beyond-blockchain.org

BBc-1 : Beyond Blockchain One

～ ブロックチェーンを超えて ～

一般社団法人ビヨンドブロックチェーン / 慶應義塾大学 SFC 研究所・環境情報学部

斉藤 賢爾

ks91@beyond-blockchain.org / 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・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
    - 今冬は 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)

はじめに

- ブロックチェーンの課題
- BBc-1 とは？
- リソース
- アーキテクチャ

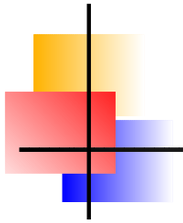
ブロックチェーンの課題

- そもそもブロックチェーンとは何か、というのはあとで議論するとして . . .

- パブリックなレッジャーの課題
  - 外因により停止したり安全性が損なわれる可能性がある
    - 外因：暗号技術の危殆化 や ネイティブ仮想通貨の市場価格の暴落
  - 実時間性・秘匿性の課題
  - ワンネスによる困難 (スケーラビリティの欠如、新技術を実地で試せない)

- プライベートなレッジャーの課題
  - 証明機能が外部に提供されない場合、
    外から見て既存のデータベースと変わらない (無意味)

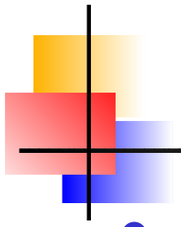
- BBc-1 にてこれらの課題を解きます



BBc-1 とは？

- BBc-1 では、
  - 記録ができます
  - 記録の存在を証明できます
  - 権限をもつ本人であることをデジタル署名で証明可能な場合に限り、その記録を更新する、といったことができます (アプリケーションレベルで)
  - 「BBc トラスト」を実装します
    - https://speakerdeck.com/beyondblockchain/bbc-trust

- 特徴
  - (1) 台帳における情報同士の関係性の記述力が高い
    - 入出力関係だけでない、より一般化された UTXO 構造
  - (2) システム上の「合意」を現実社会のそれと一致させることができる
    - サインリクエストと署名の検証、高次の検査は上位層 (ライブラリやアプリケーション) が自由に定義できる
  - (3) 改ざん検知の機会が向上している
    - トランザクション間の関連、アンカリングやコンテキスト証明の活用、能動的検知

