デジタル通貨の格付け

多変数 n(n≧2)ブロックチェーンは「お金」の原型である：関数 M()で表される。

「お金」=M（秘密変数 n=1，匿名変数 n=1，多変数 IDs n=3，偽造確率）

ここで M()の多変数 IDs n=3 は 3 個のデジタル $ID_1 \neq ID_2 \neq ID_3$ を表し、n は確率変数の個数を表す。なお、秘密変数≡a private key、匿名変数≡a bitcoin-address

この原型はビットコイン、stable coin、peg 通貨、CBDC、多変数デジタル通貨などの母なる体である。母なる体は多様な「お金」の格付けを知っている。原型の変数の個数を数えてみよう：1+1+3=5，➡格付け＝5。変数の個数が少ないほど格付けが下がる。逆に変数の個数が増えるほどシステムは安定する。変数が一つよりは二つの方が安定すること、制御可能になることは容易に想像できるでしょう。以下、典型的な事例について格付けを計算する。

1） Satoshi Nakamoto's New Privacy Model

New Privacy Model=M（秘密変数 n=1，匿名変数 n=1，偽造確率≒0）

New Privacy Model はビットコインの原型です。ここでは変数の個数は全部で 2 個であるから、格付け＝2 となる。しかし、実際の運用では秘密変数へのアクセスをパスワードに許している。だから変数は確率変数ではなく見えるデータになる（パスワードが手に入れば誰でも見れる）。したがって、New Privacy Model は次のようにして破壊される：

Bitcoin=M（秘密変数 n=1➡n=0，匿名変数 n=1➡n=0，偽造確率≒0）

変数が見えるデータに変われば、サイバー攻撃や内部犯行の的になる。

ここで 0+0=0 であるから、格付け＝0。計算関係が秘密変数➡公開変数➡匿名変数である。秘密変数が「見えるデータ」に変われば偽造確率=1 になりそうだが、ビットコインはそうは成らない。マイニングだから偽造確率≒0。なおここの本題から外れるが、マイニングは貨幣の需要に応えることが出来ない。

2）単なる IT__監視社会の「お金もどき」__

CCP 当局の目には匿名変数も秘密変数も単なる「見えるデータ」に成る。人民には固有の ID が割り当てられ、ID が「見えるデータ」に紐づく。

初めから監視社会ゆえに

デジタル人民元=M（秘密変数 n=0，匿名変数 n=0，偽造確率=1）

初めから監視社会ゆえに

ここで 0+0=0 であるから、格付け＝0。上の式は、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と仮定しての話である。デジタル人民元はマイニングしない、つまり、貨幣の需要に応える：これは何を意味するか？偽造確率=1。デジタル人民元は初めから「偽造通貨の発行」である。偽造を隠す方法が有る：ネットワークを卸売りと小口販売に分けること。いずれにしろ、世界は騙されている。

３）多変数デジタル通貨

以下の M()についての解説は本文で行われる。

匿名変数が紙幣との互換を保証する

多変数デジタル通貨=M（匿名変数 n=1，多変数 IDs n=3，偽造確率=$1/2^{256}$）

ここで 1+1+3= 5 であるから「格付け＝５」。

三者の同意署名

条件付き通貨発行、その偽造確率=$1/2^{256}$

__資金洗浄と「お金の転送」は分離される__

サイバー攻撃や内部犯罪が無力化される。お財布を紛失しても、紛失に気づいた瞬間に、暗号資産が全額確保される。

2020 年 9 月 28 日

渡邊栄治
METEORA SYSTEM