分散環境における
量子マネー決済システム

桝本　尚之

未踏ターゲット事業成果報告会

本プロジェクトの目的

- 「分散環境」において機能する「量子マネー決済プロトコル」を開発する
  - 分散環境とは
    - 信頼できる中央銀行が存在しない環境（=非中央集権的）
      - それでも貨幣の希少性は保たれる設計（=参加者が勝手に貨幣を作れない）
    - 例) 仮想通貨（ビットコインなど）
  - 量子マネーとは 👉

量子マネーとは（1）

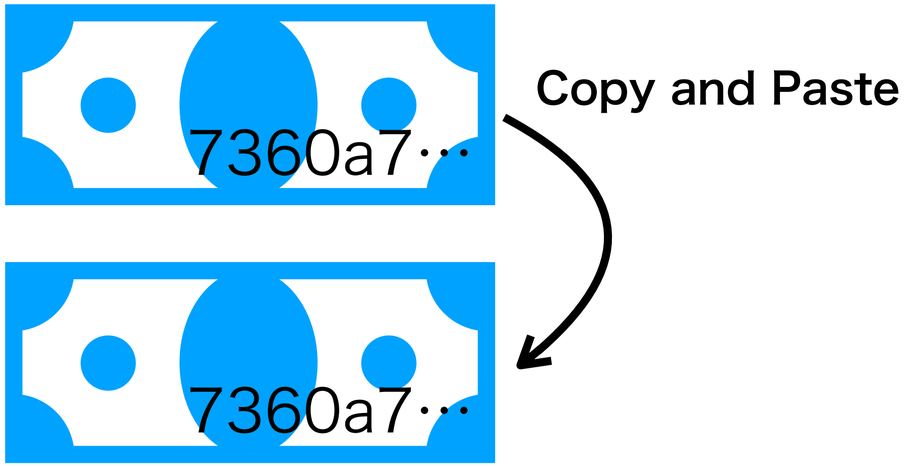
- 「量子状態」（複数量子ビット）そのものを通貨として利用するアイデア（1969 ~ ）
- 「任意の未知の量子状態は複製不可能である」（ノー・クローニング定理）
  = 通貨を偽造することは不可能
- 物理学的制約で通貨の価値を担保する

Stephen Wiesner, in SIGACT News, Vol. 15, 1 (ACM, 1983), pp. 78-88.

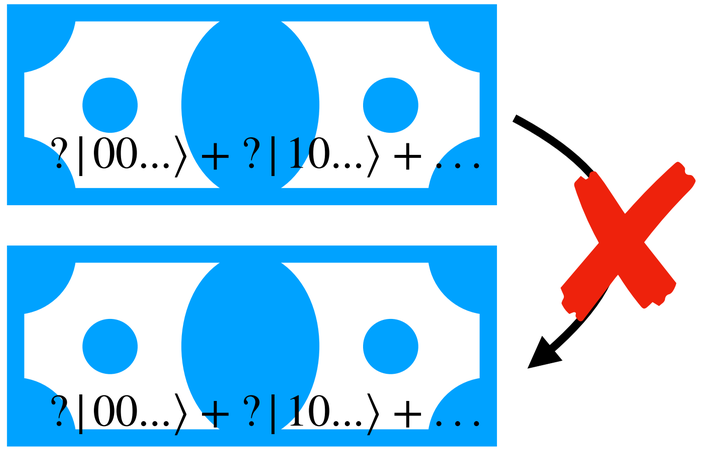
量子マネーとは（2）

- ノー・クローニング定理(No-cloning theorem, 量子複製不可能定理)
  - 任意の未知の量子状態を複製することはできない
- 例
  - $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ という量子状態のみが与えられたとき、αとβ を知らないで$|\psi\rangle$を複製することはできない

古典



量子



量子マネーとは（3）

- どういう世界で使えるの？
  - 量子コンピュータが広く普及している世界
  - 量子状態を送受信できるネットワークが存在する

量子マネーとは（4）

- どのような量子アルゴリズムが必要？
  - $|\psi\rangle \leftarrow Gen(1^\lambda)$
    - 量子マネーを「鋳造」するアルゴリズム
  - $Ver(|\psi\rangle) = accept|reject$
    - 量子マネーが確かに中央銀行によって鋳造されたか「検証」するアルゴリズム
    - 量子マネーの量子状態は損なわない
- GenとVerを中央銀行が秘匿管理する → **Private-key quantum money**
  - 量子マネーを中央銀行まで持っていって通貨を検証する（中央銀行だけが量子マネーの量子状態を知っている）
- Verを公開する → **Public-key quantum money**
  - Verを使えば誰でも量子マネーを検証できる　→ 分散環境に向いている!

