2020 年 12 月吉日
全ての産業へ

METEORA SYSTEM Co., Ltd

量子耐性ブロックチェーン

産業イノベーションの潜在力

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。発明家として私は、1）未知のバックドア（セットアップは過去時制）が活動を開始した時に、サブネット TCP/IP 層でその接続の確立を中断する技術, 2）非可換アルゴリズムを応用する技術、を確立した。

[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 標準スキームと参照する）。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、表題は、非可換アルゴリズムに依る鍵管理の特色と NIST 標準スキームの特色を統合したところのブロックチェーンの新機軸です。非可換アルゴリズムベース鍵管理は、従来の計算困難性ではなく、情報論的な防衛を得意とする技術（Mathematical defense）です。情報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、その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。

[当該表題＝非可換アルゴリズムに依る鍵管理 ＋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、それには完璧な消費者保護を求めるべきだと思います。当該表題はこの課題を「非可換アルゴリズムに依る鍵管理と NIST 標準スキームとの統合」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の実装などを可能にしました。このロジックを同サイトの「多変数デジタル通貨」に載せました。

[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。その管理手段はお財布とは別のデバイスです。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し、リストバンドが「預金口座」に相当する：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。つまり、パスワード不要。

”Euro watch”, ”Apple watch”, ”Libra watch”, and…

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。これが消費者を保護できない理由です。同じく資金洗浄も止められない理由です。一方、非可換アルゴリズムによって秘密鍵を消すことができます。これで秘密鍵を不特定者から守る境界防衛が確立します。それで「預金口座」のリモート閉鎖が可能になりました。実際、非可換アルゴリズムに移行してみましょう。

[実際、非可換アルゴリズムへ移行すると…秘密情報が漏えいしても…]

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、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、つまり、AB=BA。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 AB=BA になるから、攻撃者もユーザに成れる（攻撃が成功する）。が、非可換アルゴリズムでは AB≠BA ですから、漏えい情報 B は役に立ちません。こういう理由で、非可換アルゴリズムは消費者を各種の犯罪から守る防衛線を作ります。防衛線を実装する情報通信技術を考えてみてください。貴方が野心的な起業家なら千年に一度のチャンスが来たと感じるでしょう。

この防衛線を実装する ICT の具体例

1）金融について言えば、それは私達のプライバシーと金融資産を守ります。同じロジックで通貨の偽造を難しくし、通貨発行の信頼を守ります。そして私たちは資金洗浄を止めるプロトコルを持つようになります（☞多変数デジタル通貨）、つまり、システムは「預金口座」を閉鎖することできます。

上記に関連する認証技術が有ります：
2）非可換アルゴリズムでは、ユーザから秘密 ID1 が流出しても、サービス側から秘密 ID2 が流出しても、この実装($ID_1ID_2 \neq ID_2ID_1$)は攻撃者のアクセスを止めるプロトコルを持ちます。リストバンドとスマートフォンのセットがこのデバイスになります。この認証技術は IT の常識に入っていません。

上の文脈から、読者はもうパスワードを必要としない、パスワードとお別れの時です。無い方が安全。サイバー攻撃も全滅です。ICT は今よりシンプルになり、私達の生活スタイルを穏やかな環境に変える。これはビジネスモデルではなく、ロジックです。

[産業イノベーションの潜在力]

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。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。デジタル通貨にも紙幣と同じ特色を与えることができます。すなわち、多変数デジタル通貨は紙幣と互換です。「紙幣との互換性」に中央銀行も異論は無いはずです（表 1 をご参照ください）。

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	○	○	
多変数の DC	×	○	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。

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い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も持っています。発行者の論理は「単なる IT]ですが、多変数デジタル通貨の論理は「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、という運用が可能です。

注 3：金、紙幣、多変数デジタル通貨は人の自由を制限しない。又、パスワード入力も求めない。これが「お金」がカレントになる理由です。

[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、**この非可換アルゴリズムが起こすイノベーション全般に肩入れするような方々も歓迎しています。**このメッセージは国内国外を問わない。

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。

2020 年 1 2 月吉日