# ブロックチェーンの運用時に生じる致命的な問題点

問題点１：
公開鍵には量子耐性が無いから、秘密鍵データの計算が可能になる。量子コンピュータの計算力なら他人の暗号資産を盗み、自分の財産にすることができる。
背景：
Satoshi Nakamoto は匿名の公開鍵を情報の流れを断ち切る手段にした。
問題点２：
巨大な計算力を使わず、ハッカーなら直接オンライン上の秘密鍵を盗むことが可能である。
背景：
パスワードはアクセス制限をするが、オンライン秘密鍵の情報の流れを断ち切ることはできない。

## 検証

Satoshi Nakamoto は X.509 証明書を持たない公開鍵を用い、受取人が所有権のチェーンを検証できるようにした。彼の論文から（10. Privacy）を引用する：

> 10. Privacy
> The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: ***by keeping public keys anonymous.*** The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.

下図は「10. Privacy」から引用したNew Privacy Modelである。図中のブルーの文章や線は私が書き加えたものです。公開鍵を匿名にすることに依って、“Identities”から“Public”に至る情報の流れが境界防衛線（ビットコインアドレス）で断ち切られる。

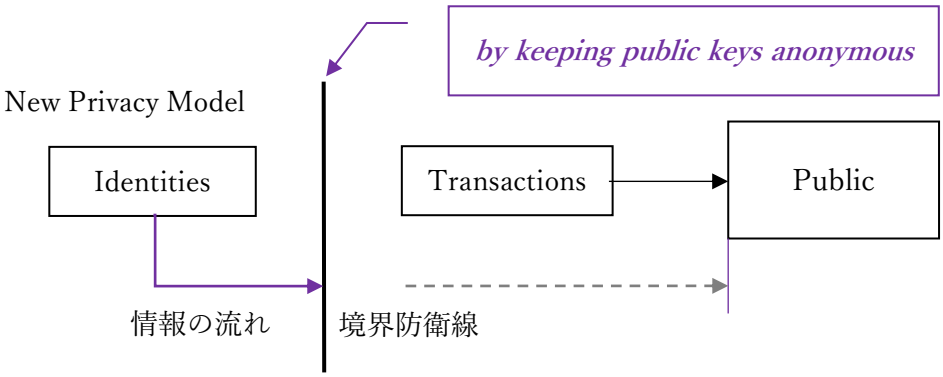


Fig.1: 境界防衛線＝匿名の公開鍵＝ビットコインアドレス

X.509 証明書付き公開鍵の“Identities”は認証局である。X.509 証明書を持たない公開鍵の“Identities”は秘密鍵データである。この“Identities”で受取人は署名を検証して、所有権チェーンを確認できる（電子コインの所有権）。☞Fig.2