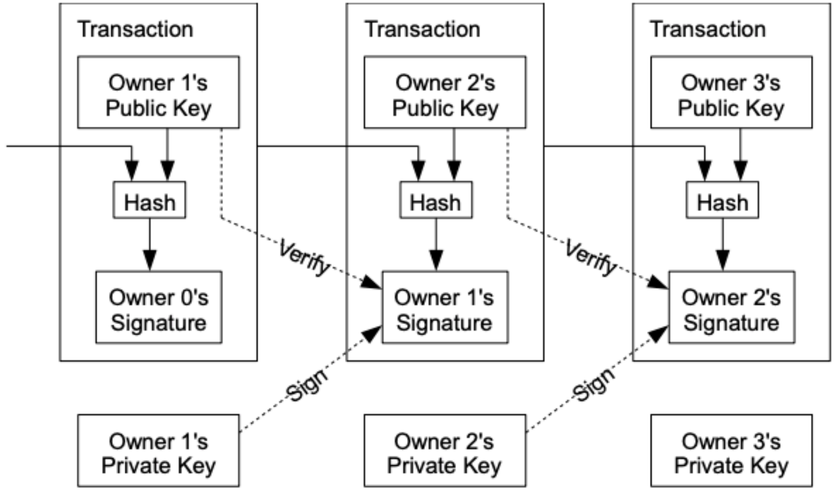
量子マネーを分散環境で管理すると
何が嬉しいの？

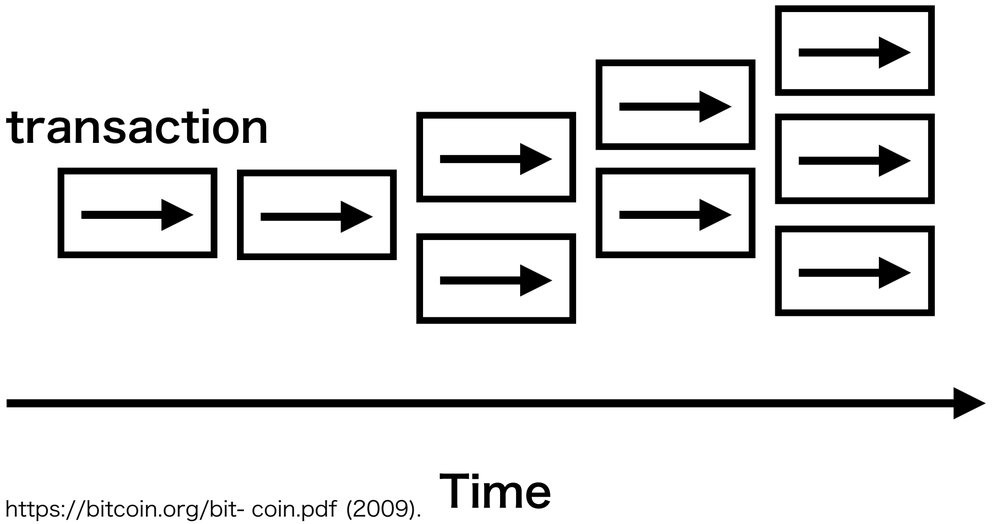
- 現在の(古典暗号を使った)仮想通貨は、決済に計算量を使いすぎる
  - 空間的計算量
    - すべての取引（transaction）の履歴を保存する必要
  - 時間的計算量
    - ブロックの承認に膨大なハッシュ計算が必要
- 量子技術を使ってブロックチェーンを効率化できるのでは

