量子耐性ブロックチェーン

2020 年 12 月吉日

産業イノベーションの可能性

ウォークマン、iMode など、振り返れば日本には世界に先駆けた発明がたくさんありました。しかし、残念ながら現在は iPhone、Android、Huawei の後塵を拝する国になっています。今、量子耐性ブロックチェーンを支える特許や著作権の数々を日本人である私が確保していることを、皆さん、どうか活用してください。

[開発者略歴]

渡邊栄治（Eiji Watanabe）
1964 年東京電気大学・電子工学科を卒業後、日本電子株式会社に入社。その後 1972 年まで（株）フジミックに在籍。1979 年メテオーラ・システム（株）を設立し、1982 年 07 月（株）アマダ様と資本提携（2005 年 03 月に資本提携を解消）。2018 年にポスト量子ビット（株）を特許の現物出資で設立。発明家として 1)未知のバックドアが活動を開始した時、サブネット TCP/IP 層でバックドア接続を自動切断する技術の確立、2）非可換アルゴリズムが創る境界防衛線。☞ Blockchain_problems_Jan07.pdf (meteora.co.jp)

[ポスト量子暗号と可換アルゴリズム]

2020 年 10 月 24 日、NIST はポスト量子暗号の標準化プロセス Round3 に入り Finalists を発表しました☞（https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions）。現状の「公開鍵スキーム」は暗号処理と復号処理が可換です（可換アルゴリズム）。この可換の関係を安定的な量子耐性にする技術は、通常、達成困難です（一つの例外を除いて）。そこで NIST は公開鍵スキームを①Public-key encryption scheme, ②Key establishment scheme, ③Digital signature scheme の三つのスキームに分け、三つのスキームそれぞれについて標準化プロセスを進めることになりました（NIST 標準スキーム）。これは、可換アルゴリズムの量子耐性が達成困難である、ことを意味しています。

[非可換アルゴリズムへの期待]

一方、表題の技術は、非可換の鍵管理技術（発見された）と NIST 標準スキームとが役割を分担して達成されたものです。非可換の鍵管理技術は、計算困難性ではなく情報理論的な防衛を行う技術（Mathematical defense）です。情報理論的な防衛を破る攻撃としてはサイコロを振る以外には無いため、標準化の必要性がありません。これは非可換アルゴリズムの特色です。

[量子耐性ブロックチェーン＝非可換の鍵管理技術 + NIST 標準スキーム]

たとえば、デジタル金融資産を想定したとき、そこには完璧な消費者保護が求められます。量子耐性ブロックチェーンはこの課題を**非可換の鍵管理技術と NIST 標準スキームの共存**によって

解決しました。これにより、利用者のプライバシー保護、サイバー攻撃の無力化、資金洗浄（不正送金）を止めるプロトコルなどを共存させることが可能になりました。同じサイトの「多変数デジタル通貨」に解説しています。

[消費者目線のイメージ]

デジタル金融資産にもお財布が必要です。スマートフォンがハードウオレットになります。量子耐性ブロックチェーンにおいてはスマートフォンがお財布になる一方、その「預金口座」も管理することが出来ます。これについては別のデバイスが管理します。今のところ”リストバンド”を想定しています。

スマートフォンがお財布に相当する一方、”リストバンド”が「預金口座」の開放/閉鎖を行う：スマートフォンを紛失した、というような緊急時に”リストバンド”が貴方の「預金口座」をリモートで閉鎖する。

”Euro watch”, ”Apple watch”, ”xxx watch”, etc…

ブロックチェーン（匿名性を保証する）では「預金口座」を一時的に閉鎖することはできません。これが資金洗浄を止められない理由です。しかし、可換から非可換アルゴリズムに移行すると、ブロックチェーンと私達の間に境界防衛線が現れる。それにより「預金口座」のリモート閉鎖が可能になりました。その理由を下記に説明します。

[実際、非可換アルゴリズムへ移行すると…]

情報の漏えい自体を止めることは不可能です。漏洩した情報 B が使われた時、従来のシステムは元の情報 A と区別しない。どちらが先に使われても同じ結果になる：つまり、元の情報 A と漏えい情報 B は可換です（A×B=B×A）。それでは非可換アルゴリズムへ移行してみましょう。鍵情報 A が漏えいして、サイバー攻撃は情報 B を得たと仮定する。攻撃者は鍵情報 A のユーザとして情報 B をネット上で使いたい。可換アルゴリズムなら A×B=B×A になるから、攻撃者もユーザに成れる。が、非可換アルゴリズムでは A×B≠B×A ですから、漏えい情報 B でユーザに成り済ますことができません。こういう非可換アルゴリズムが消費者を各種の犯罪から防衛する境界を作ります。すなわち、私達のプライバシーと金融資産を守ります。同じく、通貨の偽造を難しくし、通貨発行の信頼を守ります。そして資金洗浄を止めるプロトコルを持つようになります、つまり、「預金口座」を閉鎖できるようになります。

[パスワード登録を求めない：なぜならユーザサイドがアカウントを管理する]

アカウントについて考えて見ましょう。私たちは長年、ユーザのアカウントはサービス提供者が管理するものと考えて来ました：ここではパスワードの登録を求め、アカウントをサービス提供者が管理する。

非可換アルゴリズムへ移行すると、パスワード登録を求めない。アカウント管理をユーザサイドが行う。ユーザサイドとはユーザ、取引所、第三者の 3 人です。この 3 人の同意を衝突関数 $Y^{-1}()$ が検証した時、ユーザは署名タスクにログインできます。こんな風に➡

