多変数デジタル通貨

本記事は「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」の物語です。

先駆者 Satoshi Nakamoto に敬意を表して…

銀行口座と「お金」について深く考えて行きましょう。日本の慣習では、預金通帳とパスワード、又は銀行カードとパスワードという二つの IDs で「条件付き出金」を実行する。ここで、二つの IDs は確率変数です：ID_1 と ID_2 で表すことにする。ID_1 から ID_2 を決定するのは難しいし、その逆も難しい。それで二つの変数は独立です。私たちは「条件付き出金」を知っている：ATM に ID_1 と ID_2 を「二つを揃えて」入力すれば、紙幣が出て来るということ。大事なことは「二つを一緒に入力する」ことです。

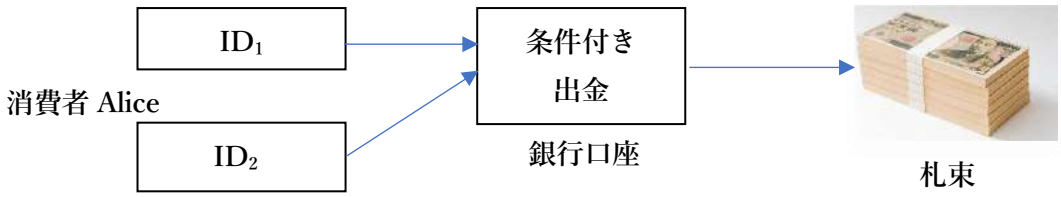


Fig.1:多変数 IDs n=2

もし、二つの事象が偶然に出会うという問題なら、条件付き確率という「ややっこしい問題」になってしまう。が、ここの ID_1 と ID_2 は「二つで一つ」になることが約束されていることです。そのような約束（プロトコル）を多変数 IDs n=2 と言う。

事件は IDs が盗まれた時に起きる：紛失した時に起きる。それで Alice が多額のお金を引き出す場合、銀行は「本人確認証」を求める；第三の ID≡ID_3 である。今度は三つを揃えて出金を制御する。これが多変数 IDs n=3 です。

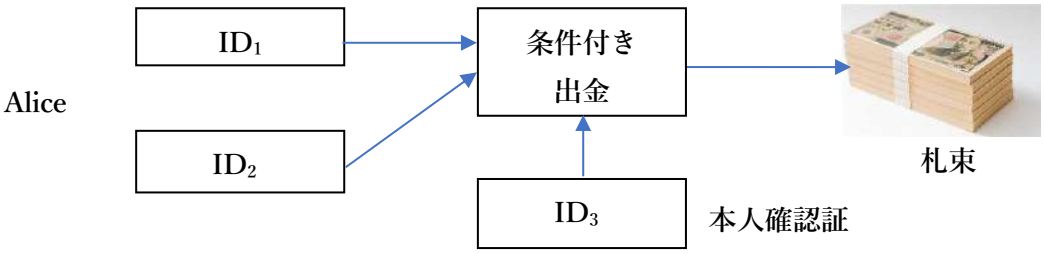


Fig.2: 三つの ID を揃える多変数 IDs n=3

ここで、Satoshi Nakamoto（☞このリンクは Hyper text 画面に在る）の設計した電子コインの定義を確認しよう：”We define an electronic coin as a chain of digital signatures.”（cited from 2 Transactions）. この定義を Fig.2 に投射してみよう：「札束」に署名チェーンの光が当たる。それ

なら「条件付き出金」は「条件付き署名手続き」になるでしょう。投射は下記の通りになる：

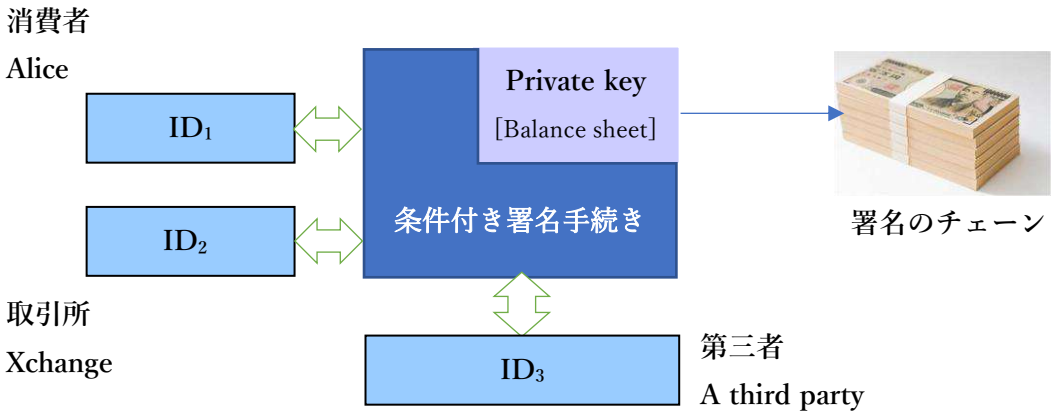


Fig.3: 条件付き署名手続き

三つの IDs が揃うと署名手続きが始まる：三つの IDs が揃わないと何も始まらない。こういう条件付き署名手続きは Satoshi Nakamoto の論文には記載が無い。