- …そもそも仮想通貨/ブロックチェーンとは👉

仮想通貨とは（1）

- 貨幣の価値を担保する中央銀行が存在しない環境で「価値のやり取り」をすることが目的
- アドレスからアドレスへの価値の移動（transaction）の総体
  - アドレスは公開鍵。秘密鍵を知るものだけがtransactionを作成することが可能
  - transactionは生成後、ネットワーク内にブロードキャストされる

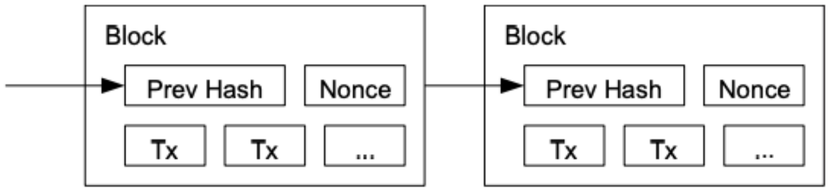




Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bit- coin.pdf (2009).

仮想通貨とは（２）

- transactionは誰でも作れるので検証する必要がある
    - 1つのアドレスから複数のアドレスに価値の移管が行われていないか（二重払い）
- 一定時間（ビットコインの場合は10分）にブロードキャストされたtransactionを全て検証して、問題がなければ「ブロック」として確定させ、前回のブロックにつなげる
    - ブロックの時間方向への連鎖 = ブロックチェーン
- 検証する参加者は誰が検証するのか？
    - 計算量を持っているものに任せればよい。計算量が悪意のある勢力に寡占されることはないだろうから。
        - nonceを含んだブロックのハッシュ値を特定の値以下に制限する
        - 制限を突破するハッシュ値を出力するnonceを計算させる
            - nonceの発見者には一定額の仮想通貨を付与する（報酬）

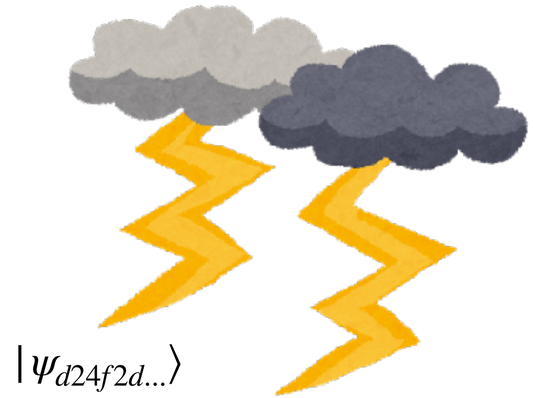


新提案

- ブロックチェーンで量子マネーの分散管理を行う
- 量子マネーはpublic-key quantum moneyの一つである「quantum lightning」を用いる
  - →これを分散化する！
- 量子マネーをその価値のまま送るときは、直接渡す、もしくは量子ネットワークを通じて量子マネー自体を送信する
- 量子マネーの両替時のみブロックチェーンを使うことにより、古典ブロックチェーンより効率は向上する
- 量子コンピュータ攻撃に耐性のない暗号技術は使わない（公開鍵暗号など）

Quantum Lightning

- Public-key quantum moneyの１つ
- Ver(検証用アルゴリズム)だけではなくGen(鋳造アルゴリズム)も公開する
  - = 誰もが通貨を発行し、検証することが可能
- 量子マネーの状態記述 : $|\psi\rangle = \sum_{\{x|f(x)=s\}} |x\rangle$
  - sは通貨のシリアルナンバー;fは一方向ハッシュ関数
  - 複数量子ビットの全重ね合わせ状態からsを測定すると、$f(x) = s$となるxの重ね合わせのみが残る
    - 量子力学的ランダム性からsが決まるので同じsを持つ量子マネーを作ることは**作成者さえも(!)**不可能
- $Ver(|\psi\rangle) = s|reject$
  - 検証アルゴリズムを通すとシリアルナンバーが出力される。同じ量子マネーからは常に同じシリアルナンバーが出力



雷は同じ場所に二度と落ちない

“Quantum Lightning Never Strikes the Same State Twice” Mark Zhandry, in Proceedings of EUROCRYPT 2019, (2019).

