Hyper text

主題：多変数デジタル通貨

副題：この記事は「デジタル通貨が資金洗浄やテロ資金になることを防ぐ発明」物語です。

親愛なる友へ：

本文をお読みいただく前に、発明の要点を、説明抜きで、お伝えします。

　ブロックチェーンそのものは歴史的な発明ですが、皆さん、未だ使いこなせていないです。当初、利害関係者の期待が大きかったが、期待した通りにはブロックチェーンを使いこなせていない。価格変動(Volatility)と資金洗浄のことがネガテイブにのみ評価されています。私は、その価格変動と資金洗浄を重要なポテンシャル「野生の馬」として見ており、これを高く買う：私はその調教のやり方を知っているからです。

調教師の目

紙に印刷しただけの不換紙幣がなぜ流通するのか？次のように考えると、その理由が判る：ある人が紙幣を見たら、貴方のプライバシーが見える、としたら流通しませんね。金や銀についても同様です。この思考実験から Satoshi Nakamoto（論文）が設計した”New Privacy Model”は重要であることが判ります：これが「お金」の出発点です。この出発点を次のような質問を読者に出して確認したい：レジでお金を支払う時、貴方は紙幣にパスワードを打ち込みますか？

上の質問は、単なる IT と「お金」との違いに気づかせるものです：この違いに興味を抱く方はきっと野心的な起業家か開拓者に違いない。私、調教師もこの違いを見ている。紙幣はパスワードを求めない。それと同じように、多変数デジタル通貨もパスワードを求めない。パスワードが求められたら、貴方は安心ですか？パスワードが有っても、サイバー攻撃が成功すれば、貴方の暗号資産は消えますよ。それと内部の者はパスワードに手が届きますよ。

現時点のデジタル通貨は”New Privacy Model”を破壊する「単なる IT」

2020 年、各国の中央銀行はいくつかのグループを作ってデジタル通貨に取り組むと聞いている。私はデジタル人民元を想像できる：CCP は既にキャッシュレス決済の情報を中国人民銀行に集める法制度を確立している(1)。監視社会の通貨だから、初めから Satoshi Nakamoto の”New Privacy Model”を無視する。監視社会における個人の ID と決済の流れは連携している：プライバシーは無い。そこでは当局が ID の使用を止めれば、お金の転送は何であれ、止まる。これは「単なる IT」の話です、通貨の話ではない。監視社会を合法的に進めているから、デジタル人民元がブロックチェーンをベースに設計されているか否か判らない。いずれにしろ、世界はデジタル人民元に騙されている。☞digital currency rating

同様に、民主主義国家の当局もデジタル人民元に近い議論をすると思います。「お金」の設計を

議論するのではなく、当局も「単なる IT」の設計を議論する：つまり、”New Privacy Model”の重要性を無視するでしょう。たとえば、監視社会を目的にする訳ではないが、個人情報（KYC）の提出を義務付ける。それこそ単なる IT、プライバシーを犠牲にする IT です。日本には住民票、健康保険証、運転免許証、など多様な社会基盤があるので、ID に不足は無い。しかるに、又一つ ID が増えた、「マイナンバー」である。こういう傾向だから、デジタル通貨の場合もマイナンバーを導入する可能性が有る：これでは CCP の監視社会と変わらない日本になる。

デジタル通貨の格付け

私はここに鏡を持っている、「お金の関数≡M()」である。この鏡に多変数デジタル通貨、ビットコイン、単なる IT を映し出して見せることにした。☞digital currency rating。ここで、最低の格付けになる関数はどれかをご確認頂きたい。

発明家の目

私は、世の中がベストを選択しないことを経験して来ました：人々が求めているものはベストでは無い。シュンペーターに言わせると「皆さんは一つの馬車と他の馬車を連結することしか考えない。連結したって汽車にはならないよ…」。馬車と馬車の連結思考を捨てるのは大変むずかしいことです。だから、私は野心的な開拓者や起業家に期待する：犯罪の抑止力だけでなく、暴れ馬を訓練する方法を彼らに伝えたいと思います（下記）。

ブロックチェーンの社会実装

資金洗浄とお金の転送は分離される、サイバー攻撃も無力化される。

多変数デジタル通貨においては、署名用の鍵（a private key）は「燃やされて」鍵データが存在しない：鍵は機能としてのみ存在する。燃やされて残った灰のことを多変数デジタル IDs n=3 と言う：式 n=3 は 3 個の変数を意味する。この「燃やされて鍵データが存在しない」という状況を暗号学で言えば、署名用の鍵データが多変数デジタル IDs n=3 の原像（pre-image）になったということです。鍵データはイメージになった訳です！

3 個の変数は、それぞれブロックチェーン社会（ユーザ、取引所、第三者）へ実装される：鍵は実装されない。署名チェーンを伸ばすかどうかについて、その都度、社会の意志は一致か/不一致かどちらかの場合に分かれる。この二者択一がデジタル通貨やブロックチェーンを制御可能にする新機軸である。その結果、