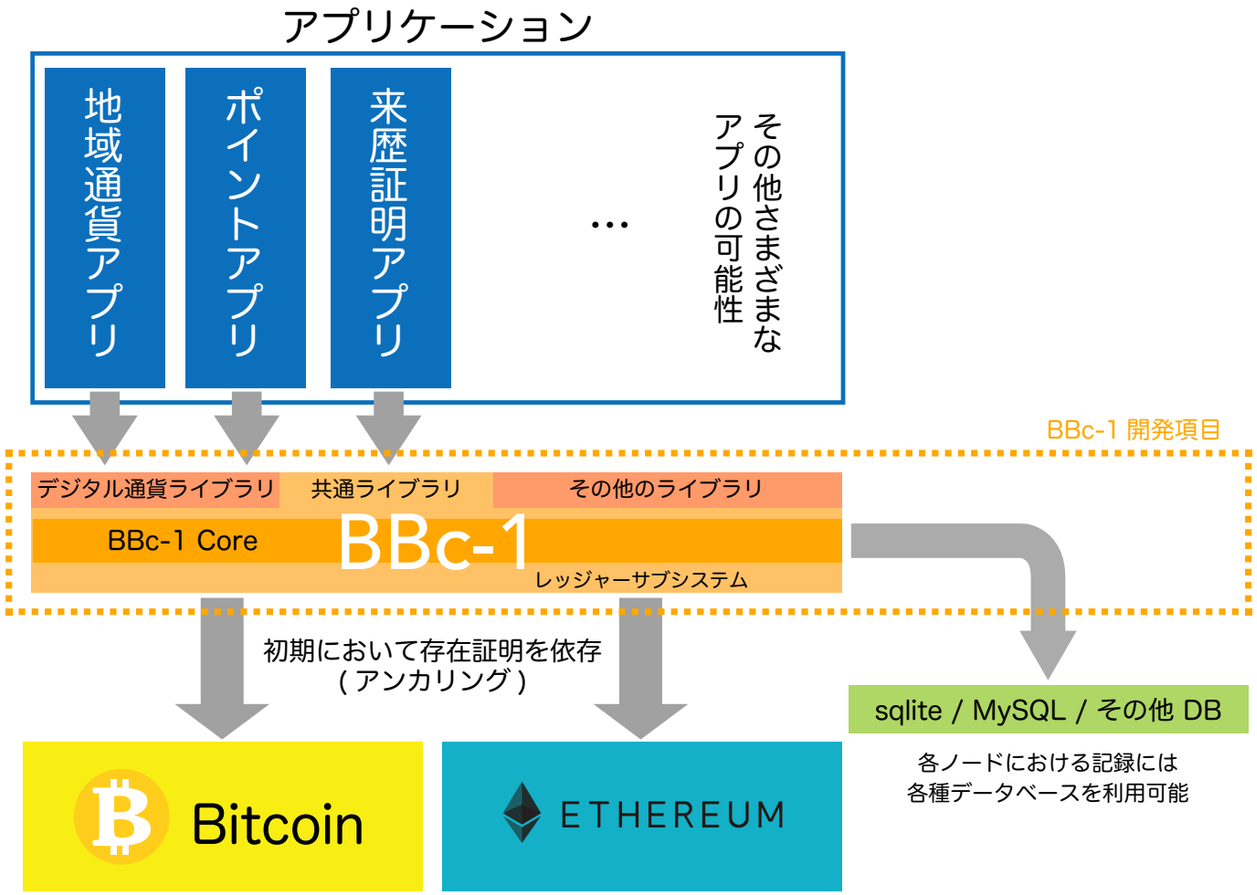


リソース

- GitHub
  - https://github.com/beyond-blockchain
- Web
  - https://beyond-blockchain.org
- Speaker Deck (スライド)
  - https://speakerdeck.com/beyondblockchain

- 連載
  - 「ブロックチェーンの課題と可能性 ~BBc-1（Beyond Blockchain One）から学ぶブロックチェーン開発」
  - https://gihyo.jp/dev/serial/01/bbc1
  - BBc-1 のメイン開発者である久保 健さんと執筆しています

アーキテクチャ



- 初期には Bitcoin や Ethereum といった既存のブロックチェーンにアンカリング (証拠の埋め込み) をすることにより、トランザクションの証明機能を達成します
- 中長期的には「履歴交差」の考え方を応用した独自方式「コンテキスト証明 (Proof of Context)」により達成します
(機能は初期から提供しつつ研究開発していきます)

ブロックチェーンを理解する

- 機能の階層構造
- 「遺言書テスト」

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

- 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)
- 例えばアセットを「債権」、トランザクションを「その証券化と売買」と置き換えて読んでみてください
  - ビットコインは 債権ではないアセット なので、実は特殊事例だということが分かります
- 新奇性はどこにある？

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！

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、
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、
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

- 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)
- 例えばアセットを「債権」、トランザクションを「その証券化と売買」と置き換えて読んでみてください
  - ビットコインは 債権ではないアセット なので、実は特殊事例だということが分かります
- 新奇性はどこにある？

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
    - 解きたい問題がこのテストの形になる → 不合格なら使えない
    - 解きたい問題はこのテストの形にならない → そもそもブロックチェーンを使うことの意味がない
    - 解きたい問題は特に無く、このテストに合格しない技術を使って「ブロックチェーン」実証実験「成功」 → 超不幸
  - 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ぎなく位置づけよ)

    (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」

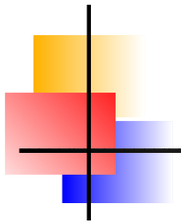
- あなたのブロックチェーンでは「遺言書」を作れますか？
  - 本人が 生前に署名した ままのかたちで遺言書が保存されていることを
  - 保存しているシステムを信用せずに (本人の秘密鍵を取得した相続人との共謀の可能性があるから)
  - 利害関係のあるすべての相続人に対して証明できますか？
    - 「内部で改ざんされていないことの証明」と「デジタル署名の事後 (永年) 証明」
    - これはあくまで問いの雛形であり、遺言書に限らず、アプリケーションに応じた具体的な問いを立てることが重要
- 多くのいわゆるプライベート/コンソーシアムの台帳技術は (少なくとも素のままでは)
  こ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、よく騒がれる「合意形成」「共有」や「非中央集権」が入ってないが？
  ⇒ 「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」を外部から行える 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 (複製の一致を保証)、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

