beyond-blockchain.org

BBc トラスト

ビヨンドブロックチェーン 憲章

斉藤 賢爾, 久保 健

2017-10-31

{ks91|t-kubo}@beyond-blockchain.org

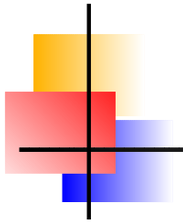
0. 用語の定義

アクター	デジタル署名できる実在
アセット	デジタルに表現される記録・資産
コミット	システムへのトランザクションの投入 (不可逆)
ストレージ	アセットを保存する分散システム
データ	トランザクションとアセットの総称
トランザクション	アセットの状態を変化させる事象
ユーザ	参加主体であり、複数のアクターから構成されうる
レッジャー	トランザクションを保存し処理する分散システム

1. BBc トラストとは

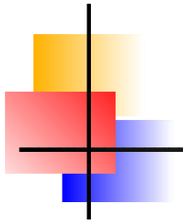
- BBc プロダクトのユーザが、このプロダクトについて何を信じられるかを定める憲章である

2. ビヨンドブロックチェーンは何でないか



2-1. データベースではない

- データが保存されていることを保証しない (ベストエフォート)
  - 保存される度合いに対して上限・下限の制限を設けない
- 保存されている場合は、暗号技術がコンプロマイズされない限りにおいて 3〜5 項に記述する「正しさ」を保証する
  - 一方、暗号技術が危殆化されることを前提に、技術の更新を可能にする
- BBc は必要に応じてデータベースを利用する

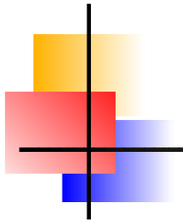


2-2. ブロックチェーンではない

- ブロックのチェーンではなく、以下の弱点を持たない
  - 実時間性の欠如 (物理プロセスと同期できない)
  - 秘匿性の欠如 (最近のブロックチェーンで挑戦は行われているが)
  - ワンネス (分断耐性・スケーラビリティ・アップデートの容易さの欠如)
  - インセンティブ不整合性 (ネイティブ通貨の死とともに死ぬ)
- BBc は必要に応じてブロックチェーンを利用する

2-3. 複製システムではない

- サービスの耐障害性が目的なのではない
  - 決定的に動作するトランザクションが複製されたサーバに同じ順序で届くような複製技術にもとづかない
  - コンセンサスを基調とするシステムではない
    - 特に、CUP (未知の参加者との合意問題) を解こうとしない
- BBc は必要に応じて複製技術を利用する



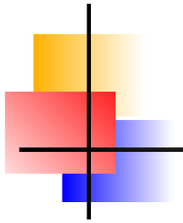
3. 正しさ — 正当性の保証

- トランザクションが改ざんできず、
- 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コミットされていることを保証する

- また、正当なユーザによるコミットは他の何人によっても止められない

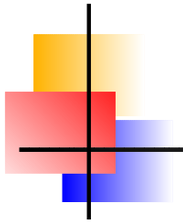
4. 正しさ — 存在の証明

- 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



5. 正しさ — 唯一性の合意

- 矛盾するふたつのトランザクションがコミットされた場合、そのどちらも正しい
- そのことが実際に起きることによる不利益を被らないように、
  当該トランザクションが扱うアセットに責任をもつ正当なユーザに、
  どのトランザクションをコミットするかについての選択権がある
  - ユーザが複数のアクターから成る場合はその間のコンセンサスの機構を提供する



6. ポリシーとその他の要求

- 前項までの「正しさ」を維持すべく、システムは次の性質をもつ
  - レッジャー自体はフリーで提供する
  - 適切に動的にスケールできる
  - 許可なく新しい技術を試験してアップデートできる
  - 参加のインセンティブが適切であり、システムとアプリケーションの持続性に対して整合的である