量子情報技術による分散型通貨決済システムの開発
― 量子マネーを分散管理するプロトコルの提案 ―

1. 背景

信頼できる中央銀行が存在しない環境において通貨の総量管理や受け渡しが不正なく行われるシステムは、現在、古典暗号を用いて提案、実装されている。暗号資産という呼称で呼ばれるようになったこの新種の通貨は、現在、世界的に流通、取引されている。しかしその一方で、分散環境での不正を防ぐために、偏ることなく世界中に行き渡っているはずの計算力を用いたハッシュ計算と全期間にわたる全ての取引の検証という、莫大な時間的、空間的計算量の消費を伴っている。近年、各分野で広がりを見せている量子情報技術を用いてより効率的な決済システムを構築することはできないだろうか?

本プロジェクトでは、量子マネーを使ってこの問題の解決を試みたい。量子マネーとは量子状態そのものを貨幣として扱う技術で、量子情報研究の初期からその研究が行われてきた（[1]）。ノー・クローニング定理により未知の量子状態は複製することができないため、物理法則のレベルで偽造を防ぐことが可能であるのが、量子マネーの大きな特徴である。この性質は決済の検証の効率性に大きく資すると考えられる。

2. 目的

本プロジェクトの目的は、Mark Zhandryによって提案されたquantum lightning[2]という量子マネーをブロックチェーンによって分散管理することで、既存の暗号資産よりも安全で効率的な通貨決済システムを提案することである。public-key quantum moneyであるquantum lightningは誰もが量子マネーの検証が可能であり、また同一のシリアルナンバーを持つ量子マネーを作ることは作成者でも不可能であるという、この目的を達成する上での利点を持っている。非中央集権的な通貨決済が求める機能群をquantum lightningを用いて実現する仕組みを提案する。

3. 開発内容

本プロジェクトの目的である分散環境で管理可能な量子マネーを実現する新プロトコルの概略を説明する。量子マネー（量子状態）を十分長い期間にわたって保存できる量子メモリーと、任意の量子アルゴリズムが実行できる量子コンピュータが広く普及していることを技術的な前提とする。

[2]で提案されたquantum lightningは、量子マネーの生成プロトコル(Gen)、検証プロトコル(Ver)、ハッシュ関数(H)で構成される。ここに、古典ネットワークで共

有される全量子マネーのシリアルナンバーと額面の対応表（共有テーブル）と、それを更新するためのリクエスト・フォームとプロトコルを追加することで、本提案に必要な構成要素が揃う。

quantum lightning は以下の安全な量子アルゴリズムが存在すると仮定した上で成立する量子マネーである。ここでいう「安全」とは量子マネーを複製できる多項式時間量子アルゴリズムが存在しないという意味である。

$$(Gen, Ver, H) \leftarrow QL.Setup$$

$$|\psi\rangle \leftarrow Gen$$

$$Ver(|\psi\rangle) = s \mid \perp$$

$QL.Setup$はそれぞれ対応するGenとVerの量子アルゴリズム、関数Hを生成する機能を持つ。Genは実行するたびにランダムに異なる量子マネーを生成するアルゴリズムであり、実行者でさえも同一の量子マネーを発行することはできない。Verアルゴリズムは量子マネーを入力とし、その量子マネーのシリアルナンバー(s)もしくは量子マネーの却下（Genアルゴリズムにより生成された量子マネーではないとみなすこと）を出力とする検証アルゴリズムである。このアルゴリズムを使用することで入力の量子マネーの状態が破壊されることはない。量子マネーと関数Hは以下の性質を満たす。

$$|\psi\rangle \propto \sum_{\{x|H(x)=s\}} |x\rangle$$

関数Hは一方向関数でsからxを推測するのは困難であるとする。つまり、量子マネーは同じハッシュ値を持つ原像（を量子ビットにコーディングした状態）の重ね合わせ状態にあると言える。

本プロトコルにおいて、基本的な量子マネーの支払いは、直接的な受け渡し、もしくは量子ネットワークを通じた送信で行われる。量子マネーを受け取った側はVerによって判明するシリアルナンバーで共有テーブルを引き額面を知ることで、その価値を検証すればいい。

相手に支払いをするのに十分な量子マネーを持っていたとしても、支払いたい額とちょうど同額の量子マネーを用意出来ないことがある。そのときは、1 つの量子マネーを共有テーブルから消去し、同額の合計額を持つ 2 つの量子マネーを作る操作を行う必要がある。これを両替と呼ぶことにする。この操作により、任意の額面の量子マネーの支払いが可能となる。

図 1 に示される例で考えてみよう。例えば、150 単位の量子マネーを作りたいとする。まず、両替後に通用させる 2 つの量子マネーを自身で作成する。一方は目的とする 150 単位を、もう一方は残りの 50 単位を割り当てるための量子マネーである。