機能設計の各論

- ドメイン
- 正当性の保証
- 存在性の証明
- 唯一性の合意

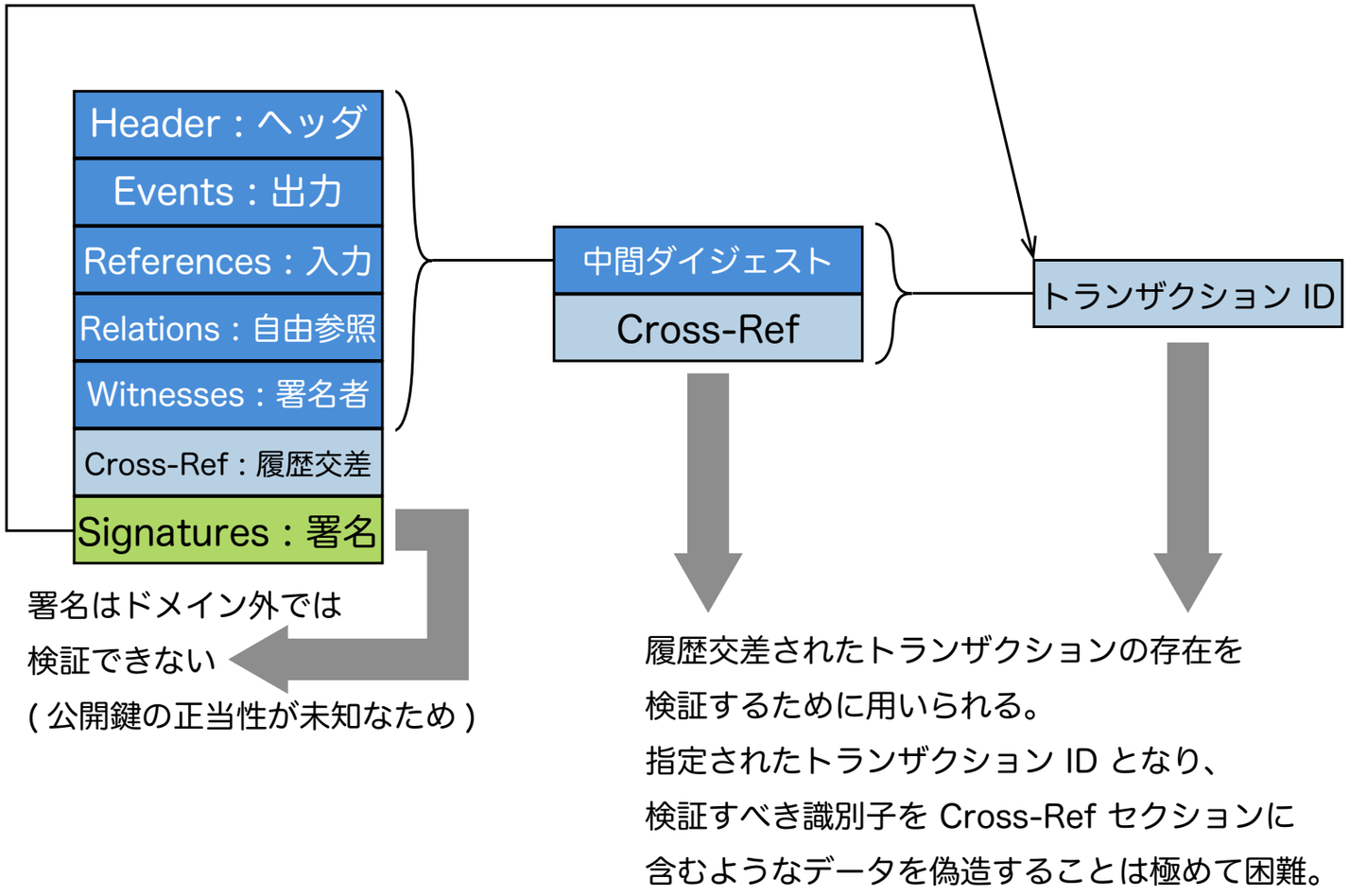


ドメイン

- ドメインは自治される台帳システムの単位
  - ドメイン外にはトランザクションの内容と存在は秘匿され、
    ドメイン内へのアクセスは制御される
  - アクセス権を得られるのであれば、複数のドメインに跨がる
    アプリケーションも構築できる

- コンテキスト証明 (Proof of Context; PoCX)
  - 利害関係の無いドメインの無関係なコンテキストの中に、
  - トランザクションの (ハッシュ木のルート) ダイジェストを埋め込むことで、
  - 存在性を外部から証明可能にする