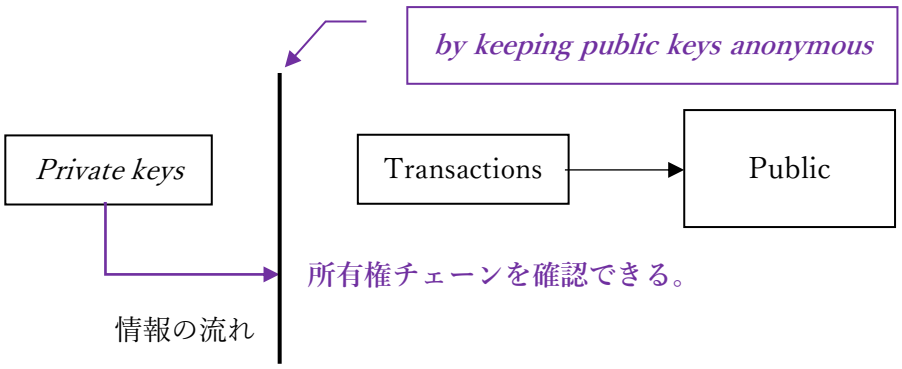


Fig.2: この“Identities”で受取人は署名を検証する。

しかし、電子コインの所有権は次の二つの要因で盗まれる。一つは、公開鍵に量子耐性が無い：もう一つは、オンライン上の秘密鍵データはサイバー攻撃に依り漏洩する。

## 問題点 1 の検証

可換アルゴリズム型の公開鍵には量子耐性が無いことから、Fig.2 は Fig.3 になる。

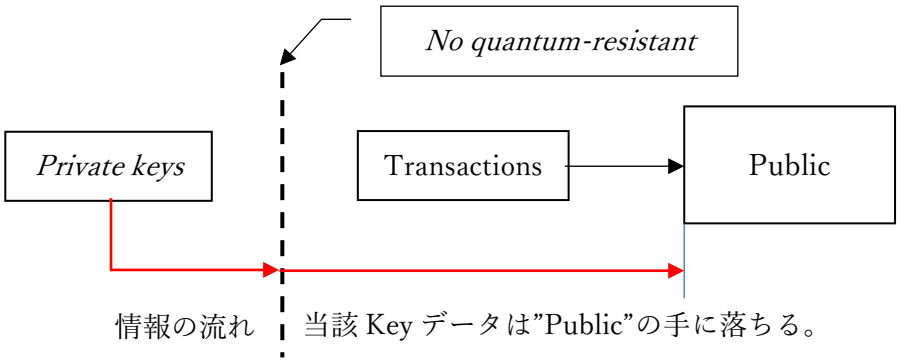


Fig.3: 電子コインの所有権が盗まれる。

## 問題点 2 の検証

ブロックチェーンの運用時に ID パスワードが用いられる。パスワードは元々情報へのアクセスを制限するものであり、情報の流れを切るものではない。深刻なことは、パスワードはその定義自体から情報が洩れること。下図の通り：

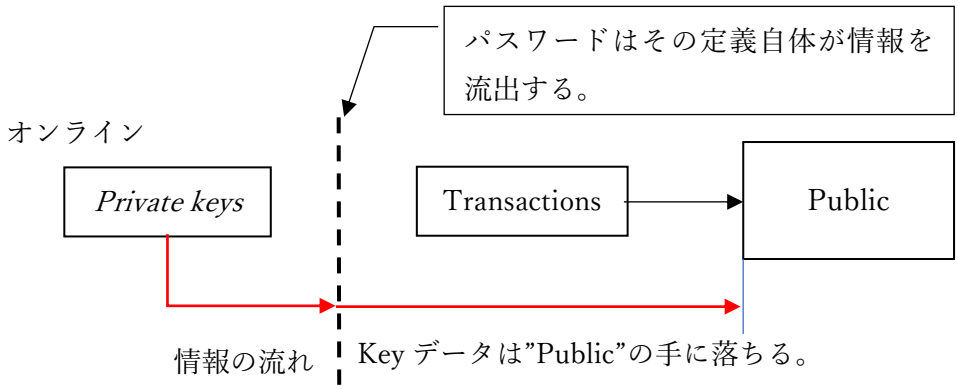


Fig.4: 電子コインの所有権が盗まれる。

## 問題点１＆２の重なる部分

Fig.3 と Fig.4 は「“Private keys”から“Public”に至る情報の流れを断ち切れない」ことにおいて同一であることを表現している。すなわち、Fig.3＝Fig.4。ということは、公開鍵を量子耐性にしたとしても Key データは”Public”の手に落ちることに変わりない。

## 真なる課題は何か？

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登録をサービス提供者が管理する。それですからブロックチェーンにおいても、取引所や証券窓口がユーザのアカウントを管理し、署名用の鍵へのアクセス制限をパスワードが行うことに成る。

しかし、パスワードを用いる限り、鍵の情報の流れを断ち切れない。真なる課題はパスワードを用いないで署名用の鍵を運用することである。この要件を論理的に突き詰めると：*システムはオンラインにもオフラインにも鍵データを持たない一方、署名をする時には鍵データを利用できる。*何と不思議なシナリオではないか。

## 非可換アルゴリズムは上記の不思議なシナリオを実行する。

定義１：

パスワードの登録を求めない。

定義２：

秘密鍵データは生成されると同時に「燃やされる」。

**定義 3：**

**この実装は量子耐性である。**

**上記三つの定義すべてをカバーする現実的なアルゴリズムが有る：非可換アルゴリズムである。この非可換アルゴリズムの形式論を Appendix 1 にメモした。ここに、暗号関数に相当する関数 Y()、及び、復号関数に相当する衝突関数 $Y^{-1}$()を引用し、Satoshi Nakamoto の New Privacy Model に適用する。以下の通り。**

