2019年度未踏ターゲット事業

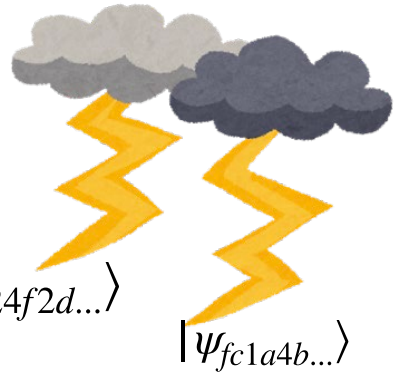
量子情報技術による分散型通貨決済システムの開発

ー　量子マネーを分散管理するプロトコルの提案　ー

桝本尚之（フリーランス）

・　「信頼できる中央銀行」が存在しない分散環境でも量子マネーを決済できるシステムを作りたい
・ なぜ？
  - 現在の暗号資産は計算量を消費しすぎる
  - 量子情報技術でなんとかできないか？
・ 採用したアプローチ
  - 量子マネーを分散環境で管理する

・量子マネーとは
  - 量子状態を長期間保存できるデバイスや量子コンピュータが普及した世界で使用可能な決済システム
  - 量子状態（=量子ビット）を貨幣として使用するアイデア
  - 「ノー・クローニング定理」 により貨幣の複製が困難
    - ノー・クローニング定理 = 任意の未知の量子状態は複製することが不可能



・「Quantum Lightning」という電子マネーは分散化に向いている
  - 量子マネーを作った者でさえ同一の量子マネーを作ることは不可能
  - 構成
    - $(Gen, Ver, H) \leftarrow QL.Setup$：各アルゴリズムとハッシュ関数の用意
    - $|\psi\rangle \leftarrow Gen$：量子マネーの生成アルゴリズム
    - $Ver(|\psi\rangle) = s \mid \perp$：量子マネーの検証アルゴリズム。sは量子マネーのシリアルナンバー。
    - 量子マネーとハッシュ関数Hは以下の性質を満たす。
      - $|\psi\rangle \propto \sum_{\{x|H(x)=s\}} |x\rangle$

·新提案の構成
- 量子マネー（quantum lightning）
- 分散台帳
  - 量子マネーのシリアルナンバーと価値を紐付ける共有テーブル
  - 両替コミット・メッセージ
  - 両替実行メッセージ

·新提案のプロトコル
- 基本的な量子マネーの支払い方法 = 直接渡す
  - 量子マネーの受け取り側が検証アルゴリズムで知ったシリアルナンバーを共有テーブルから引くことで価値を知ることができる
- 両替プロトコル(図1)
  - 望みの額を作るために手元の量子マネーを崩すことができる
  - ハッシュ関数Hの原像であるxを測定することで量子マネーの所有権を確かめられる
  - 両替コミット・メッセージをネットワークにブロードキャストする
    - 一定時間経ったあとに出される両替実行メッセージで共有テーブルを更新
- 分散台帳の更新（図2）
  - 全両替コミット・メッセージの検証に対して報酬を与える
  - (共有テーブル+両替コミットメッセージ+新量子マネーのシリアルナンバー)のハッシュ値に上限値を設ける
    - 新量子マネーのシリアルナンバーはビットコインのnonceに相当
    - 制限突破する量子マネーが見つかるまで作り続ける=マイニング

·解決する課題
- ブロックチェーンの使用率を下げることで時間/空間的計算量を節約
- 量子コンピュータ耐性のない古典暗号を使わないため安全

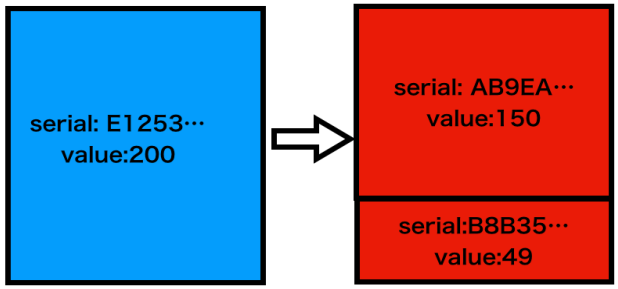


図1 両替

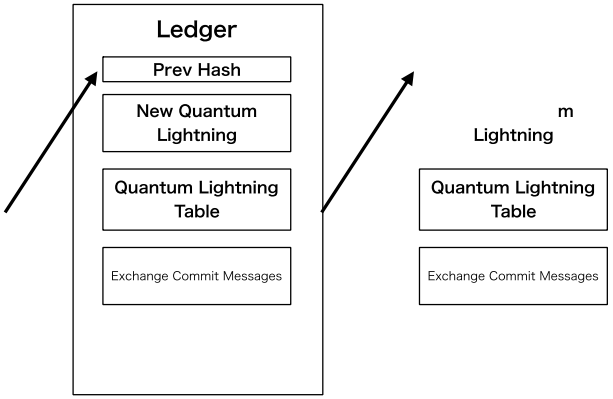


図2 分散台帳