スマートコントラクト
人類が夢見たブロックチェーンの理想を実現する

＜はじめに＞

昨年１月５日、仮想通貨に関わる人々にとって、衝撃的なニュースが流れた。最も起こり得ないとされていた「51%攻撃」が仮想通貨の本流のひとつである「イーサリアムクラッシック」に対して行われたという。イーサリアムはビットコインと並ぶ仮想通貨の中でも重要なコインであり、イーサリアムクラッシックはイーサリアムがフォークする元となったコインである。発表当初から、スマートコントラクトという、仮想通貨以外の価値の移動などの応用も考慮され、大変注目されていた。最近は仮想通貨に対しては懐疑的でも、仮想通貨以外のブロックチェーン技術の応用は何ら問題なく、人類の新しい未来を約束する技術であると考えていた人が多く、ブロックチェーンの崩壊を決定的にしたこの攻撃に、関係者の動揺は大きかった。

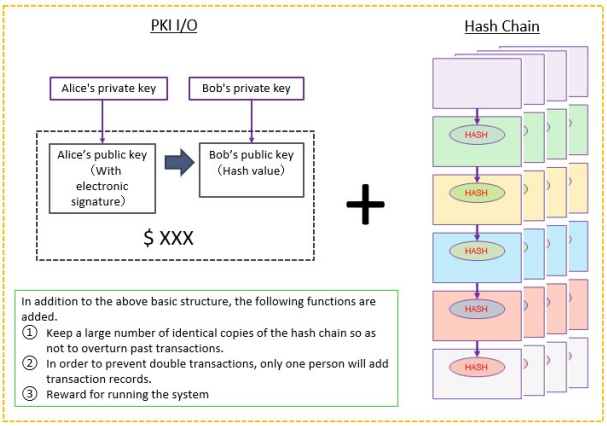
イーサリアム系だけではない。より規模の大きいビットコイン系でも、比較的小さい各種ブロックチェーンでも「51%攻撃」は度々報告されている。

ブロックチェーンの崩壊で人類が一度は夢見た未来は消え去ってしまうのだろうか？

＜ブロックチェーンの真実と 51%攻撃＞

ここでブロックチェーンについて総括する。ここでは合意形成を行う本格的なブロックチェーンのみを扱い、プライベートブロックチェーンと呼ばれる合意形成を全く又は一部しか行わない特殊なものは扱わない。

ブロックチェーンは、全ての参加者が所有するハッシュチェーン（改竄検知と反対方向計算不可という特徴を持つ）を利用するデータ保存部分と、PKS（公開鍵暗号方式）を利用する入出力部分から成る。さらに以上の基本構造に加え、マイニングと呼ばれる以下の合意形成の機能を追加したものである。



a. 過去の取引を覆されないようにするため、多数の台帳を、少なくとも過半数を正確に同一に保ちつつ常に更新する。
b. 二重取引を防止するため、取引情報の追加は１度に、フェアに決定される１人だけが行う。
c. システムを稼働させ続けるために報酬を与える。

その結果、中央集権的な存在に依存することなく、改竄困難な台帳（データベース）を作成できる上に、合意形成をフェアに行うことができるシステムとして評価されてきた。

ところが、ブロックチェーンには以下のような多くの問題が指摘されてきた。

a. 台帳（ブロックチェーン）を使うので、仮想通貨の中にはコインと呼ばれるものが多いが、貨幣ではないので即時決済はできない。とはいえ、銀行振り込みと同様、時間をかけての送金には使える。
b. 台帳（ブロックチェーン）が 200 ギガバイトを超えるものが出てきており、日々増え続ける取引量からいずれ修正を余儀なくされる可能性が出てきた。
c. 巨大な台帳（ブロックチェーン）の共有には、ファイル共有 P2P 方式では「データが抜ける」可能性

があるので、現在は全複製をしたあとの稼働としている。

d. その結果、同一台帳の維持に莫大な通信量及び電気量が必要で、多数の巨大台帳の維持が困難になりつつある。
e. マイニングに見合う報酬が得られ続けるかどうか疑問視され始め、マイニングを止める業者が出現しつつある。実際にブロックチェーンが事実上停止したコインも存在する。
f. Wallet または預け先からプライベートキーを紛失しまたは盗まれる。
g. 必ずしも公開鍵方式だからというわけではないが、秘密鍵のみによって管理されるのは本方式の弱点であり、秘密鍵を悪用する多くの事件が発生している。
h. 入出力時に PKS を使用するので、中間者攻撃（man-in-the-middle-attack、MITMA）により取引内容が改竄される。
i. 意見の相違で、容易にフォークが起きる。旧コインと混ざらないような対策を施し（リプレイ攻撃対策）、台帳を全部変更すれば、別のコイン（フォークコイン）となり得る。
j. 取引がないのにブロックを追加する、空マイニングができる。