共有テーブル

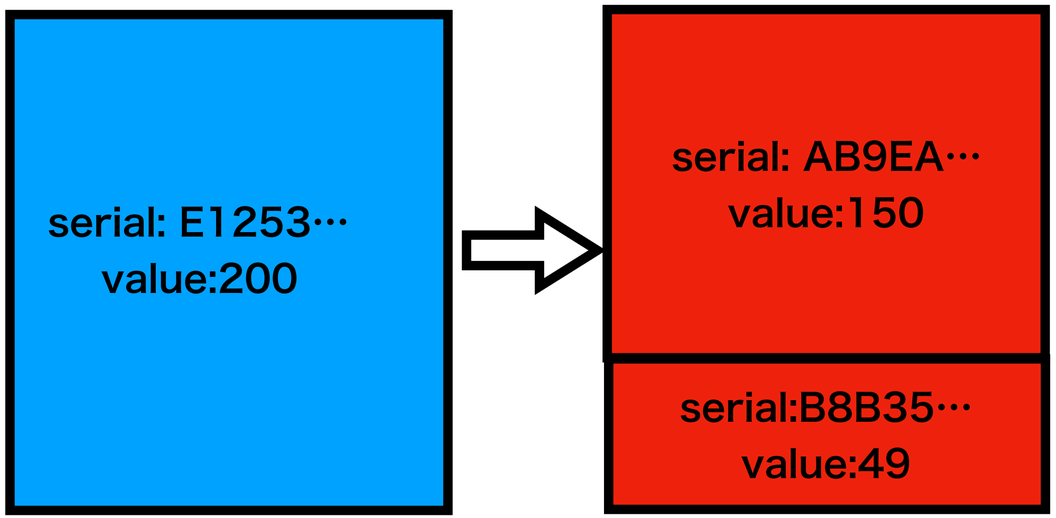
- Quantum Lightningのシリアルナンバーと価値をその時点での共有テーブル（分散台帳にある）で保存

- 量子マネーを受け取ったら、Verを使って得たシリアルナンバーを共有テーブルから引けば価値が分かる

Serial number	Value
76EE9D30B604E492	11.204907940931
F1061B0552B5E95F	46.0735188743681
DF21419C59325BF7	39.5127205724947
379A31782DC6C73D	34.7546510008965

両替プロトコル（1）

- 支払い額に端数が出る場合には、量子マネーを「崩す」事が必要
  - このとき、共有テーブルの「書き換え」が必要になる = 登録された量子マネーのsを消し、鋳造した量子マネーのsを登録する
  - 両替要求の適用にブロックチェーンを使用し、分散合意をとる
    - ビットコインのトランザクションと同じく手数料をとる（直接、量子マネーを送るときには必要ない=できるだけ直接送って欲しい）
    - 1つの量子マネーを2つの量子マネーに崩す両替要求しか許さないため、ビットコインのトランザクションに比べサイズが小さくてすむ
- 量子マネーの分割ではなく、結合は量子ネットワーク全体の負荷を下げるため、手数料を徴収しない