デジタル通貨の新しい定義

Satoshi Nakamoto（☞このリンクは Hyper text 画面に在る）の設計には「お金の転送」を条件付きにするプロトコルは無い。デジタル通貨の新しい定義を導入する：次の署名を条件付きで実行する：

出金＝送金＝通貨発行

その条件は何かと言うと、Fig.3 が示すように、１）ID1 と ID2 と ID3 各々を消費者、取引所、第三者が所持する：２）三者（消費者、取引所、第三者）が上記処理に署名することに同意している。この同意を検証する暗号学的な数学が有る：

__三者の同意を検証する衝突関数__

三者の同意検証は「異議なし」/「異議あり」に分かれる。「異議あり」の場合は、多変数 IDs n=3 のどれか一つが欠けた時、又は、どれか二つが欠けた時である。この場合は署名用の鍵データが再現しない（署名手続きが中断する）。この中断は、フェールセーフ、である。下記の状態を継続する：

送金の凍結＝資金洗浄資産の凍結=通貨発行の停止

ここでプライバシーは守られていて誰の「顔」も見えないことに注意する。この点が「お金」の設計と「単なる IT」を峻別する重要な基準である。「単なる IT」は個人情報の登録を求めるので当局にはユーザの「顔」が見える。以上がプロローグです。

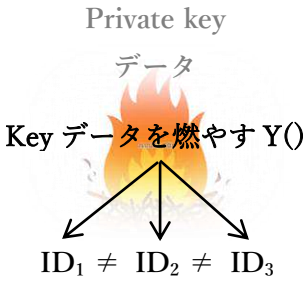
Ⅰ．鍵管理の新機軸

多変数デジタル通貨は数々の新機軸を備える：１）署名用の鍵は、機能として存在するが、実装されない：２）サイバー攻撃は無力化される：３）資金洗浄と正常なお金の転送は分離される：４）マイニングに代わりデジタル通貨の発行主体が存在する：５）デジタル通貨を偽造するのが

困難である(通貨の発行主体への内外から攻撃は成功しない)。これら新機軸を支える唯一の技術ベースが有るので、それを紹介する。

1．Private key を燃やす関数__残った灰__多変数デジタル IDs n=3

Private key は、言うまでもなく、署名用の鍵である。Satoshi Nakamoto はビットコインを署名チェーンとして定義した(cited from 2 Transactions)。私が今開示するテーマはビットコインではなく、多変数デジタル通貨である。多変数デジタル通貨もビットコインと同じく署名チェーンであるが、プロローグで示した「条件付き署名手続き」に基づく署名チェーンである。この技術ベースは唯一である。まず、Private key データを燃やす関数 Y()、燃やした後に残ったものは「灰」、こういう概念を下に図解した。



Key データを燃やす関数を Y()と表記する。

関数 Y()に Key データを入力した後、Key データを消去する。

Y()の出力に多変数デジタル IDs（ID_1 と ID_2 と ID_3）が現れる。

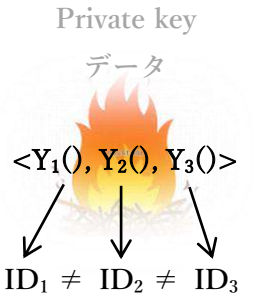
残った「灰」が多変数デジタル IDs（ID_1 と ID_2 と ID_3）である。灰には次の関係が有る：$ID_1 \neq ID_2 \neq ID_3$　この不等式は互いに計算して決定するのが困難と言う意味である。この水平方向の計算に対して垂直方向の計算も有る。すなわち、$ID_1 \neq ID_2 \neq ID_3$ から private key データの計算をしても「これです」という答えが返って来ない。

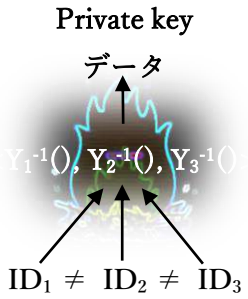
以上の関数 Y()は独特な形式で表される：$Y() \equiv <Y_1(), Y_2(), Y_3()>$