これらに加えて、ほとんど可能性はないと考えられていたとは言え、51%攻撃の可能性が以前より指摘されていた。ブロックチェーンは、分散台帳と誤った説明をされることが多いが実体は、1 つの台帳の各部分を多数人で分担して保持する一般的な分散台帳ではなく、同一内容の台帳が複数存在する同一台帳多数複製型といったほうが的確なものである。ブロックチェーンはデータ保存にハッシュチェーンを使っているので改竄はほぼ不可能である。しかし、この台帳全体を偽物にすり替えられてしまうと、改竄は成功してしまう。そこでブロックチェーンでは、同一台帳を多数複製することで、台帳全体の改竄を困難にしていた。多数の台帳の内容に齟齬がある場合において真正な台帳を多数決で決定するとした場合、台帳全体をすり替えるとしても多数の同一台帳の過半数をすり替えないと改竄したことにはならない。それゆえこの攻撃は 51%攻撃と呼ばれる。ビットコインの場合では 1000 万台を超えるノードそれぞれに保存された台帳の 51%をすり替えるなど到底不可能との前提に基づき、まさかこの攻撃が成功するとは考えられていなかったのである。
ナカモトサトシと名乗る著者がブロックチェーン及びビットコインを提案した論文「ビットコイン：P2P 電子マネーシステム」でも以下の通り、このブロックチェーンが多数決を基本とすることが強調されている。

ビットコイン：P2P電子マネーシステム

ナカモトサトシ

1.イントロダクション
この論文では、時系列取引のコンピュータ的証明を作成するP2P分散型タイムスタンプ・サーバーを用いた、二重支払い問題の解決策を提案する。本システムは、良心的なノードが集合的に、攻撃者グループのノードを上回るCPUパワーをコントロールしている限り安全である。

12. 結論
本論文では、信用に依存しない電子取引のシステムを提案した。電子署名で作られるコインという従来通りのフレームワークは所有権を強くコントロールを実現できるが、二重支払い防止対策なしには不完全である。その解決策として、良心的なノードがCPUパワーの過半数をコントロールする限り、プルーフ・オブ・ワークを使って記録された公開型の取引履歴を攻撃者が変えようとすることが、コンピュータ的に加速度的に実質上実行不可能になっていくP2Pネットワークを提案した。

実は、ブロックチェーンの場合、51%の支配権を確立すれば、付け加えられる新しいブロックを自分に都合

の良い内容のブロックにすることができるので、台帳全部をすり替える必要はなく、事実と異なる台帳を作ることのハードルは比較的低い。

＜人類が夢見たブロックチェーンを再考察する＞

脆弱な暗号技術に因るが故に盗難が頻発し、同一の巨大な台帳維持が困難になり、莫大な電気と通信量を必要とするバベルの塔と化しても、ブロックチェーンとコインによって作り出される未来図はまだその魅力を失っていない。中央管理を不要とし、取引終了後当事者の了解なしに勝手に改竄されることがなく、当事者が求めればいつでも台帳の内容をチェックできるという特徴からブロックチェーンは依然注目を集めている。中央集権的でなく、自分たちだけで作ることができるシステムこそが未来社会を形作る基盤になるという、一種の思想が生まれ、問題が山積する現代の一筋の光明とさえ考えられ始めている。