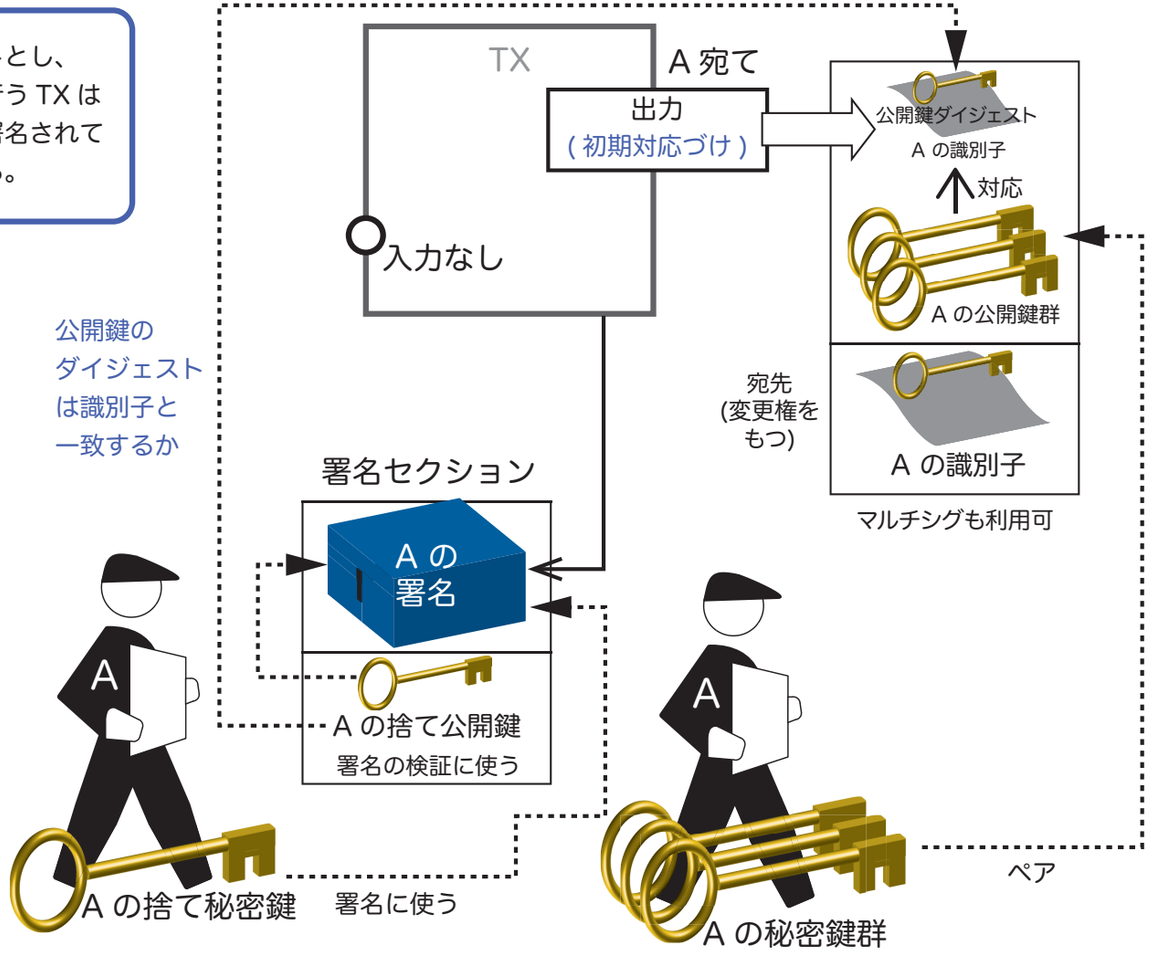
正当性の保証 – トランザクションの構造



- 必要な署名を揃えた上でこの構造がレッジャーに格納されることを以て、トランザクションはファイナルとなる
- UTXO (入出力関係の記述) と状態のトラッキングのいずれの方法でもトランザクションを記述できる