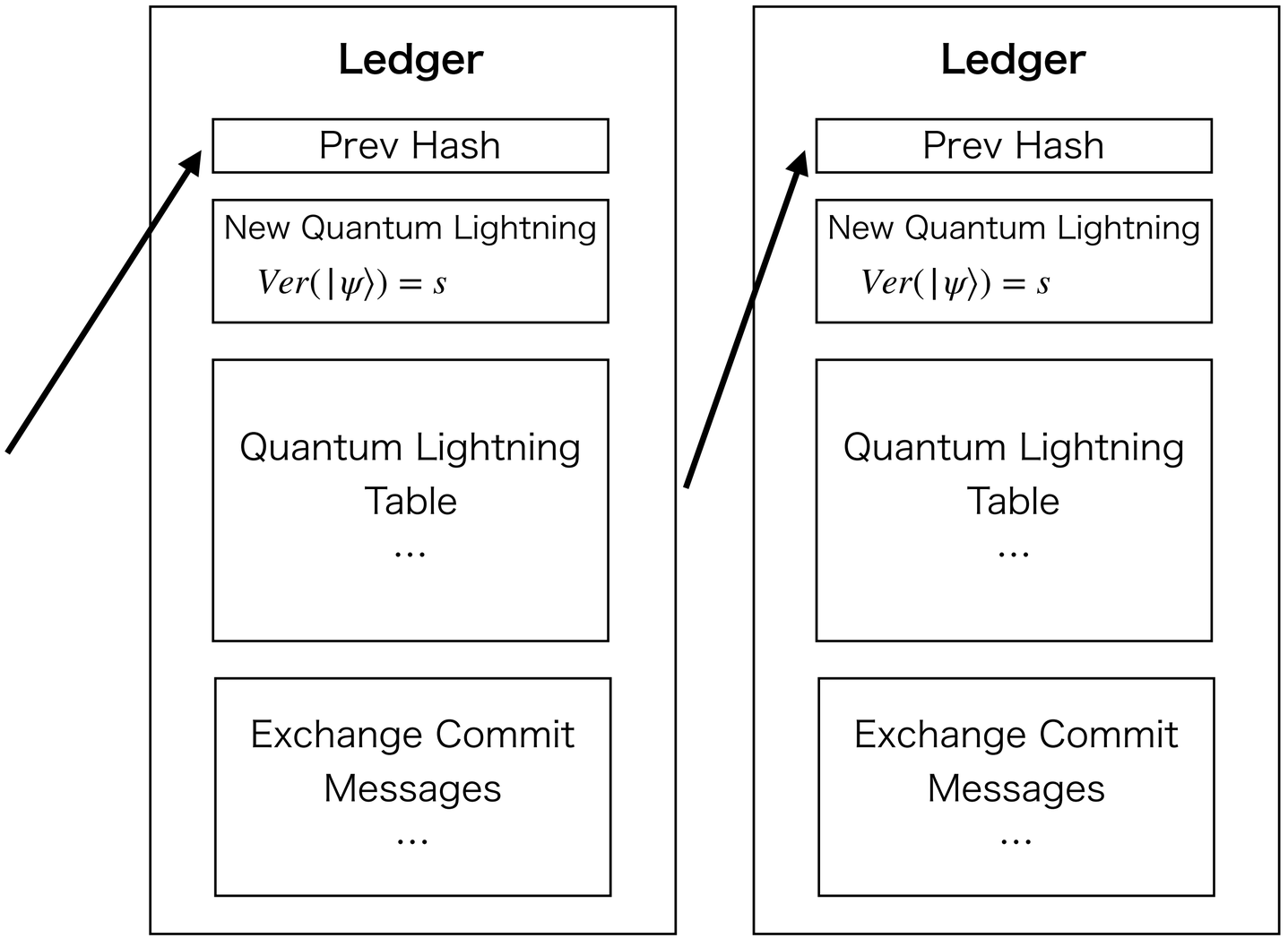


両替プロトコル（2）

- 両替を要求するメッセージをネットワーク内に流す
  - Exchange commit message
    - あくまでcommitするだけのメッセージ。実際に共有テーブルに反映させるには分散合意が必要。
    - 分散台帳に取り込まれる
  - $f(x) = s$ となるxの１つを書くことで両替前の量子マネーの所有者であることを証明
    - xを測定するとき、$|\psi\rangle = \sum_{\{x_i | f(x_i)=s\}} |x_i\rangle$ は $|x_i\rangle$に収束してしまい、$|\psi\rangle$は量子マネーとしては機能しなくなる
  - One time pad による暗号化が必要
    - メッセージは誰にでも見れるため x を知った参加者が両替後の量子マネーを自分が作った量子マネーに書き換えてしまう可能性がある
    - Exchange commit messageが分散台帳に取り込まれたあとに、Exchange open messageで鍵を送り復号する

分散台帳の書き換え

- 分散台帳更新の歴史
  - = ブロックチェーン
  - 仮想通貨におけるブロック=分散台帳
- 両替要求は検証が必要
  - 前の分散台帳にある両替要求を復号化して検証し分散台帳を更新する
- 仮想通貨におけるnonceは検証者が鋳造した量子マネーのシリアルナンバーに置き換える
- 量子マネーを作成し続けて、条件を満たすものを探す
  - その量子マネーはそのまま報酬となる
  - 検証の報酬と両替要求手数料分を付与する