１）任意のビットコインアドレスに資金洗浄の疑いが生じれば、ブロックチェーン社会の不一致が起き、取引所はその手続きに介入して止める。同時に、「公開呼びかけ」を行い、その応答を見て、流れの真と偽を分ける。すなわち、資金洗浄をブロックする。

２）ブロックチェーン社会に鍵データが存在しないから、サイバー攻撃のターゲットそのものが無い。このことは消費者の暗号資産を完璧に保護する。さらに,

３）財布を紛失した時、紛失に気づきさえすれば、暗号資産を消費者の手元に全額取り戻す。

デジタル通貨の条件付き発行

４）3 個の変数を社会実装することで「貨幣の発行に責任を負う主体（主語）」を確立した。

あのビットコインのマイニングは貨幣の需要に応える仕組みではない。私は「貨幣の発行に責任を負う主体（主語）」を n=3 社会実装に見た。デジタル通貨も、当然、Satoshi Nakamoto が定義した署名チェーンである。この署名用の鍵データを奪えば、大量の偽造が可能になる：テロリストが機関銃を連射しながら、奪うシーンではないから、鍵の漏えいには誰も気づかない。

この主体（主語）の呼び名が二つ有る：一つは、A)変数の個数が 3 個のマネタリーベース、もう一つは、B)変数の個数 n=3 の社会実装。A)は通貨の偽造の困難性に注意を向ける。B)は価格の制御に注意を向ける。いずれも貨幣の需要が発生する度に即応する。それで、価格の乱高下(volatility)をコントロールすることが可能になる。すなわち、暴れ馬のポテンシャルを殺すことなく、S&P500 のように、ゆるやかな上昇曲線を描くようにすることも可能…。

可用性

この書類を書き始めた頃、5 月 1 日、私はコロナパンデミックに入った辺りに居た。心配なことが多々有った…日本に限らず、コロナや大災害に限らず、恐怖を煽る勢力が強く、人々が恐怖に煽られて、人が人のための経済基盤を「破壊」してしまう…民主主義は大きな政府という罠にかかり、人々は自ら臨んでその罠にかかりに行く。中央銀行もサプライチェーンも疲弊する、当然、中小企業も疲弊する…この罠の引力はますます強くなる一方。しかし、今や心配は消えた。未来の事実は心配した通りに成るとしても、こういう時こそ、民間が立ち上げることの出来る通貨が有る、私の手元に有る：多変数デジタル通貨の可用性である。

本ペーパは「犯罪への抑止力」と「デジタル通貨の条件付き発行」の 2 点に絞っている。それで第三者を資金洗浄やテロ資金を監視する機関として位置付けている。可用性を考える時は、第三者を、社会を再起動する、経済を再起動する、幸福を追求する政治を再起動するポジション、として考える。どういうことかと言うと。民間が発行する通貨、「自立する通貨、a self-sustaining currency」である。経済学のためのお金ではなく、人々の自助努力に喜びを与えることを目的とした通貨である、と言えるかも知れない。マルクスもケインズも、このような通貨を知らない。第三者のポジションを知る参考として、本文の付録に Swift coin を載せた。

ここから本文 PDF へ

ライセンス情報

多変数デジタル通貨は、他の通貨には不足しているコンビニエンスを提供することができます☞表 1. そういう能力を持っているので「通貨のための通貨」です。このライセンス契約について私の考えを本文 PDF の末尾に掲載しています。現在の金融システムを刷新することも可能です

し、協調関係を築くことも可能です。あるいは「小さな政府コイン」に代表される民間発のデジタル通貨も実現可能です。しかし、通貨のための通貨は「何をやれ！」と私達に命令しているのか未だ判りません。私は、現状の政治経済に迎合する「馬車と馬車の連結」を意図していませんでした。しかし、通貨のための通貨は今の進行状況と協調関係も築けます。

さらには CBDC との協調関係も築けます。どういう所かと言うと、CBDC は閉域網にサービスする「鎖国通貨」ですね：もし、私が CBDC(a)を持ち歩いて CBDC(b)の国へ行ったら、両替できるのでしょうか？私は今の紙幣と同じやり方で両替するんでしょうか？オンライン・リアルタイムで交換する方法が有ります。表 1 の「通貨のための通貨」を買ったり売ったりすればいいのです。こういう文脈では「通貨のための通貨」は基軸通貨 de jure standard になります。

ライセンス候補のミッションに発明の開示が為されます：議論を通して、そのミッションの姿が馬車と馬車の連結ではなく、汽車となって現れます。ここでライセンス契約に至るでしょう。
敬具
渡邊栄治
METEORA SYSTEM
2020 年 10 月 20 日

本文目次

[技術データのリンク一覧]
Satoshi Nakamoto（論文）
多変数ブロックチェーンの設計図
digital currency rating
多変数 n=2 の実装例

(1) Magazine “The Liberty” December 2019 No. 298

Hyper text

この Hyper text の印刷