蓋の鍵を無くす人がいる)

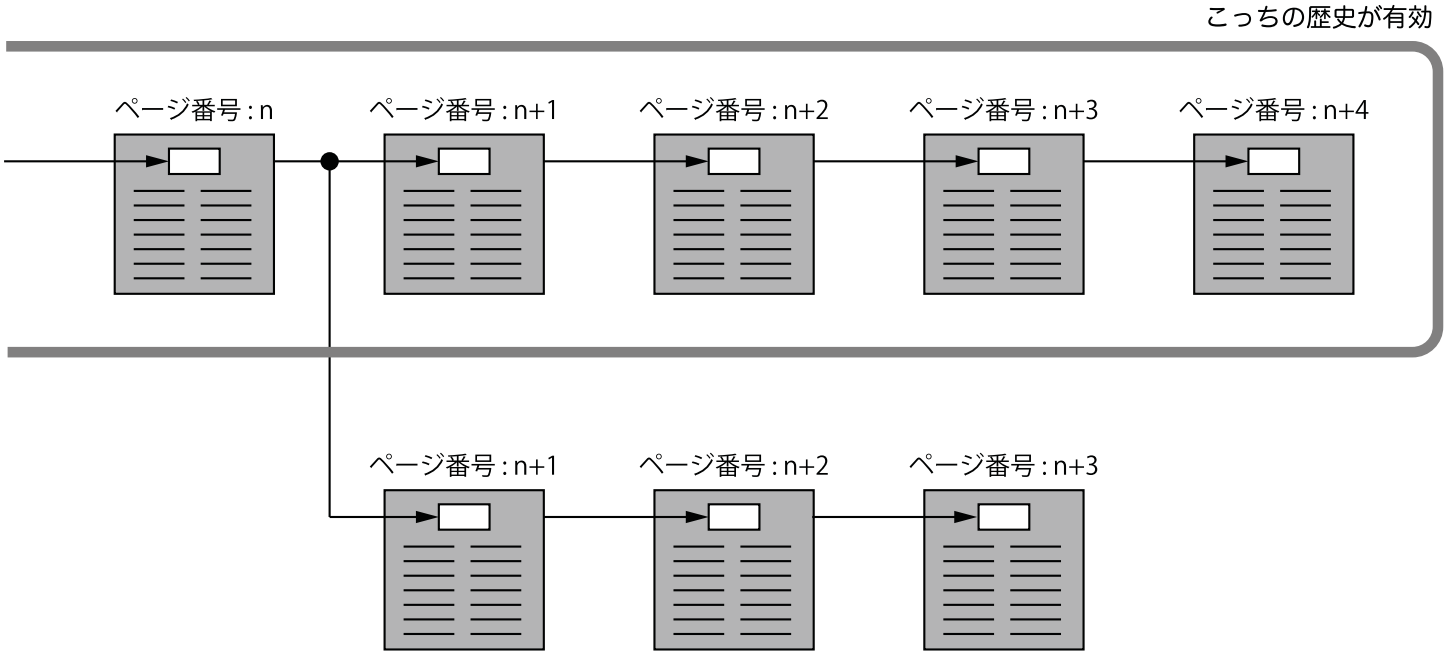
- そんな仕組みをデジタルでつくり、通貨と見なしてみた
  → ビットコイン
  (見なしを必要としない貨幣・通貨は法貨も含め存在しない)

存在の証明 ~ 作業証明付きハッシュチェーン



- ページのダイジェスト (暗号学的ハッシュ関数による出力) はターゲット以下でなければならない
  - 元のデータをどういじればどんなダイジェストになるのかは予めわからない → 途方もない作業を要する
- これがくじ引きの原理であり、同じだけのコストをかけなければ改ざんできない

唯一性の合意 ~ ナカモト・コンセンサス



- ほぼ同時に別々の誰かがくじに当たってページ列が分かれてしまう現象はたまにある
- くじ引きに累積で最も大きなコストがかかっている歴史が最も改ざんしにくい
- それが正史であると全員が合意する (厳密なコンセンサスは実現できていない)