## Private key データが「燃やされる」

**関数 Y()を Private keys に適用して、 keys データを「燃やす」。鍵データがどこにも存在しなくなるので、情報の流れ自体が消える。つまり、アクセスを制限する対象が存在しない。**

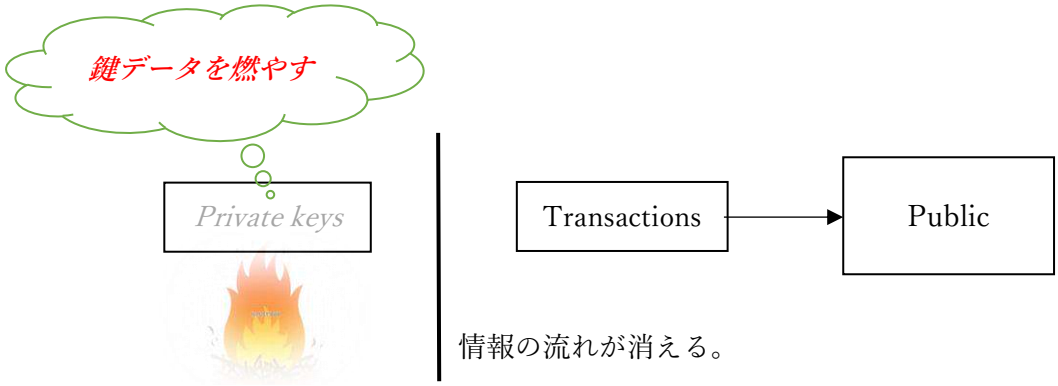


Fig.5: アクセスを制限する対象が存在しない。

**Private key データを燃やした後、関数 Y()の出力にコード ID が 3 個現れる。これで key データはあらゆるメモリから消える一方、署名タスクだけがメモリ残る。Fig.6:のように境界防衛線が左に移る。**

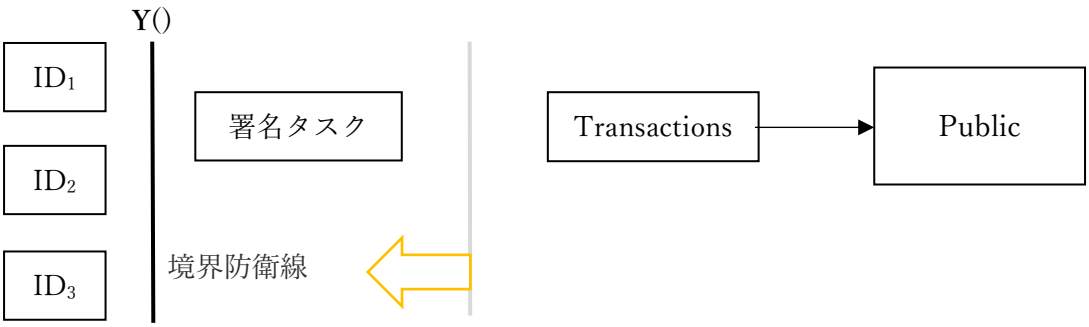


Fig.6: 境界防衛線が左に移る。

上の 3 個のコード{$ID_1$, $ID_2$, $ID_3$}が署名タスクを起動する。

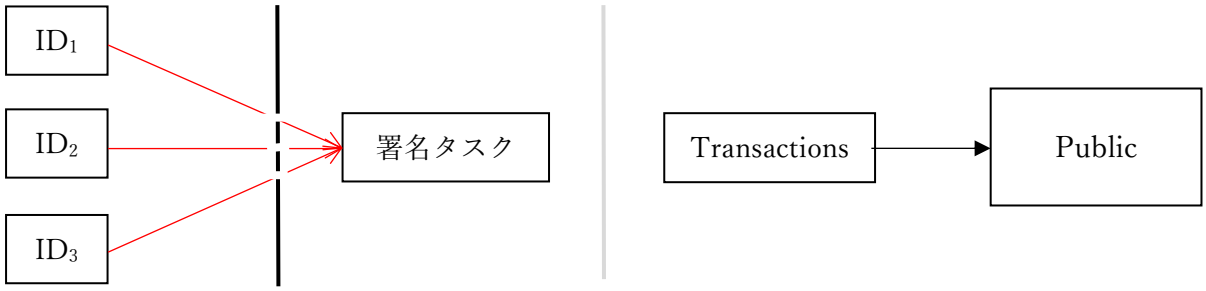


Fig.7: どんなパスワードも存在しない：アカウントも存在しない。

すなわち、ユーザが $ID_1$,を持ち、取引所が $ID_2$ を持し、第三者が $ID_3$ を持つ：ユーザ、取引所、第三者それぞれが署名に同意した時、署名タスクを起動する：署名を実行後、直ちに鍵データは削除される。この辺りの詳細についてホームページの記事に譲る。☞https://meteora-system.com
☞ Multivariable Digital Currencies