２．衝突関数

関数 Y()の逆向き関数が有る：それは「衝突関数 $Y^{-1}()$」である。関数 $Y^{-1}()$は上記灰から Key データを復活する。次のような形式で表される：$Y^{-1}() \equiv <Y_1^{-1}(), Y_2^{-1}(), Y_3^{-1}()>$

下のイラストレーションは、Private key データを燃やす関数を左側に示し、灰から鍵データを復活させる関数を右側に示す。二つの関数は私のパテントに関連する。



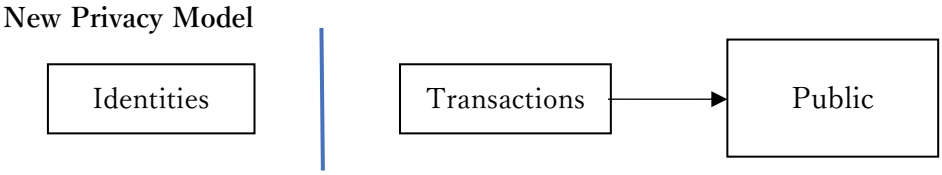


これら関数を Satoshi Nakamoto の論文に書き加える、それが多変数ブロックチェーンの設計図である。(☞このリンクは Hyper text 画面に在る)

Ⅱ．不換紙幣との互換性

１．Satoshi Nakamoto の”New Privacy Model”

元々ブロックチェーンには中心的な権力者が存在しないように設計されている。だから資金洗浄が可能になる。ここで注意することが有る：資金洗浄の追跡は可能であることだ。➡お金の転送記録の追跡は可能だがその「顔」は見えない。この仕組みを Satoshi Nakamoto（論文）は”New Privacy Model”と名付けた。彼の描いた図解を見ましょう。



上図のブルー線は、左側に描かれたプライバシーを守り、その右側の取引は全てインターネットに公開することを表す。すると「プライバシーは政府（権力機構）からも干渉されない、ただ、送金記録は公開される」。不換紙幣もその通りではないか：

__”New Privacy Model”は不換紙幣と互換である__

今、”New Privacy Model”を無視した「デジタル通貨？」を想定すると、それは紙幣と互換ではない、「単なる IT」であることが判るだろう。

個人情報やパスワードの登録を求める IT、これは「お金」ではない。

監視社会や一国の中で「お金」の働きをする「デジタル通貨」なら、「単なる IT」で国民を騙すことが出来る。*しかし*、取引所が扱う通貨は国境を自由に往来する。ここで他の通貨が「多変数デジタル通貨」と競争したら、どんな事件が起きるだろうか？

こんな事例が有る：貴方は雑誌記者として新種の「xxx コイン」の取材に行ったとしましょう。貴方は説明の途中で次の質問を出した：「そのスマートフォンが盗まれたらどうなるのか？」…「いや、ご心配なく、ほら見て、パスワードが有るから安心ですよねー？」と答えが返って来る。貴方はさらに質問をする:「ということは、お金の流れを当局は知る訳だね。徴税にも便利だね？」。私ならさらに質問したいことが有る：「パスワードでサイバー攻撃を防げるのか？」

２．それはプライバシーを守るからカレントする：

冒頭の「Dear Friend」にて「紙に印刷しただけの不換紙幣がなぜカレントするのか？」と問いかけた。その答えが”New Privacy Model”に在る：すなわち、「不換紙幣はプライバシーを守る

からカレントになる」。ビットコインも同じ式を共有する：

ビットコイン＝”New Privacy Model”

それなら、何故ビットコインは金融商品に成って、通貨に成れなかったのか？ 二つ理由が有る。一つは貨幣の需要に応える仕組みを持っていないこと。もう一つは下記です。

３．匿名変数と秘密変数

”New Privacy Model”を現金輸送車に喩えることが出来る：誰でも積荷を見ることが出来るが、誰から誰の所へ行くか分からない。この車について Satoshi Nakamoto（論文）[10 Privacy]は：“The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.”。さらに続けて：“privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.”。

解説する：ここの公開鍵は X.509 証明書を持っていない、➡誰の公開鍵か分からない、➡従ってビットコインアドレスも誰であるか分からないから、それは匿名変数である。もう一つ、秘密変数が有る：Private key である。変数の個数は各々1 個だから、n=1 と表す。これらの事実を「お金の関数 M()」に投射する：

M（匿名変数 n=1, 秘密変数 n=1）＝”New Privacy Model”

これは秘密変数が漏洩しなければ、プライバシーが守られる、という式です。

ビットコイン会社の株式公開！

サービス設計者は、*しかし*、どこかでパスワードを登録するように設計する。パスワードが匿名変数や秘密変数と連携する時、変数は「見えるようになる」。

ビットコイン≠”New Privacy Model”