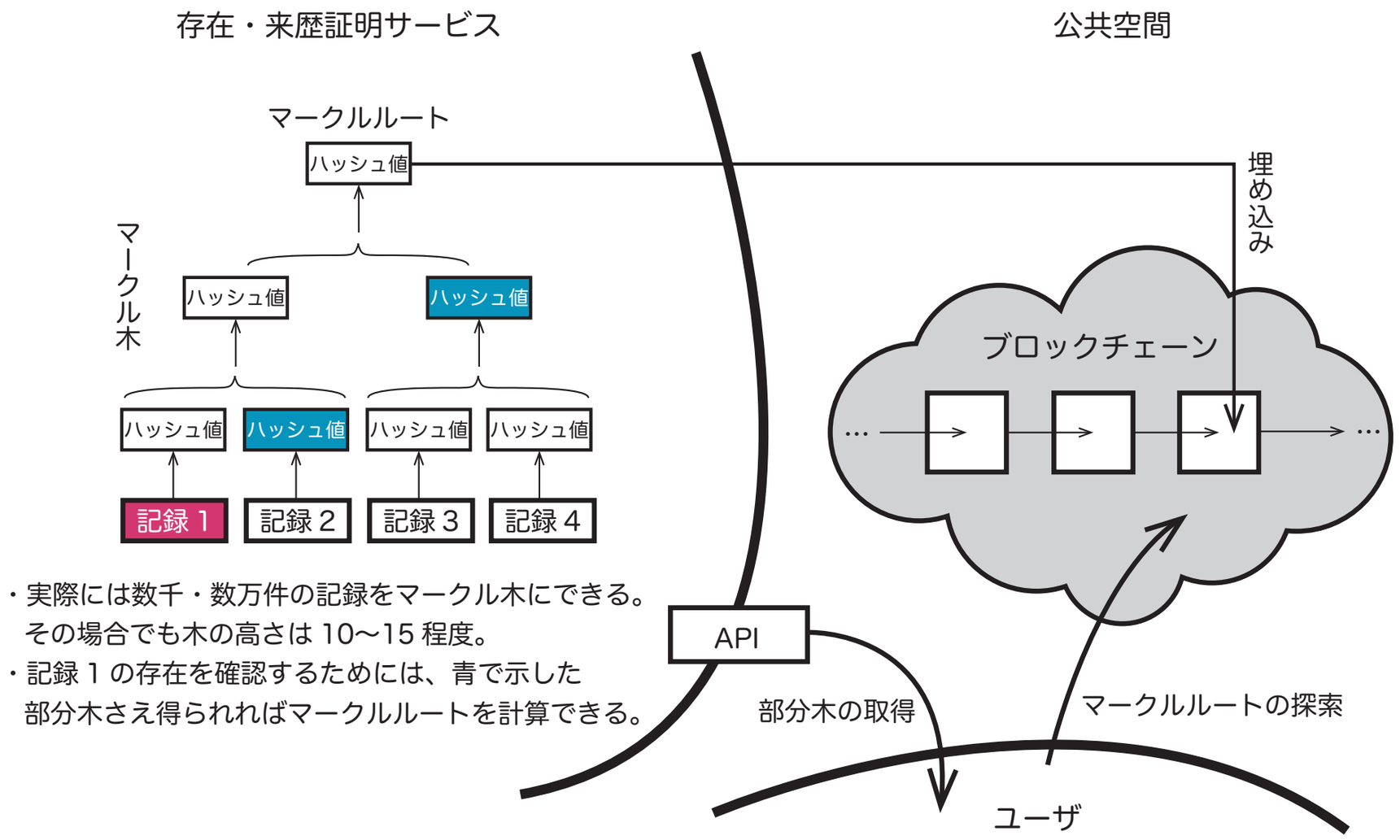
正当性の保証 – 識別子と公開鍵の分離

識別子を公開鍵のダイジェストとし、
公開鍵群との初期対応づけを行う TX は
識別子とペアとなる秘密鍵で署名されて
いなければならないことにする。



- 秘密鍵が失われたらアセットのコントロールを失う、という事態を避けるため、識別子と公開鍵は分離する必要がある
- 識別子と公開鍵の対応づけはアプリケーションに任されており、上はその方法の一例 (bbc1-lib-std で提供)

