ブロックチェーン技術とビヨンドブロックチェーン

～ Introduction to BBc-1～

一般社団法人ビヨンドブロックチェーン 代表理事　斉藤 賢爾

ブロックチェーンの技術的・技術ガバナンス的課題

ブロックチェーンは何をしたい技術か

- 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
  - (否定 = 改ざん・抹消・捏造)
- 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
  - 「誰にも/誰でも」 = 定義されたステークホルダーのうち「誰にも/誰でも」

⇒ あたかも「空中に記録を固定」できる
- 特定の誰かによって支えられるのではなく、
- 内部者によっても記録を否定できない

- そのことは本当にできていますか？

ブロックチェーン/分散台帳の現状

- ブロックチェーン
  - Bitcoin (ザ・ブロックチェーン + OAP: Open Assets Protocol)
  - Ethereum (アプリケーション基盤)/ EEA: Enterprise Ethereum Alliance

- その他の分散台帳技術 (DLT: Distributed Ledger Technology)
  - Hyperledger (Linux Foundation)
    - Fabric (IBM/DAH), Sawtooth (Intel), Iroha (ソラミツ) などの開発が進行中
  - Corda (R3), Tangle (IOTA), …, BBc-1 (私たち)

- ビットコイン(にも問題があるとして)以外の応用は正しく設計されているのだろうか

ブロックチェーン/分散台帳の基本的な構造

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

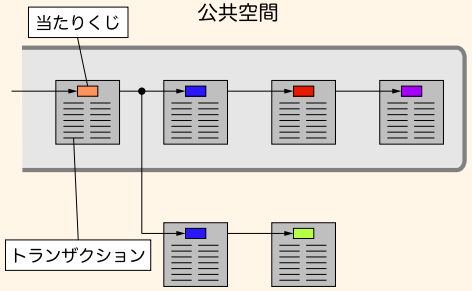
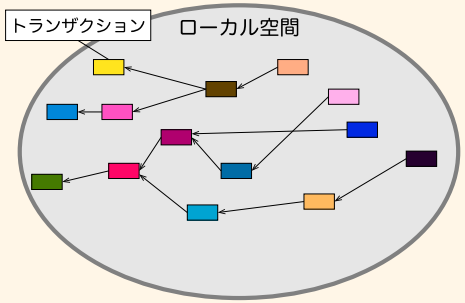
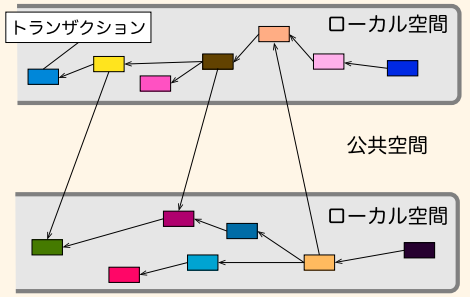
・過去にあったトランザクションの証拠を抹消できず、
・かつ、過去になかったトランザクションの証拠を捏造できない

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

ブロックチェーン/分散台帳の技術

beyond-blockchain.org

プラットフォーム	ブロックチェーン	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	文献モデル (ハイブリッド)
存在性の証明の方法	作業証明 (コストで守る)	ない (内部無矛盾性)	履歴交差 (外部性で守る)
唯一性の合意の方法	ナカモト・コンセンサス	第三者の集合の合意	関係者(特に責任者)の合意
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合意に舵を切ろうとしている
  - それも (市場原理的) (民主的) 新聞モデルであり、コストで守ろうとしていることには変わらない

ブロックチェーン/分散台帳の課題

- 非実時間性 (確率的動作)
- 秘匿の困難性 (万人への検証可能性の担保)
- ワンネス (分散 vs. 複製)
  - スケーラビリティがない (全参加者に複製するならスケールしない)
  - 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)
- インセンティブ不整合性
  - ネイティブ通貨の市場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)
- その解決 (プライベート DLT 一般) はそもそもの機能を満たすか
  - 改ざんは困難なのか

改ざんは防げるか

- ソフトウェアシステムではデータの改変自体は可能
  - 検知できるか、いつ検知するかという問題
- 従来のデータベースはアクセス制御で守っていた
  - ジャーナル (ログ) による検知に留まる
- データ同士を関連づけ、単純な改変では矛盾が生じるという考え方
  - 矛盾が残っていれば検知できる
  - 矛盾が残らないように改変されると検知できない

改ざんは検知できるか、いつ検知するか

プラットフォーム	無矛盾に改変するコスト C	扱う価値 V	抑制条件 C ≧ V	積極的検知
Bitcoin (基本)	マイニングのコスト	bitcoin	成立 (コストと価格が均衡)	してない
Bitcoin (応用)		応用次第	不成立になりうる	
Ethereum	マイニングのコスト	応用次第	不成立になりうる	してない
プライベート DLT 一般	見積もりにくい (比較的小)	応用次第	一般に不成立	してない？
BBc-1 (履歴交差)	見積もりにくい (極大)	応用次第	一般に成立	する

- 抑制条件 C ≧ V が不成立なら、合理的理由により無矛盾に改変され検知不可能になりうる
- 部分的な改変を積極的に検知するか？
  - 部分的に改変されると、正しい情報の取得に失敗する恐れがある
  - ただしブロックチェーンでは、全体と矛盾するトランザクションは投入できない
  - 一般の DLT では、検証・承認者 (の過半) に侵入される恐れを無視できないなら積極的検知した方がよい

BBc-1 はブロックチェーンの課題を解決しつつ、内部者による改ざんも検知可能にし、かつ、システム上の「合意」を現実社会のそれと一致させる

ブロックチェーンでできるとされていることを、本当に。

BBc-1 の活用：開発中案件事例

beyond-blockchain.org

事例	実施主体
サービス履歴活用プラットフォーム	㈱デンソー　＋　㈱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㈱
地域通貨を用いた「社会課題解決」学習の支援	㈱アイネス総合研究所　＋　㈱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㈱　＋　㈱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	㈱ブロックチェーンハブ
資格証明	㈱ブロックチェーンハブ
独自通貨・ポイントシステム	㈱ゼタント
暗号鍵管理・共有プラットフォーム	㈱ゼタント