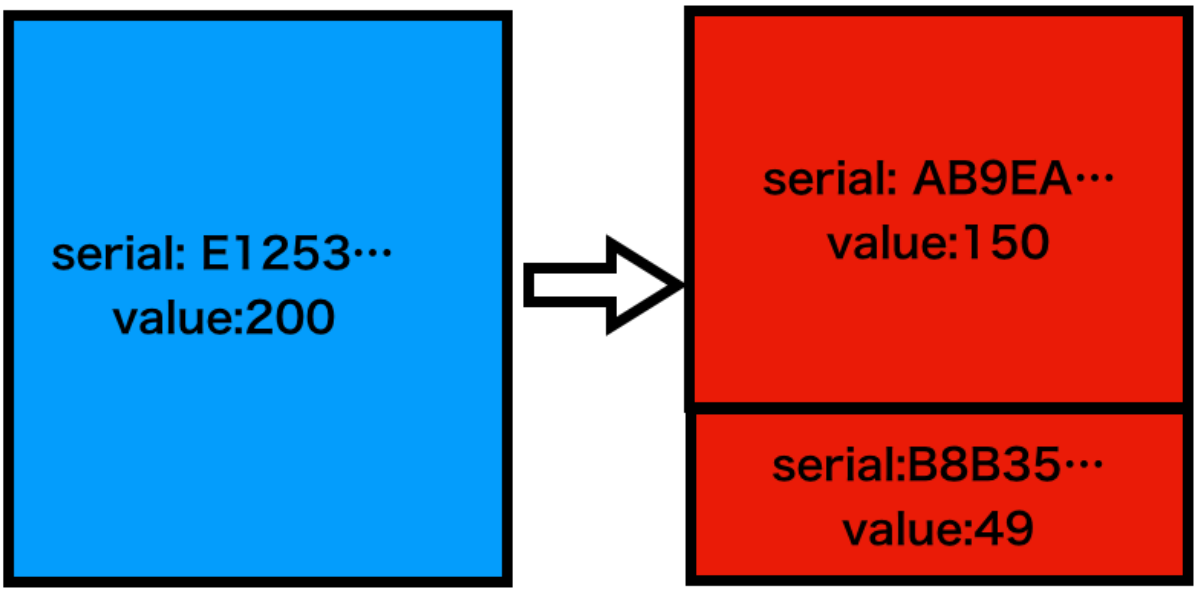

図 1　両替

ただし、両替の承認には分散環境において計算量が費やされるため、何らかのルールに基づいた手数料を課す必要がある。ここでは 1 単位を 50 単位の量子マネーから差し引くことにする。

逆に複数の量子マネーを 1 つの量子マネーに統合する両替には手数料を課さないことにする。これは量子マネーの統合が、ネットワークや計算量など、このシステム全体の負荷を下げることに寄与するためである。

一定時間以内の両替要求は両替要求者のみが知る秘密鍵によって暗号化した後、両替コミット・メッセージとしてネットワークにブロードキャストされる。両替コミット・メッセージは全世界に送信され、各量子コンピュータ・ノードでその正当性が検査される。ここで、ある時点での共有テーブルと両替要求に関わるメッセージ（後述）を合わせて分散台帳と呼ぶ。両替コミット・メッセージを検証し承認することで、次の時点（一定時間を経た後）の分散台帳が生成される。両替コミット・メッセージの検証に報酬を与えることで、分散台帳作成のモチベーションが確保される。

両替コミット・メッセージの検証は、両替要求者が一定時間後にネットワーク内にブロードキャストする両替実行メッセージを使って行われる。両替実行メッセージには、両替コミット・メッセージを復号する秘密鍵が含まれており、確かに両替コミット・メッセージが両替実行メッセージを出した者により作られたことが確かめられる。

ここで両替コミット・メッセージを秘匿しなければいけない理由は、両替コミット・メッセージが、確かに両替前の量子マネーの持ち主である者によって作られたことの証明となる値が入っているためである。その値とは量子マネーの原像であるxで、この値は量子マネーの持ち主の量子ビット測定で得られる（その過程で量子マネーは重ね合わせ状態ではなくなり、Verアルゴリズムで却下されることになる。両替が実行されるまでこの量子マネーの価値は宙に浮くことになる）。検証者は$H(x) = s$を確認

することで、確かに量子マネーの持ち主が両替コミット・メッセージを発行した事がわかる。

分散台帳は図 2 に示されるようにある時点での分散台帳は以下の構成要素を持つ。

- 直前の分散台帳のハッシュ値
- 分散台帳の検証者が追加する量子マネーのシリアルナンバー
- 共有テーブル
- 両替コミット・メッセージ群
- 両替実行メッセージ群