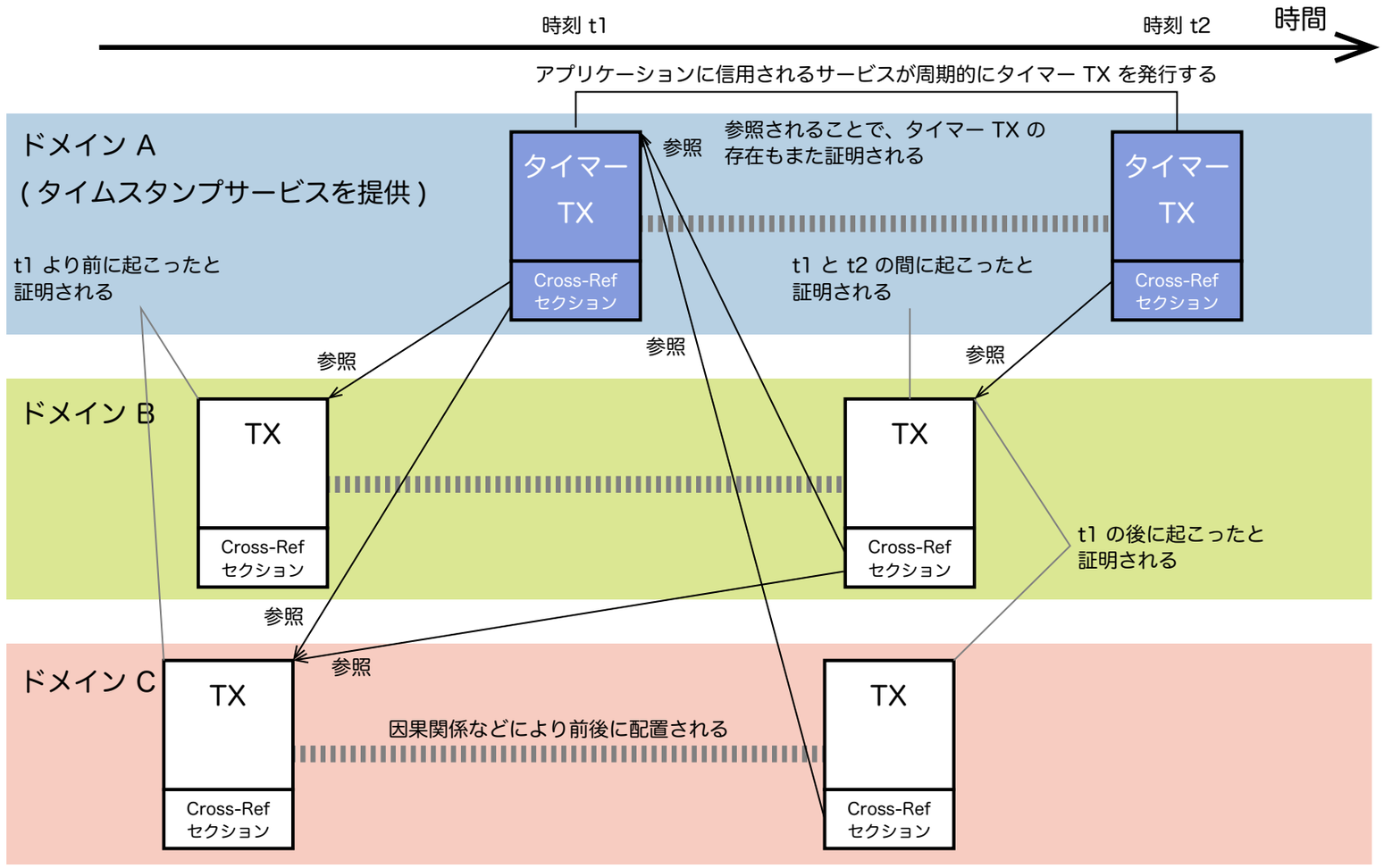
存在性の証明 – アンカリング



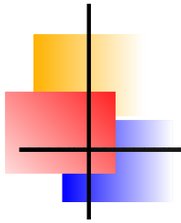
・実際には数千・数万件の記録をマークル木にできる。
その場合でも木の高さは 10〜15 程度。
・記録 1 の存在を確認するためには、青で示した
部分木さえ得られればマークルルートを計算できる。

- コンテキスト証明が実働するまでの間、レッジャーサブシステムにより提供

存在性の証明 – コンテキスト証明



- タイムスタンプサービスは無くてもよい (相対時刻を互いに証明する)
- 「参照」は < 相手ドメイン ID, 相手トランザクション ID or ハッシュ木ルート > を格納すること



唯一性の合意

- アセットには、通常の設計では債務者や責任者が存在する
- 移転が二重に起こる (二重消費; double spending) 場合に不利益を被るのは