政府が管理する土地台帳（登記簿）を考えてみよう。土地は登記されて初めて所有者が明確になり、法律上の効果が生じる。しかし土地台帳が正しく記載されているかどうかは別の話である。間違った登記がなされた可能性は排除できないし、土地移転の後いつも速やかに登記されるわけではない。地面師等による登記簿の偽造や不正な登記簿改竄もしばしば問題になっている。独裁政権では、突然政府の命令によって台帳が書き換えられるリスクもある。間違った登記がされることを防ぐには、当事者が求めればいつでも内容をチェックでき、訂正できることが必要である。また、独裁政権に対しては、中央管理を不要とし、取引終了後当事者の了解なしに勝手に改竄されることがない仕組みとすればよい。現時点の本当の所有者が必ずしも登記されていない問題については、登記と所有権に関する別の法律が必要であろう。例えば、相続発生後１年以内に登記が行われなければ、その土地は政府の管理下に置かれるなど、実際の運用に則した決め事が重要になる。その上で、当事者が求めればいつでも内容をチェックできるようにすれば、この問題も改善できる。これらの問題を一挙に解決するものこそ、中央管理を不要とし、取引終了後当事者の了解なしに勝手に改竄されることがなく、当事者が求めればいつでも内容をチェックできる技術である。人類はその決定版としてブロックチェーンに夢を託そうとした。ブロックチェーンの参加者全員が互いに監視し合うことで、勝手な改竄を防ごうというのである。

このネット時代の基盤技術は、以下の３つの特長を具備しなければならない。

何らかの契約が締結された場合、

① 非中央管理：中央管理なしに、真のすべての契約当事者（関係者）だけで契約を締結できること。

② 真正性保証：すべての当事者の合意なしに改竄できず、
かつ、当事者全員の合意があればいつでも契約内容を確認できること。

③ 存在性証明：締結した契約が、少なくとも１つ確実に存在することを保証できること。

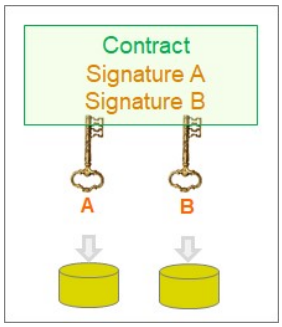
ブロックチェーンは、公開鍵暗号技術で参加者を遠隔認証できるうえ、参加者全員で台帳を管理するので中央管理は不要で、大量のハッシュチェーンを利用することで台帳の改竄を防止する。参加者全員が同じ台帳を持っていることがシステム的に保障されているので、自分の台帳を確認すればいつでも契約内容と契約が少なくとも１つ確実に存在することをチェックできる。上記の特長を有するまさに人類が長く求めてきた技術のはずだった。

しかし実際は、公開鍵暗号を使うので中間者攻撃に弱く（ネットを介しての遠隔認証ができない）、参加者全員で大量の同一台帳を維持することは物理的限界があり（非中央集権管理できず）、台帳が巨大すぎ、かつ参加者が匿名なので内容をチェックすることは困難であることが分かってきた。その上、今年になってもっともあり得ない攻撃（51%攻撃）が実際に起こったことで、ブロックチェーン技術への信頼は完全に揺らいだ。

さらに、非中央管理ということだけで、民主的と考えられてきたが、中国が人民元のデジタル化を、全てを記録し監視できるという特徴を持つブロックチェーンを使って実現しようとしたことで、自由とは真逆で民主的とはとても言えない仕組みであることが徐々に明らかになってきた。

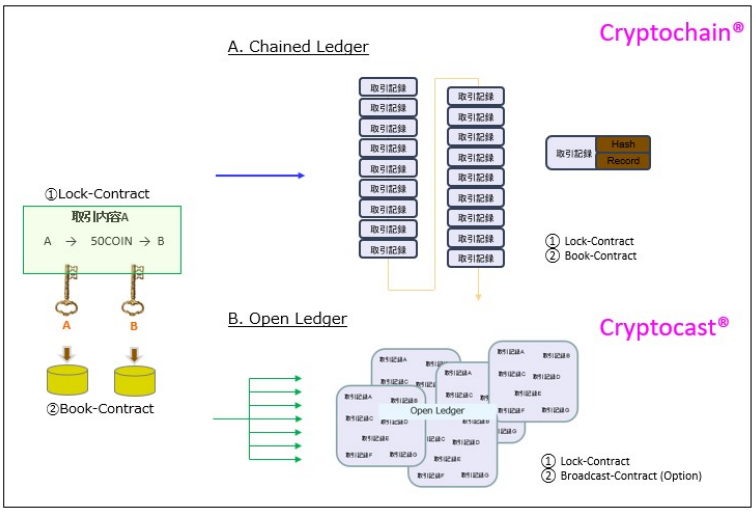
＜人類が夢見たブロックチェーンの理想を実現する＞

実は、①非中央管理、②真正性保証、③存在性証明の 3 つの特長を満たす基盤技術は、適切な暗号技術（コンプリートサイファー）を用いれば、はるかに簡便な方法で実現できる。