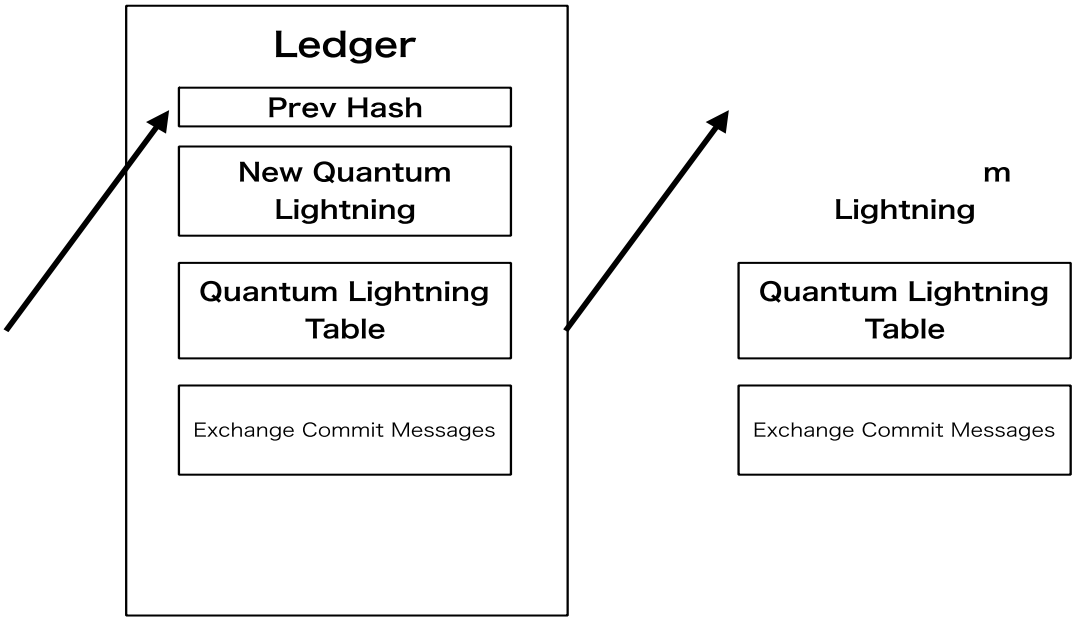

図 2　分散台帳

ここで、ビットコインのブロックチェーンの nonce のような役割に相当するのが quantum lightning におけるシリアルナンバーである。全量子マネーのシリアルナンバーと検証時に生成する量子マネーのシリアルナンバーを結合した値のハッシュに制限（特定の値よりも小さいことを求めるなど）を設けて特定の勢力が不正な分散台帳を作成することを防ぐ。制限を突破したシリアルナンバーをもつ量子マネーが見つかったならばそれをそのままこのブロックの報酬として分散台帳に書きこむことを認める。

分散台帳は直前の分散台帳を参照するため、チェーン構造を形成する。新しい分散台帳はネットワークから最も早く受け取ったものを採用するため、異なる分散台帳を双方ともネットワーク内で受け入れられ、別系統の分散台帳チェーンが形成される可能性がある。「分岐が形成されているときは、最も長いチェーンを正統として採用する」というルールを課しておくとこの問題は解消される。分岐後、後が続かなかったチェーンが伸びる可能性は減り、最終的に時系列の中で取り残されることになる。

4. 新規性・優位性

今回提案したプロトコルは、量子マネーの一種である public-key quantum money の特性を活かし、ブロックチェーンの安全性、効率性を上げるという点で新規性を持つ。量子マネーの直接のやりとりには分散台帳は使わず、両替時にのみ計算量を使用する本プロジェクトのプロトコルは、従来の暗号資産技術に比べ計算量で優位に立っている。また、量子コンピュータによる暗号解読がリスクとなる古典暗号も使っていないため安全性も高いと言える。

5. 期待されるユーザー価値と社会へのインパクト

古典的な公開鍵暗号を使った暗号資産が実用化され世界中でやりとりされている現在において、古くから研究されてきた量子マネーが中央集権的な通貨発行と通貨検証の仕組みしか提供しない未来は考えにくい。人々は既に分散環境で管理運営される通貨の便利さに慣れ親しんでいるため、量子マネーにも同等、もしくはそれ以上の機能を求めるのは自然であろう。

本プロジェクトが分散環境での量子マネー管理を提案することで、量子情報技術が社会基盤をさらに便利に安全にすることをアピールできるようになると考えられる。

また、誰もが量子コンピュータを使って量子マネーを発行できる今回の仕組みは、量子情報技術をよりユーザの身近に感じさせるようになる提案とも言える。

6. 桝本尚之（フリーランス）

参考文献

[1] Stephen Wiesner. Conjugate coding. In SIGACT News, 15(1), pages 78-88, 1983.

[2] Mark Zhandry. Quantum Lightning Never Strikes the Same State Twice. In Proceedings of EUROCRYPT 2019, pages 408-438, 2019.