  その債務者/責任者
- 従って、移転や状態操作一般に債務者/責任者の署名を要するように
  アプリケーションを構成する

- 債務者/責任者が単一故障点 (single point of failure) になるのを避けるため、
  必要ならば複製と分散合意 (Paxos 系) を行う
  - 識別子と公開鍵は分離されているため、複製は個々に鍵ペアを持てる

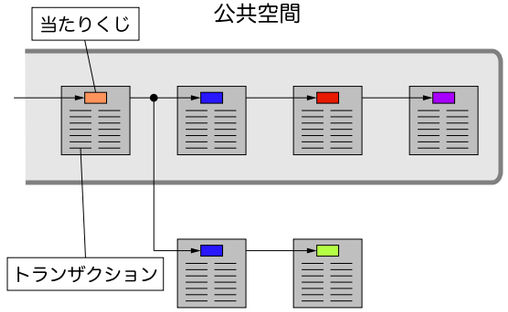
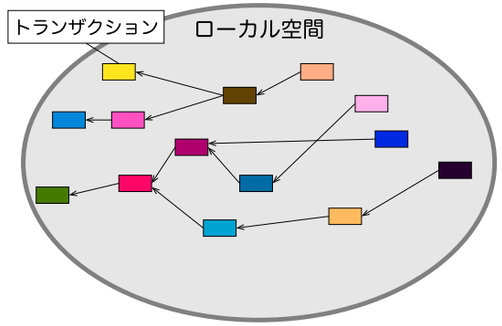
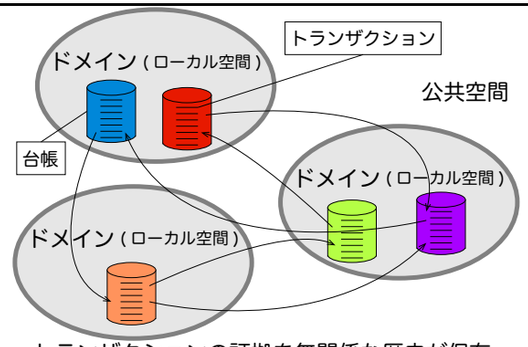
課題は解けたかどうかをふりかえる

- BBc-1 での課題解決のアプローチ
- ブロックチェーン/台帳技術の比較
- PoW/(D)PoS と PoCX (コンテキスト証明) の比較
- PoCX / BBc-1 に関する FAQ
- これまでの応用事例 (実証実験・研究開発)