ブロックチェーン/DLT の現状

- ブロックチェーン (主として「空中」はグローバル)
  - Bitcoin (ザ・ブロックチェーン)
    - Open Assets Protocol (OAP)
      (ビットコインブロックチェーン上に任意の量を定義して移転できる)
  - Ethereum (分散アプリケーションのための基盤) (多分に実験システム)
    - Enterprise Ethereum Alliance (↓ こっち方向への進化)

- その他の分散レッジャー (DLT) (主として「空中」はローカル)
  - Hyperledger (Linux Foundation)
    - Fabric (IBM/DAH), Sawtooth (Intel), Iroha (ソラミツ)
      などの開発が進行中
  - Corda (R3)
  - 本当に記録の内容も存在も誰にも否定できないのか？
  - 記録の確かさを誰でも確認できると本当に言えるのか？

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 (巨大にスケール、暗黙的に実時間)

- 赤字はビットコインの流れを汲む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
  - その問題を解こうとして、元々解けていた問題が解けなくなることもある

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, Everledger, Factom, ...
    - 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
  - 来歴証明 (トレーサビリティ、トラッキング、アカウンティング)
    - 元々の設計用途の範疇 (「新聞」の代わり)
    - 権限の推移を証明するという意味では不動産にも関わる

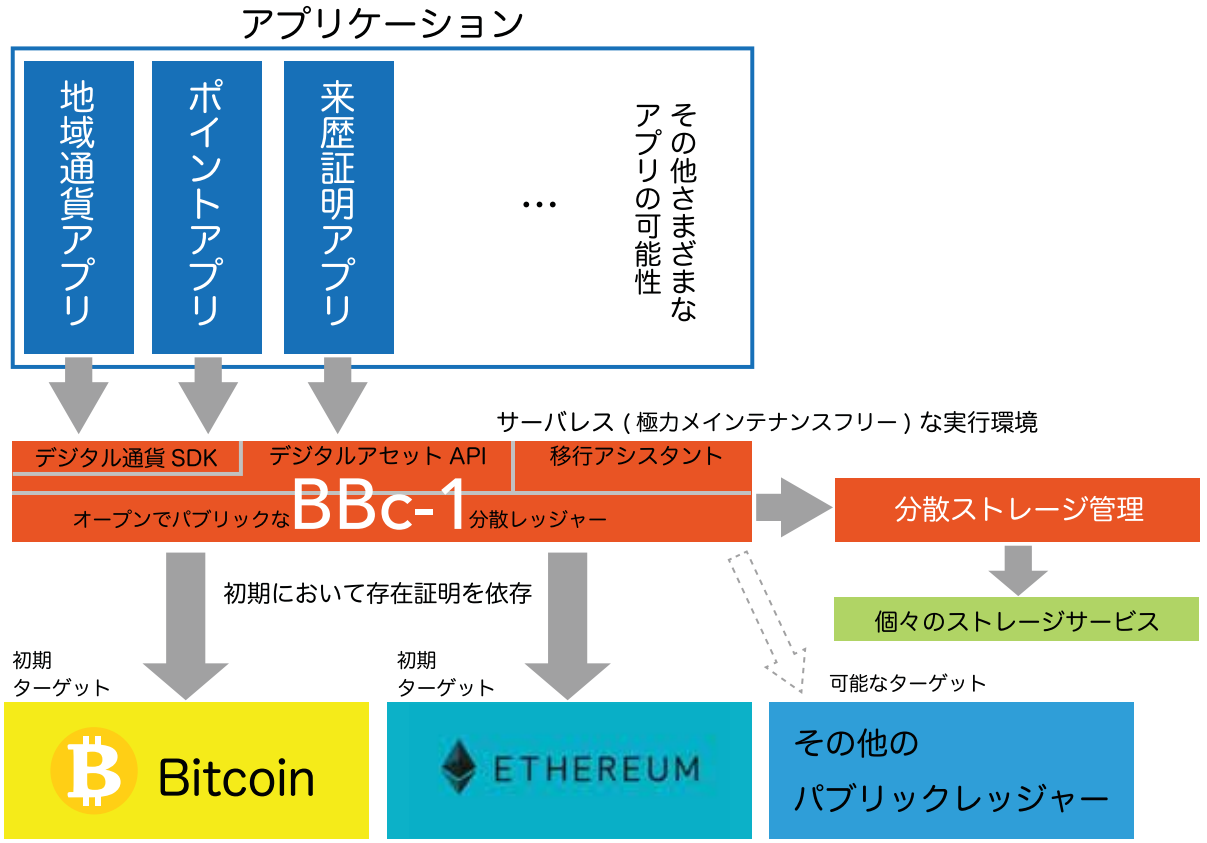
ブロックチェーン/DLT の課題

- 実時間性 (確率的動作)
- 秘匿性 (万人への検証可能性の担保)
- ワンネス (分散 vs. 複製)
  - スケーラビリティ (全参加者に複製されるならスケールしない)
  - 進化のガバナンス (全員が一丸となる必要があるなら変われない)
- インセンティブ不整合性
  - ネイティブ通貨の価値で支えられている (暴落するとすべての応用が止まる)

⇒ ゼロベースで設計し直せば解ける

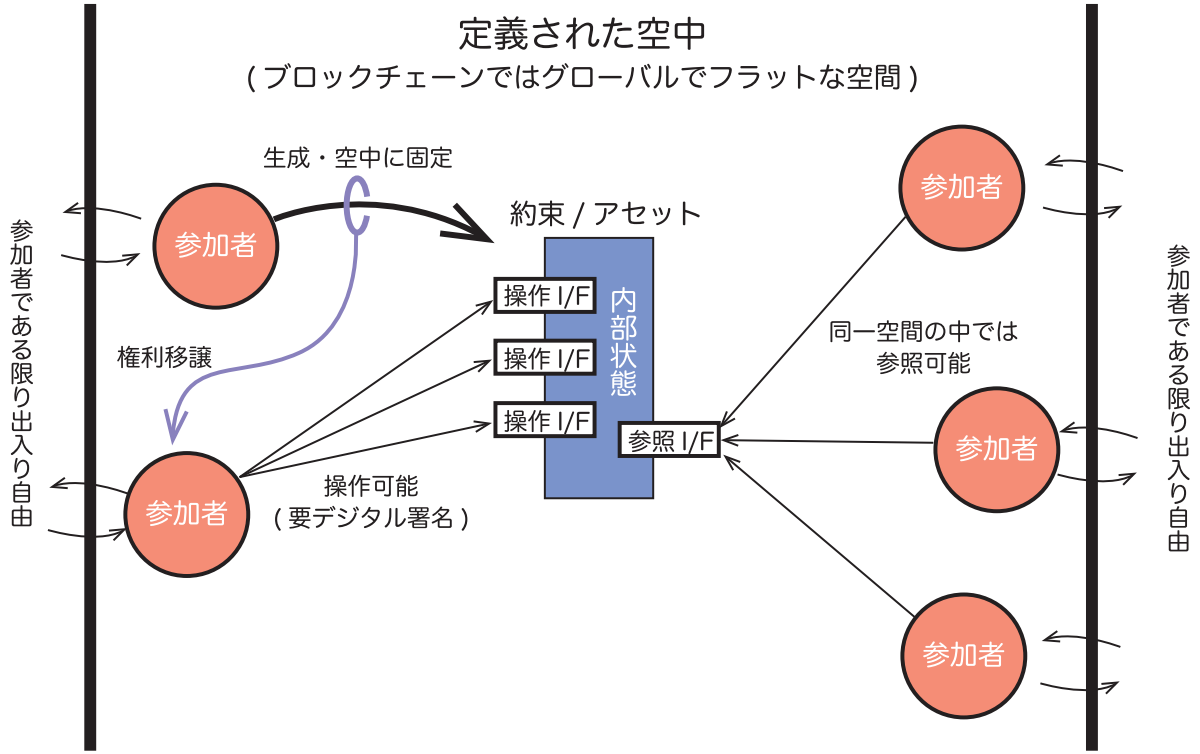
- 実際に進行中です
- 多くの DLT はゼロベースで考えていないところが問題
  - 例：作業証明の付かないハッシュチェーンは改ざんし放題
  - 例：新聞モデルで、業界紙や社内報に載せるようなことをしても存在証明にならない

Beyond Blockchain One (BBc-1)