これだからビットコインは紙幣と互換には成らない。この非互換ビットコインは「ビットコイン株式会社」が行う株式の公開である、決して通貨ではない。実際、現在のビットコインはポートフォリオに組み込まれている。

Ⅲ．資金洗浄に対抗する暗号資産の凍結プロトコル

１．ビットコインアドレスの使用を制限する__プライバシーを犠牲にしない__

デジタル人民元が送金を行う時、条件付き送金である：当局が Alice を気に入れば、お金の転送を行う：当局が Alice を気に入らなければ、Alice（人）の自由を制限して送金を停止する：つまり、デジタル人民元は Alice（人）の自由を制限する。他方、多変数デジタル通貨は、人 Alice ではなく、ビットコインアドレスの使用を制限する。だからプライバシーを犠牲にしない。これには条件付き署名が必須である。

”New Privacy Model”は「顔」を見せないが、過去から現在までの送金の流れを検証する仕組みを提供する：所有権チェーンの検証できる。ただ、この送金の流れが不正であると判っていても今までは制御する方法が無かった。言い換えると、我々は不正送金のチェーンは見えるが、今までは制御する方法が無かった。しかし、今回は違う、以下の通り：

三者の同意を検証する衝突関数

今、不正送金チェーンをこの瞬間に切りたいと読者が思ったと仮定する。ただ、今の段階では、不正か否かは未だ決定できない。その願いは簡単に実現する：不正チェーンのビットコインアドレスの使用を制限する：これが全てだ。

そのために当該ビットコインアドレスと結合している多変数 IDs の一つをオンライン運用からオフに移動する。このようにすると、システムが署名手続きを中断する。プロトコルは言う：IDs n=3 のどれか一つが「衝突関数」の入口に集まらないから署名用の key データを再現できない：
➡送金が中断させられる：

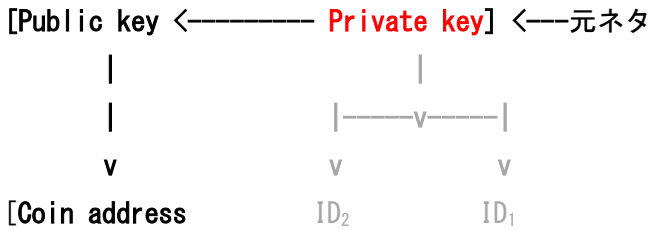
送金の中断 ＝ 資金洗浄資産の中断

ここで課題が浮き彫りになった：当該ビットコインアドレスと多変数 IDs をどうやって紐づけるか、という問題である。

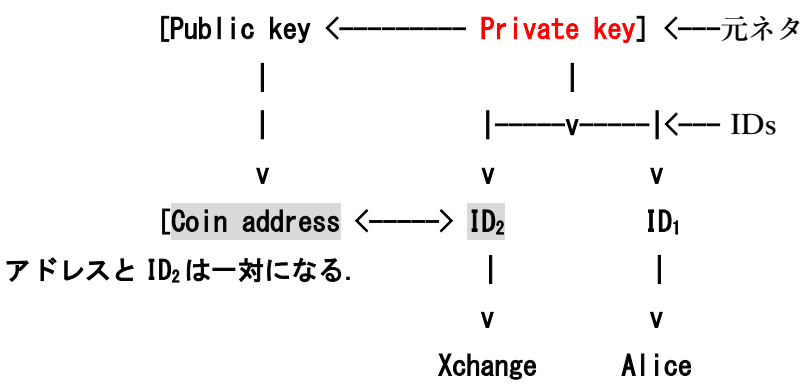
２．ビットコインアドレスと取引所が持つ ID_2 を紐づける：

通常、Alice は ID_1 を手元に置き、第二番目の ID_2 を取引所に転送し、第三番目の ID_3 を第三者に転送する。これが「多変数 IDs n=3 の社会実装」である。

ビットコインアドレスと多変数デジタル IDs の一つを結合することは簡単である：Alice の手元で行える。なぜならビットコインアドレスも多変数デジタル IDs も Private key データが元ネタになっているからである。その元ネタを持っている人は Alice だけであるから、Alice は両者の紐づけを行える：第三者にはできない。そのプロセスは：



矢印の方向は計算が容易な方向である：右から左の矢印は署名に使われる：上から下の矢印は所有権チェーンの検証に使われる。ここでは多変数 IDs の個数を n=2 にした：ビットコインアドレスを Coin address と書いた。



Alice の手元で ID_2 と Coin address を一対にする。この一対を取引所に送達する：取引所はこの一対を DB に格納する。ここで取引所はその一対が誰であるか分からない：このように Alice のプライバシーが維持される。