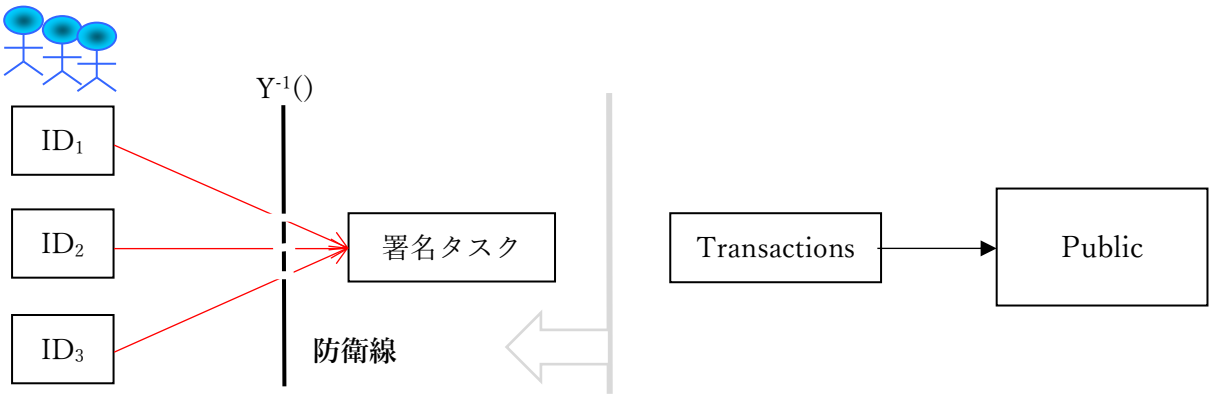

Fig.1: ログイン ID が 3 個現れる。

ログイン ID（ID_1 ID_2 ID_3）と衝突関数 $Y^{-1}()$と通信プロトコルが従来のアカウントに相当する。衝突関数 $Y^{-1}()$には量子耐性が有り、それだけでなく、いかなる攻撃も衝突関数 $Y^{-1}()$を騙すことは現実時間では成功しない：要するに、いかなるサイバー攻撃は無力化されます。このログインの概念実証を web 環境で行いました。

[産業イノベーションの可能性]

量子耐性ブロックチェーンは既存の産業をアップデートします。「多変数デジタル通貨」として金融分野に応用することも可能です。

基準	目に見える	ユーザ ID を持たない	手渡し支払いが可能	人の自由を制限しない	タンス預金が可能	
不換紙幣	○	○	○	○	○	Money
金、Gold	○	○	二重支払いを止める	○	○	
多変数デジタル通貨	×	○	二重支払いを止める	○ 注 3	○	
Bitcoin パスワード使用	×	○	二重支払いを止める	○	○	
デジタル人民元 パスワード使用	×	×	○	× 注 2	×	単なる IT
CBDC パスワード使用	×	×	○	×	× 注 1	

表 1 ：非可換アルゴリズムは「預金口座」の閉鎖を行える。いかなる鍵データも実装されない。

私達はだれしも、お財布と紙幣（不換紙幣）を見ない日は有りません。紙幣には「目に見える」「ユーザ ID を持たない」「手渡し支払い可能」「人の自由を制限しない」という特色があります。多変数デジタル通貨にも紙幣と同じ特色を持たせることができます。つまり、多変数デジタル通貨と紙幣とは互換です。「紙幣との互換性」に中央銀行も異論は無いはずです（表 1 を参照ください）。

注 1：紙幣は匿名性を保証するから日本人は現金を信頼している。匿名性が有るからタンス預金も可能です。これはキャッシュレス決済の普及が進まない一因であるという。現在進行中の CBDC は、金利を付ければ、タンス預金を回収する手段にもなり得る。匿名性を保証する CBDC なら、永く広く愛されるでしょう。そういう CBDC を中央銀行に期待したい。

注 2：一般に、発行者の論理に立った設計になりがちですが、多変数デジタル通貨は消費者保護の立場に立ってプライバシーと金融資産を守り、同時に、資金洗浄をブロックするプロトコルを持っています。前者の設計は「単なる IT]ですが、後者の設計は「Money」です。「単なる IT]は日常のお買い物には使えるが、航空券の購入には使えない、そういう運用も可能です。

注 3：多変数デジタル通貨、金、紙幣は人の自由を制限しない。これが「お金」の性質です。これらは国家の威信とバランスするが、発表されている CBDC はバランスしない。

[日本が起こす世界的なイノベーション]

ウォークマン、iMode など、振り返れば日本には世界に誇る発明がたくさんありました。しかし、残念ながら現在は iPhone、Android、Huawei の後塵を拝する国になっています。今、量子耐性ブロックチェーンを支える特許や著作権の数々を日本人である私が確保していることを、皆さん、どうか活用してください。日本が再び先陣を切るチャンスが来たことを確信します。日本が先陣を切らなければ、”Euro watch”、”Apple watch”、”Libra watch”が世界中の人々に愛され、日本は再びガラパゴスになってしまうでしょう。このような危惧が有るので、ライセンス候補に限らず、立ち上げを支援するような方々も歓迎しています。

なお、上記に関連して、未知のバックドアが活動を開始した時、その接続をサブネット TCP/IP 層で自動切断する技術についても（PoC 済み）、ライセンスする用意が有ります。これは 5G と 6G を差別化する要因になるでしょう。

2021 年 1 月 28 日更新

©著作者　渡邊栄治　METEORA SYSTEM