デモ

まとめ

- 量子マネーを分散環境で運用するプロトコルを提案した
- 使用する量子マネーは鋳造、検証が誰にでも可能なQuantum Lightningを用いる
- 量子マネーを直接送り合うときには、共有テーブルの参照のみで支払いが完了する
- 両替が可能なプロトコルを開発した
- ビットコインに比べ、両替時にしかブロックチェーンを使用しないので効率がいい
- ビットコインのトランザクションに比べ、両替要求そのもののサイズが小さい
- ビットコインのように公開鍵暗号を使わないので量子コンピュータ耐性がある

今後の展開

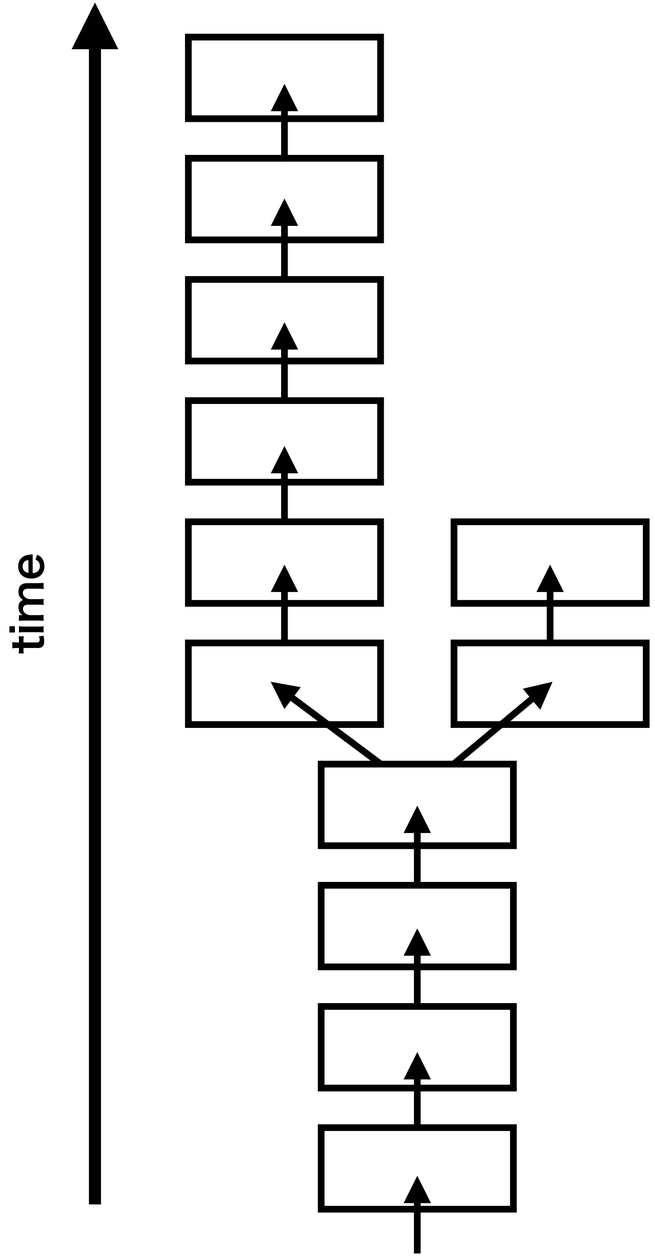
- ブロックチェーンの使用効率を定量化して検証する
- シミュレーションプログラムで実際に複数クライアントで機能するか検証する
- ブロックチェーンを使わない共有テーブル更新の方法を考える