３．資金洗浄の凍結プロトコル

多変数デジタル IDs の一つ ID_2 を制御変数に使うプロトコルを紹介する：プロトコルは ID_2 をオンライン運用からオフに移動させる。たった、これだけで送金を中断させる。

今、ビットコインアドレス（ボブ）とビットコインアドレス（オスカー）はダークサイドのアドレスかも知れない、という通報が取引所に来たとしよう：判定者は通常 ID_3 を持つ第三者である。通常、この第三者が資金洗浄を監視する。又は、取引所がその送金の流れは怪しいと判定したかも知れない。

条件付き署名、公開呼びかけとフェールセーフ、この組合せが資金洗浄ソリューション

このような通報が来た時、取引所は ID_2 のオンライン運用を止め、ネットに次のような公開発表をする…当方はコインアドレス（ボブ）とコインアドレス（オスカー）の運用を止めた。これに異議の有る者は連絡せよ…。呼びかけに対し何の連絡もなければ、第二変数 ID_2 はオンラインに戻らない➡送金手続きは中断を維持する（ブロックチェーンの性質に基づくフェールセーフ）。

上の凍結プロトコルはブロックチェーンの性質に基づくフェールセーフである。資金洗浄の意思は「公開呼びかけ」に応えると、その意思の「顔」がバレる：応答が無ければ「送金手続き中断」を解除できない。➡自動的な資産凍結と言える。このプロトコルは、資金洗浄だけでなく、インサイダー取引や市場操作、さらに裁判所の資産保全命令にも適用可能である。

金融制裁の根拠

監視社会の合法性がデジタル人民元の行う金融制裁の根拠である。私の発明は中央集権的な権力に基づくのではなく、金融制裁を公開呼びかけとフェールセーフに基づいて実施する。

Ⅳ. CBDC マター、デジタル通貨の条件付き発行、適正価格の制御

条件付き通貨発行__マイニングとは異なる解__

１．あなたはパスワードが有れば、安心ですか？

紙幣はリアルな存在である：手に取って、触って、手渡す、そのプロセスがリアルである。紙幣にパスワードの登録を求める人は居ない。それに比べて暗号通貨の方は空気感に近い：「これは私のものだ」と言える「これ」が手元に無い。ある日「事件だー、貴方の暗号資産が消えたー！」と言われて、貴方は抗議できますか？それでパスワードの登録を求められると、何か安心する？でも、盗もうと思えば盗めるのがパスワードです。

多変数デジタル通貨はパスワードの登録を求めない。パスワードで守りたいと思うような対象が存在しない。秘密鍵は署名のために必須であるが、その鍵データは実装されない。だから、パスワードや生体情報の登録を求める理由が無い。「事件だー、貴方の暗号資産が消えた！」、これは冗談で言うしか言えない。

ある日、アリスは、お財布が無いと気付く：どこかに置き忘れたかも知れないし、落としたかも知れない。お財布を落としたら通常、紙幣は戻ってかない。パスワードが無いから多変数デジタル通貨も紙幣と同じ運命である、と貴方は思うかも知れない。その通り、紙幣と同じである。

私は、多変数デジタル通貨が紙幣と同じ運命である方が良い、と思っているが、アリスは暗号資産を全額保全したいと思っている。そういう方には下記リストバンドはいかが？

スマートフォンが無いと気付いたアリスは直ぐ取引所（又は第三者）に第二変数 ID_2 と共に通報する。変数 ID_2 は CIM ﾊﾟﾗﾒｰﾀを持っている、➡取引所は変数 ID_2 の運用をオンラインからオフにする➡送金手続きが中断する。ここで問題になるのは直ちに取引所（又は第三者）に知らせること。どうやって？多変数デジタル IDs をバックアップデバイスが保管しているので、ここから緊急のメッセージが最寄りの基地を経由して取引所に飛んで行く：メッセージは変数 ID_2 と CIM ﾊﾟﾗﾒｰﾀを持っている。バックアップデバイスをイメージすると：リストバンドが出て来る。

富裕層アリス向き

”Wristband” とスマートフォンがお財布を構成する。デバイスは送信機能だけ備える。取引所は送金中断をキャンセルする手続きを用意している。

２．プライバシーからプライバシーへの転送チェーン

多変数デジタル通貨、ビットコイン、デジタル人民元をお金の関数 M()に投射し、格付けをした：☞Digital currency rating（☞このリンクは Hyper text 画面に在る）。多変数デジタル通貨の関数形は：

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

ここには匿名変数 n=1 が有る：秘密変数 n=1 は無い。それゆえ、如何なる Key データも漏えいしない：多変数デジタル通貨はプライバシーからプライバシーへチェーンする。これはプライバシーを犠牲にする IT とは違う：利便性を理由にしてプライバシーを犠牲にする「xx コイン」やデジタル人民元とは違う。下図は左から右へ時間が進む：