まず、A、B の 2 者の間で交わされる契約書を考える。互いの面前で契約書に署名捺印し例えば PDF ファイルにしたあと、A の持つ暗号鍵 A と B の持つ暗号鍵 B によって暗号化する。順番はどちらでもよい。この両方の鍵で暗号化されたファイルをクリプトプルーフ®（CryptoProof®）と呼び、それぞれが複製を一部ずつ保管する。このクリプトプルーフ®の存在により、契約書は少なくとも 1 つ確実に存在することを保証できる（③）。このクリプトプルーフは、両者の鍵を共に用いなければ復号化できないため、どちらか片方による改竄はできず、第三者も改竄できない（②）。また 2 人の当事者のみによって管理され中央管理者はいない（①）。A と B が再び各自の暗号鍵で暗号化した時と逆順で復号化すれば、元の契約書をいつでも確認できる（②）。その上、契約書は必ず暗号化された状態で保管されるので、取引内容は 2 人の当事者の許可なく決して外部に漏洩しない。これは従来のブロックチェーンにない特長である。最後に、面前で署名捺印、暗号化できない場合は、コンプリートサイファーを用いて、その Remote Synchronization 機能により互いに遠隔認証を行った（①）うえで、暗号通信環境下で、契約書に署名捺印して PDF 化したあと、両者の暗号鍵によって暗号化する。以上の方法を用いれば、ブロックチェーンで果たせなかった夢は、容易に実現できる。尚、クリプトプルーフ®においては、暗号化を行うのは当事者に限定されず、弁護士や公証人の暗号鍵を用いて、更に暗号化を行うこともできる。

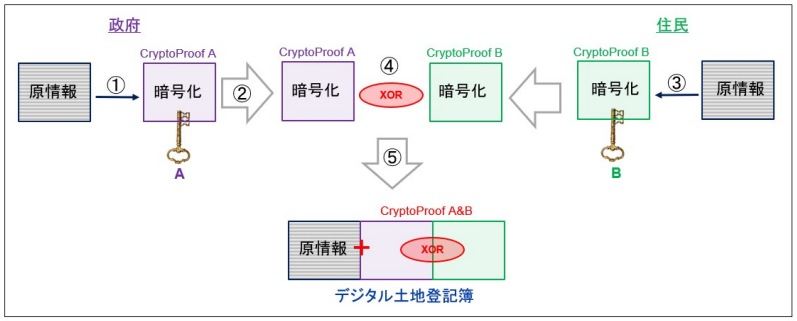
ところが、契約の関係者が、署名捺印する当事者以外に存在する場合がある。会社代表と労働組合長が、その他の従業員の給与を決める場合などである。このケースでは、会社代表と労働組合長が結託すれば、他の従業員の給与額を契約後も自由に変更できる可能性が残ってしまう。しかし、改竄不可能な台帳に記帳してあれば、このようなことは起こらない。そこでこのようなケースに限って、両者の暗号鍵で暗号化したファイルを、従業員もアクセスできるハッシュチェーンに繋ぐことで、変更を不可能にする。この方式を「クリプトチェーン®（CryptoChain®）」と呼ぶ。しかし、このハッシュチェーン台帳を管理するのはブロックチェーンほどではないにしろ煩雑である。そこで新たに考案されたのが、「クリプトキャスト®（CryptoCast®）」である。特定のハッシュチェーンに繋ぐ（記帳する）代わりに、インターネットにブロードキャスティングする。文字通りインターネットに対し放送する（ネット上に拡散する）ことで、暗号化した契約書がインターネットのどこかに存在することとなり、代表と組合長が結託して改竄しても、ネット上の証拠と突き合わせれば、改竄の事実がばれるようにすることができるの



である。クリプトキャスト®された契約を保管する事業もあり得る。
このように、人類がブロックチェーンを通してみた夢は、クリプトプルーフ®に加えて、クリプトチェーン®、または、クリプトキャスト®を用いれば実現できる。

＜政府提供の情報管理の非中央集権化＞

次に非中央集権的運用について考察する。上記のように少数の関係者しかいない場合は誰でも上記のような方法で当事者だけで契約を締結できるので、全く非中央集権的な管理ができる。