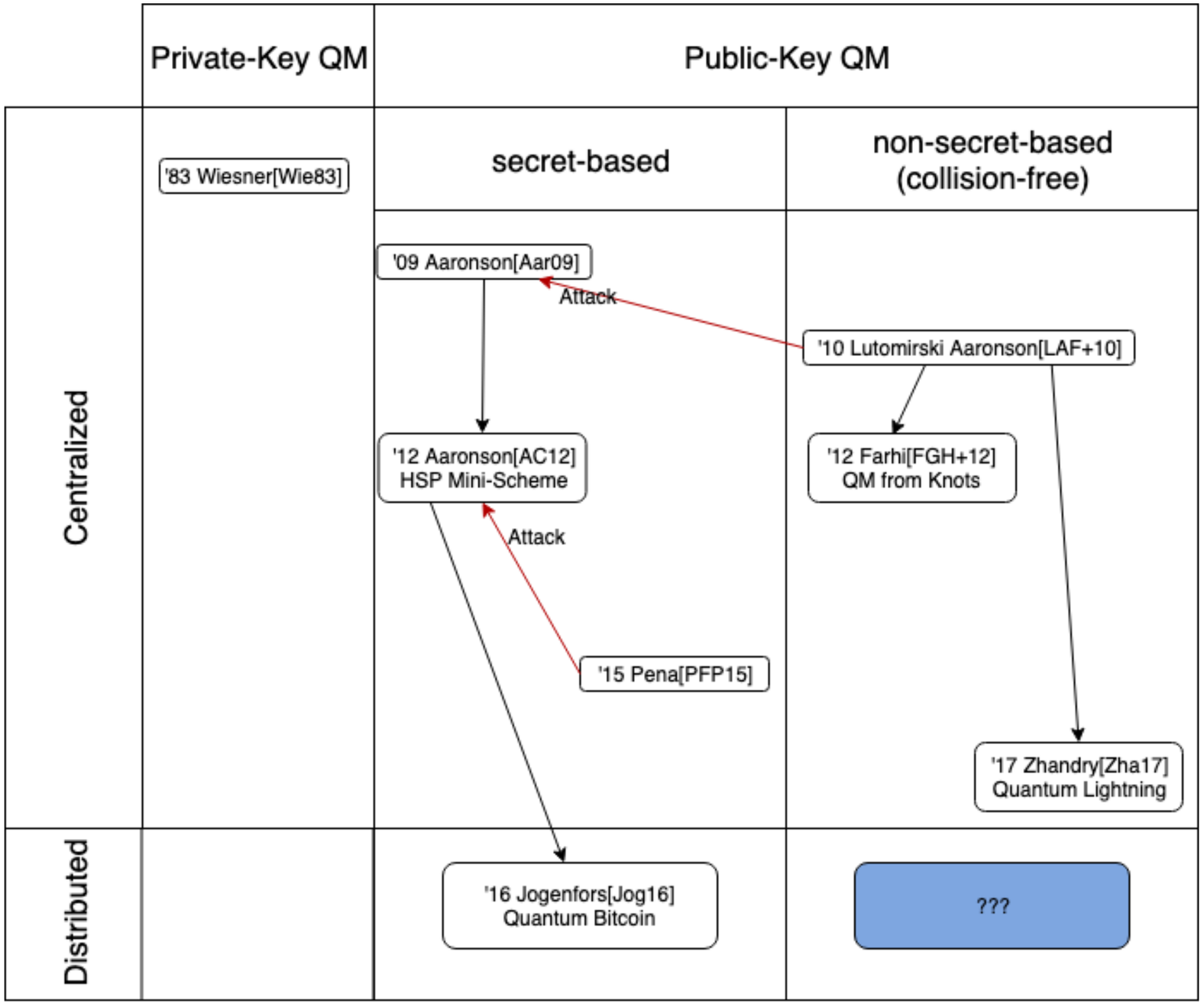
ご清聴

ありがとうございました

補足資料

- ブロック/分散台帳は分岐する可能性がある
- 「最も伸びているブランチを採用する」というルールを採用すれば、ネットワーク全体が合意するブランチは1つに収束する




Private-Key QM
Public-Key QM
Centralized
Distributed
'83 Wiesner[Wie83]
secret-based
non-secret-based
(collision-free)
'09 Aaronson[Aar09]
Attack
'10 Lutomirski Aaronson[LAF+10]
'12 Aaronson[AC12]
HSP Mini-Scheme
'12 Farhi[FGH+12]
QM from Knots
Attack
'15 Pena[PFP15]
'17 Zhandry[Zha17]
Quantum Lightning
'16 Jogenfors[Jog16]
Quantum Bitcoin
???