プライバシー	Forming a chain	プライバシー
IDs のバックアップ		IDs のバックアップ

Fig.4: プライバシーからプライバシーへの転送チェーン

チェーン形成の仕方は Satoshi Nakamoto（論文）[3. Timestamp Server]に載っている。

３．三者の同意検証、マイニングに代わる「お金の信頼」

概況

通常、消費者 Alice が取引を行う時は、ID_1 を Alice が持つ一方、第二番目の ID_2 を取引所に転送し、第三番目の ID_3 を第三者に転送する：取引所や第三者はスマートフォンを CIM パラメータで識別する：三者各々は互いに独立である。これが「変数の個数 n=3 の社会実装」である。この社会実装から二つの果実を収穫できる：１）犯罪抑止力（ブレーキ役）と２）お金の発行主体の信頼（アクセル役）

１）三者の同意が無ければ、送金が行われない：これは事故や犯罪に対して Fail-safe が働く。これがブレーキ役である。

２）三者の同意を検証する衝突関数が有ることは、単一の意志が行う決済よりも信頼できる。これはアクセル役である。

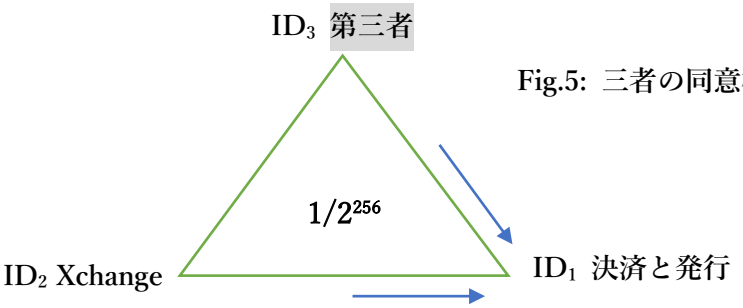


Fig.5: 三者の同意検証 ＝ デジタル通貨の発行主体

三者の同意検証を図式したものが Fig.5 である。これを CBDC に適用すると、デジタル通貨の発行は中央銀行の意志に基づくのは当然であるが、発行時の IT の動作は単一意志プロトコルで

はない。元々ブロックチェーンのマイニングには発行主体が存在しない。三者の同意検証のメカニズムがデジタル通貨の発行主体である。

数理を基礎にした第三者

Fig.5 第三者は、単に第三番目の ID_3 を受け取り、不正送金の監視を行うだけの存在であっても決済の信頼性に絶大な寄与をする。莫大な費用を投じた中央集権的な決済システムよりも第三者を含む数理の方が信頼できる。この数理ベースの第三者が多大な貢献をする事例が有る：実施例の一つは”Swift coin”である。Appendix（☞このリンクは Hyper text 画面に在る）。

三者の同意検証チェーン

Fig.5 は、変数の個数 n=3 の社会実装を三角形で表現し、変数 ID_1 と ID_2 と ID_3 が「衝突関数」に集まる様子を矢印が表す➡「衝突関数」の出力に署名用の Key データが再現する➡通貨発行者は署名チェーンを更新する（送金）。

Satoshi Nakamoto はビットコインを署名チェーンとして定義した：”We define an electronic coin as a chain of digital signatures.” (cited from 2 Transactions). これに習い多変数デジタル通貨も「三者の同意検証チェーン」として定義される。☞Fig.6 である：左から右へ時間が進む。