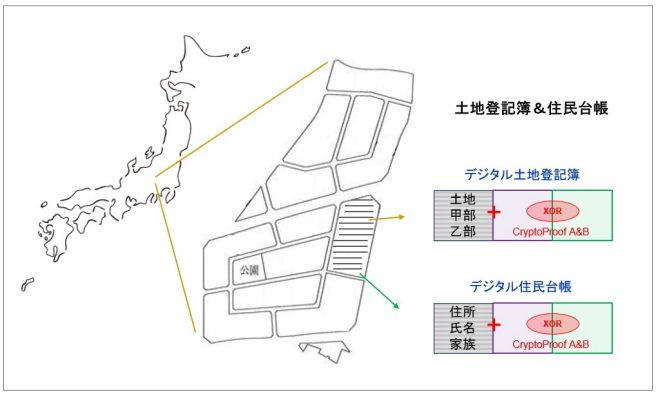
しかし、現在政府が管理する土地登記簿の場合はどうであろうか？政府(法務局)が管理する土地登記簿(住民が所有する場合)では、登記の関係者は政府及び住民（土地所有者）となり、立場は政府(法務局)の方が圧倒的に強く、必要なら勝手に内容を変更できるので、一見民主的でないと考えられがちである。

そこで右の図のように、クリプトプルーフ®技術を用いて、以下の手順で作成するデジタル土地登記簿について考察する。

① 政府は、住民Bの土地の所在・地番・地目・地積や、所有者に関する事項、所有権・抵当権などの原情報を政府の鍵Aで暗号化してCryptoProof Aを作る
（※原情報のハッシュ値を計算してから暗号化すれば小さいCryptoProof Aを作ることができる）
② 政府は、CryptoProof Aを住民Bに提供する
③ 住民Bは、住民Bの土地の原情報を住民Bの鍵Bで暗号化してCryptoProof Bを作る
（※原情報のハッシュ値を計算してから暗号化すれば小さいCryptoProof Bを作ることができる）
④ 住民Bは、 CryptoProof AとCryptoProof Bを用いてXOR演算を行い、CryptoProof A&Bを作る
⑤ CryptoProof A&Bに原情報を繋いで、デジタル土地登記簿が完成する
⑥ デジタル土地登記簿を両者で保存するとともに、台帳として公開する

その上で、クリプトチェーン®、または、クリプトキャスト®を用いれば、デジタル土地登記簿の改竄は不可能になる。政府は自身のCryptoProof Aを使ってXOR演算を行えばいつでも住民BのCryptoProof Bを得ることができる。また反対に、住民 B は自身の CryptoProof B を使って XOR 演算を行えばいつでも政府のCryptoProof A を得ることができるので、万一デジタル土地登記簿が変更されていた場合には、政府または住民のどちらが変更したのか明らかにできる。原情報にCryptoProof A&Bというクリプトプルーフ®がつながるので、この方法をクリプトプルーフチェーン®（CryptoProofChain®）と呼ぶ。

今後、土地登記簿と共に住民台帳を非中央集権的に管理・更新・維持するために、ネット上に公開された国土地理院発行の原地図上に、土地の所有者が原土地登記簿に記される土地の測量情報をこの原地図に反映させた上で、政府がデジタル土地登記簿及びデジタル住民台帳を加えれば、土地区画をクリックするといつでもデジタル土地登記簿及びデジタル住民台帳を表示できるようになる。このように将来は、政府の発行する地図上にクリプトプルーフ®とクリプトチェーン®



技術を応用して、改竄できない土地登記簿と住民台帳を作成し、新しく土地を購入したい人などの利用者に、常に不正に改竄されていない真正の情報を提供できるようになる。

＜まとめ＞

2019 年、ブロックチェーンは崩壊した。人類が夢見た①非中央管理、②真正性保証、③存在性証明の 3 つの特長を有する理想のスマートコントラクトもまた一時可能性がなくなったかに見えた。

ところが、コンプリートサイファー（完全暗号）を用いれば、はるかに簡便な方法で実現できることを考察した。今後人工知能や量子コンピュータと共に、コンプリートサイファー（完全暗号）は、世の中を変えていく原動力となり、デジタルで価値の認証や移動を可能にする時代を招来する。