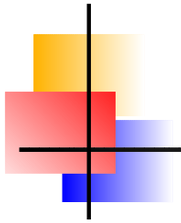
BBc-1 での課題解決のアプローチ

- 非実時間性 (確率的動作)
  ⇒ トランザクションのコミットまでに確率的動作が入らない
- 秘匿の困難性 (万人への検証可能性の担保)
  ⇒ ドメイン外へはトランザクションの内容を秘匿、内側でも暗号化可
- ワンネス (分散 vs. 複製)
  - スケーラビリティがない (全参加者に複製されるならスケールしない)
    ⇒ ドメイン単位でスケールアウト、ドメイン内も将来的に DHT
  - 進化のガバナンスが困難 (全員が一丸となる必要があるなら変われない)
    ⇒ ドメインごとの自治 (ドメイン内プロトコルは関知しない)
- 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)
    ⇒ ネイティブ通貨は持たず、コンテキスト証明は互助的に動作

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	(買収可能な) 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



PoW/(D)PoS と PoCX (コンテキスト証明) の比較

- PoW (Proof of Work; 作業証明)
  - 数学的くじ引きのコストを払わなければ書き込めない/改変できない (電力コスト大)
  - ナカモトコンセンサスを要する (不完全かつ実時間と同期しない)
- (D)PoS ((Delegated) Proof of Stake; (代表者) 持ち分証明)
  - 仮想通貨の持ち分の大きさに応じた投票権で投票して正史を決める
  - 囚人のジレンマ問題 (買収に弱い？)

$\Rightarrow$ いずれも仮想通貨のコストで防御 (価格低下 $\rightarrow$ 停止 / 通貨総額を上回る価値を守れない)

- 仮想通貨の価格変動にシステムの安全性が左右される

- PoCX (Proof of Context; コンテキスト証明) (研究中) (「履歴交差」を応用)
  - ランダムに選択されるドメイン間でトランザクションの証拠 (ダイジェスト) を無関係なコンテキストの中に埋め込み、検索可能とすることで、外部からの検証可能性を担保する
  - 書き込みが安価、アプリケーションの自律性を担保、検証コストは要評価

PoCX / BBc-1 に関する FAQ

- 必要なノード数は？
  - ドメインが分散していることが重要で、個々の台帳システムは可用性上の要求にもとづいて冗長化されていれば OK
- 従来の RDBS からの移行は？
  - 既存の DB に、検証可能なトランザクションシステムをアドオンするという考え方もアリ
- クライアント/サーバ方式と比較してどう？
  - クライアント/サーバ方式なのだが応答の真正性を検証可能、といった話です (P2P でなくて可)
- 情報の秘匿性は？
  - PoCX を用いる際も含め、トランザクションの内容はドメイン外に対して秘匿されます
  - ドメイン内でも適宜暗号化は可
  - 個人情報保護も、全体が維持する同一のストレージ等は無いのでやりやすいはず
- 参加のインセンティブは？
  - PoCX を利用したいドメインが参加し、コストを分かち合います (ネイティブ通貨を持たない)

これまでの応用事例 (実証実験・研究開発)

事例	実施主体
サービス履歴活用プラットフォーム	(株) デンソー ＋ (株) ブロックチェーンハブ
宇宙ゴミ除去目的の減価する通貨	九州大学 ＋ 慶應義塾大学 SFC 研究所 ＋ MUSCAT スペース・エンジニアリング (株)
地域通貨を用いた「社会課題解決」学習の支援	(株) アイネス総合研究所 ＋ (株) ブロックチェーンハブ
センサー情報への課金システム	横河電機 (株) ＋ (株) ブロックチェーンハブ
中小企業向けインボイスファイナンス	(株) ブロックチェーンハブ
資格証明	(株) ブロックチェーンハブ
独自通貨・ポイントシステム	(株) ゼタント
暗号鍵管理・共有プラットフォーム	(株) ゼタント

- どれも他のプラットフォームで実現できないわけではないが、BBc-1 では開発しやすい

おわりに

- ブロックチェーンの真価を発揮するために、ブロックチェーンの設計を捨てて BBc-1 を設計しています
- 現在、コアの設計は version 1.2 で、引き続き洗練させていく他、
  ライブラリの充実化やサンプルアプリケーションの拡充を行っていきます