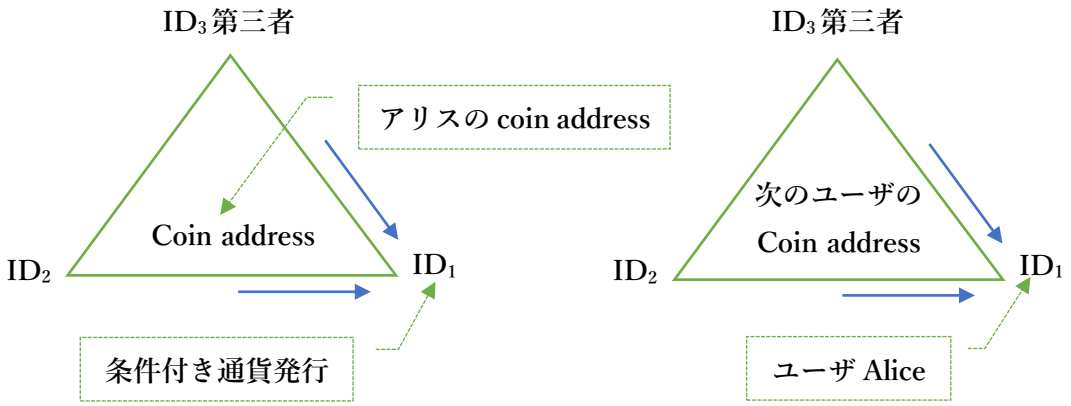


Fig.6: 三者の同意検証チェーン

図の説明：
条件付き通貨発行はアリスのビットコインアドレスに送金する：(左➡右)：アリスは次のユーザのビットコインアドレスに送金する。通貨発行者が中央銀行の場合は、取引所（民間銀行）又は第三者を経由して、消費者アリスにコインを転送するかも知れない。いずれにしても、アリスは所有権チェーンを検証し、次のユーザのビットコインアドレスに送金する。これが条件付き通貨発行のチェーンである。

単一意志が行う署名チェーンと比べて、三者の同意検証チェーンの方が信頼できる、と誰でも直観するだろう。どのくらい信頼度が高いか、計算してみよう。偽コインを創る難易度を計算してみよう。その前に、読者が知りたいことが有るだろう。

現状のブロックチェーンならばCBDCをどのように発行するか？

1）マイニングは貨幣の需要に応えることが不可能。通貨の発行に責任を負う主体が存在しない。これを無理やり市場に出せば、ご存知のように、金融商品になる。

2）中央銀行や国債に信用が有ることを前提に置き、100万円の送金がブロックチェーンに記録されれば、100万円の貨幣を発行したことに成る？そうはならない。なぜなら、100万円に署名をしたKeyデータはもしかしたら、漏えいしたKeyデータであるかも知れない：Keyデータの漏えいには誰も気づけないから、決済フローの履歴を当局が持たねばならない:これが監視社会である。秘密変数n=1の漏えいを止める方法は私のパテントしか無い。☞I節

3）昔は金に銅を混ぜて需要に応えようとした。同じ手口でマイニング解決をしたとして、運用においてはパスワードや生体情報を匿名変数や秘密変数に結合する。その場合、プライバシーを犠牲にした「x xコイン」を貴方は持っていたいと思うだろうか？きっと貴方は両替所に行く。そこで多変数デジタル通貨のアプリで出会えば、迷うことなく、「x xコイン」を投げ売りする。

偽のコイン作りの困難性、圧倒的な信頼と安定力

鍵管理の問題について世界は未だスッキリした解を知らない。では、再び、デジタル通貨の格付けを見ましょう：☞Digital currency rating（☞このリンクはHyper text画面に在る）

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

IDs n=3はPrivate keyデータを燃やした後に残った「灰」であるから、如何なるKey データも関数M()から漏えいしない。 だから読者には贋金を作れない。

では…私が多変数デジタル通貨の贋金を創ってみよう。贋金とは、アリスのkeyデータを奪ってコインを作り、何者かのビットコインアドレスへ送金することである。3ページに衝突関数を紹介した：そこでは多変数デジタル$ID_1 \neq ID_2 \neq ID_3$を衝突関数に入力すると、衝突を起して、出力にkeyデータを再現する。この知識を持つ攻撃者は次のようなシナリオを描く：$ID_1 \neq ID_2 \neq ID_3$のどれか一つの通信路を乗っ取り、任意乱数を流して衝突を起し、その出力データを内側か外側から奪う：

何回攻撃をやれば衝突が起きるか？ 2^{256}回の内、1回は衝突を起し、keyデータを再現する。これは総当たり攻撃である。衝突を起す確率=$1/2^{256}$である。実際、ネットの中で2^{256}回の攻撃が許されるでしょうか？贋金を創るのは大変難しいと思います。

単一の意志が行う決済にはタイムスタンプが必要

従来の署名チェーンは単一の意志で更新するので、タイムスタンプが必要になる。☞Satoshi

Nakamoto [3. Timestamp Server]。同じく銀行オンラインシステムもタイムスタンプで決済を完了する。

他方、三者の同意検証チェーンはそれ自体が非可逆である：次のような理屈である。上記の通り：多変数デジタル通貨の贋金作りの確率は=$1/2^{256}$。この贋金と正規のコインとの区別は無い。次のユーザが贋金から贋金作りに成功する確率は=$(1/2^{256})*(1/2^{256})$である。このチェーン自体はタイムスタンプである：Satoshi Nakamoto [3. Timestamp Server]と同じ理屈である。これだから単一の意志が行う決済よりも信頼できることが判る。

４．多変数デジタル通貨を持っているとボーナスが付く！

ここはボーナス記事だ：記事の内容が民間部門に多変数デジタル通貨を立ち上げる梃子を与える。将来、役に立つ。

我々は多変数デジタル通貨を「三者の同意検証チェーン」であることを見抜いた。この主体は、通貨発行者の単一意志ではなく、通貨発行者と取引所と第三者から構成されるシステムである。ここには署名用の鍵データが実装されていないが、通貨発行者はデジタル署名を実行する。次の効果が期待できる。