## 注目点

常識に依れば、ユーザのアカウントを管理するのはサービス提供者である。それ故、パスワードを用いる限り、鍵の情報の流れを断ち切れない。これがブロックチェーンの運用時に生じる致命的な問題点である。この問題を非可換アルゴリズムが解決する。それはどんなソリューションであるか？

どんなパスワードも存在しない：アカウントも存在しない。敢えて言えば、ユーザと取引所と第三者の合意プロトコルがアカウントである。ID パスワードを保持するような DB が存在しない。この様子を Fig.7 に表現した。

ハッカーは量子コンピュータを駆使して、公開鍵データから秘密鍵データを盗む。秘密鍵データが手に入れば、電子コインを盗むのは容易である。誰もそれを止める者は居ない。しかし、Fig.6 では、鍵データはオンラインに存在しないし、オフラインにも存在しない。署名チェーンを更新する（or 電子コインを盗む）方法は Fig.7 に示す手段に準拠するしか無い。

やっとハッキングした秘密鍵データであるが、Fig.7 に対しては、その使い道が無い。すなわち完璧な量子耐性である。この非可換アルゴリズムには寿命が無い。NIST 標準の成功を待つ理由が無い。

2021 年 01 月 28 日

Appendix1
非可換アルゴリズムは暗号処理 $K_1()$と復号処理 $K_2()$が互換ではない。ここで $K_1$, $K_2$ はどちらも確率変数を表す。平文 P について暗号処理を行うことを $K_1(P)$と表し、次に復号処理を行うことを $K_2(K_1(P))$と表す。ここでは単に $K_1K_2$ と言う表現を用いる。

公開鍵を暗号鍵にして平文 P からコード C を作り、秘密鍵を復号鍵にして平文 P に戻した場合も、その逆の場合も、結果は同じ P に戻る：

$$K_1K_2 = K_2K_1$$

これが可換アルゴリズム。ところが、非可換アルゴリズムでは、イコールの部分が不等号です：

$$K_1K_2 \neq K_2K_1$$

この非可換アルゴリズムにおいては、暗号処理 $K_1()$に相当する関数を Y()で表す：そして Y()は独特な形式で表される：

$$Y() \equiv <Y_1(), Y_2(), Y_3()>$$

この出力に 3 個のコード IDs(n=3)が現れる（Fig.6:)。この内、(n-1)個の IDs が漏洩したとしてその漏洩 IDs から秘密情報を計算するのは難しい：なぜなら、計算は確率計算になり、秘密情報に当たる確率は $1/2^{256}$ です。これは量子コンピュータの内部ではなく、ネットでサイコロ投げを $2^{256}$ 回も行う計算です。一方、復号処理 $K_2()$に相当する関数として「衝突関数」と名付けられた関数が有る。これも独特な形式 $Y^{-1}()$で表される：

$$Y^{-1}() \equiv <Y_1^{-1}(), Y_2^{-1}(), Y_3^{-1}()>$$

このように、公開鍵に相当する鍵は無い。ただ、公開鍵に代わる利便性として、(n-1)個のコード IDs が漏洩したとしても、衝突関数 $Y^{-1}()$の計算を騙せない。衝突という事象そのものが総当たり攻撃を想定したものだから騙せない。**この意味で衝突関数 $Y^{-1}()$は公開鍵に相当する。同じく関数 Y()が秘密鍵に相当する。これが非可換アルゴリズムの存在と特色を示している。**

関数 Y()と $Y^{-1}()$をサーバに収納するモデルが有る。この場合は Static 関数である。ブロックチェーンに適用する場合、関数 Y()**が** One-time に使用される一方、衝突関数 $Y^{-1}()$に使用回数の制限は無い。$K_1K_2 \neq K_2K_1$ を $K_1K_2 - K_2K_1 = \Delta$ と表すと、これは量子力学の形式である。
//