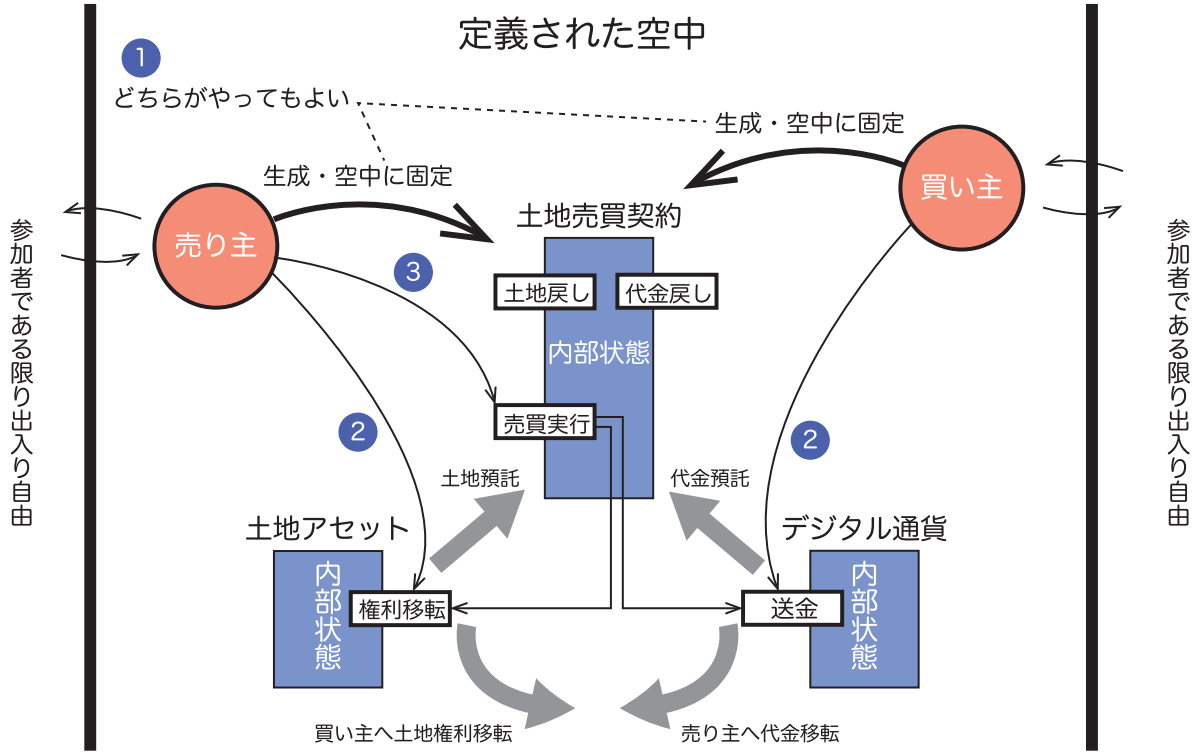
- 言わば「お客様も社内報にアクセスできます」といっただけの状況でも存在証明ができる
- 2017 年 10 月 31 日からオープンソースソフトウェアとして公開 (https://github.com/beyond-blockchain/bbc1)

空中約束固定装置



- 定義された空中は参加者たちの力だけで維持する (特定の管理者はいない)
- 約束/アセット (=スマートコントラクト) は権利を持つ参加者しか操作できない
- 特定の誰かが維持していないので、定義された空中が存続するかぎり約束/アセットも存続できる

例題 — 自動エスクローによる土地の売買



- 1. 土地や代金の持ち逃げを防ぐために売買契約を空中に固定 (どちらがやっても内容を検証可)
- 2. 土地の権利や代金を売買契約に預託する (気が変わったら取り戻してよい)
- 3. 実行 (これもどちらがやってもよい) すると、条件が揃っているなら土地の権利と代金が同時に移転する

まとめ

- 0) 土地・建物のアセットがデジタルに一意に表現され記録される
  - 政策としてそのことが支えられていくことが必要
  - 記録の「正しさ」を保証する在り方とは？
- 1) 内容も存在も誰にも否定できない記録を保存・維持できる
  - 権限をもつ者ならば、
  - 記録の更新を (外部イベントを契機に) 自動的に実行できる
- 2) その確かさを誰でも確認できる

- 以上が本当に実現されるなら、不動産にブロックチェーンが応用できる
  - 新聞モデルで言えば、社内報や業界紙に載せるレベルでは通常は「誰にも」や「誰でも」を実現できない

- 技術的・政策的課題は山積しているが、ポテンシャルは秘めている