今、Alice は銀行口座から私の口座へ送金したと仮定する：それには手数料が徴収される。その手数料を私が負担する；そうすると、私にマイナスのボーナスが付く。

多変数デジタル通貨で送金するならプラスのボーナスが付いて回る。その理由は次の通り：Alice が私に送金する場合、Alice は多変数デジタル通貨を取引所で購入する；その売り手は不特定者であるが、その中には通貨発行者も居る。三者の同意検証チェーンは適正価格を維持する責任を担う。

通貨発行者はルールに従い適正価格を調整し販売する。多変数デジタル通貨を受け取った私は、紙幣に両替するもよし、そのまま持ち続けるのもよし、私の自由だ、私のプライバシーだ。この通貨は私のプライバシーを法制度ではなく数学が保証する：確率論が私の自由を保証している。

私が両替しない場合、多変数デジタル通貨を持ち続ける、ちょうど自宅に保管する紙幣と同じだ：多変数デジタル通貨は紙幣と互換だ。私は受け取った時の価格より上なら売っても良いと思っている：これがボーナスだ。発行主体（三者の同意検証）が居るから、価格の下落や暴騰を制御できる：S&P500 のような、なだらかな値上がりを許容している。

Appendix（☞このリンクは Hyper text 画面に在る）

Swift coin、超儲かる銀行間送金、基軸通貨の未来像

総括

不換紙幣の発行は中央銀行の貸方科目（負債）である。そのメカニズムは中央銀行の単一の意志である。ブロックチェーンのマイニングは単一の意志ではないし、貨幣の需要には応えられない。それだから CBDC はマイニングを放棄し、閉域網で運用する「国内デジタル通貨」になるしかない：小口決済時には消費者に固有の ID を割り当て、パスワードの登録を求める：結果、デジタル人民元と同じく、立派な監視社会の「お金もどき」になる。格付け計算は 0+0=0➡「格付け＝0」になる。☞Digital currency rating（☞このリンクは Hyper text 画面に在る）。「格付け＝0」には致命的な弱みが有る：監視社会の「お金もどき」を人々が買う訳が無い。しかし、民主主義社会において不思議な力を発揮する。

中国人民銀行は法律に基づき、全てのキャッシュレス決済を「見ている」[1]。我が国においてはこういう法制度は無いが、「格付け＝0」CBDC が社会実装されると、監視社会になり、徴税力を背景に「大きな政府」の仕上げに入る。民主主義国にあって、中国共産党の監視社会がこんな風に実現するとは、マジックである。そんな「馬車と馬車の連結ショー」を私は見たくない。私は汽車をみたい。汽車とは「格付け＝5」のデジタル通貨の発行である。☞Digital currency rating（☞このリンクは Hyper text 画面に在る）。

私は Satoshi Nakamoto に敬意を表する：彼は電子コインをデジタル署名のチェーンとして定義し、なおかつ全ての参加者を匿名変数にした。彼の洞察に従い、私は「三者の同意検証チェーン」を定義することが出来た：消費者にパスワードの登録を求めない。最初から終わりまで消費者を匿名変数として扱い、プライバシーを守り、資金洗浄と正常な送金とを分離し、インターネットで運用する。このプログラムにはいかなる鍵データも実装されない。それゆえ、これはブロックチェーンを量子耐性にする決定的な方法論である：また、実装手段である。

終わりに

私は今８０歳の高齢である。いつ終わるか知れない。秒読みに入っているかも知れない。５年以内に発明の全容を全て開示したい、後世のためである。開示業務の期間を５年と見積もり、私の開示業務を買う方を求めることにした。私はお金を「天国」に持って行けないので、契約や奉納金（ライセンス料）は後世への投資に託す。皆さんの国々へ投資する財団を設ける。

開示業務は貴方の事業を推進する力になるだろう。私の開示業務は「実施権の許諾」と「著作権の共有」を含む。又、通貨発行益についての考え方も合意事項に含まれる。

貴方が獲得するライセンスは「私の権利を制限する約束」である。だから私は貴方のビジネスを加速する。後から来る方々には不利になるが、初めに井戸を掘った人が優先されて当然である。ブロックチェーンの利害関係者、エンタープライズ、中央銀行、貴方のフィードバックを待つ。質問も歓迎する。

2020 年 10 月 07 日

©著作者
渡邊栄治
METEORA SYSTEM
eiji-dualcontrol@ozzio.jp
patento-info@meteora.co.jp

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