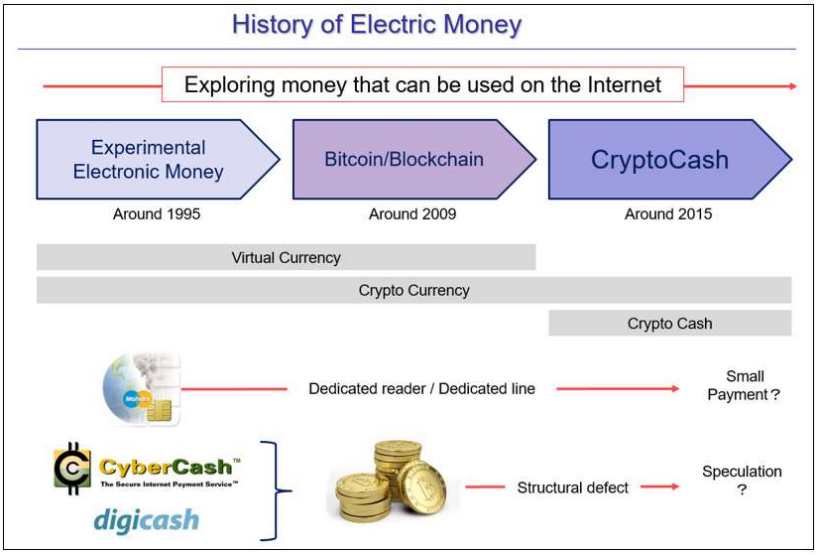
ブロックチェーンを超えて
貨幣の進化

＜はじめに＞

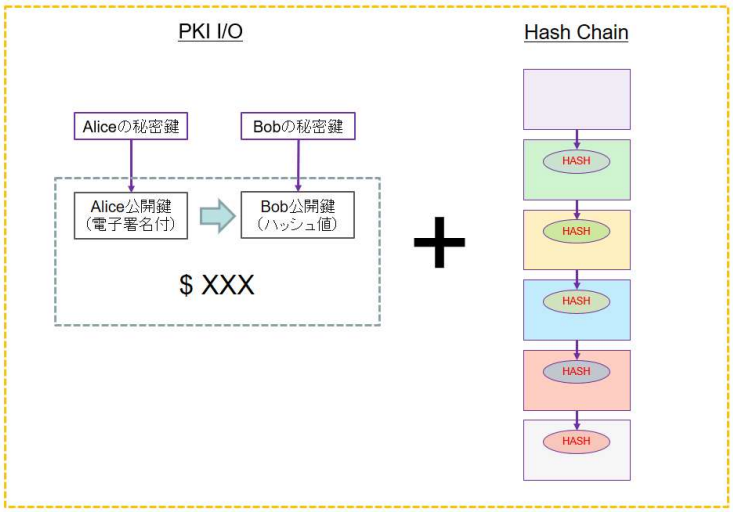
古来人類は、「決済手段」、「価値の保蔵手段」、「価値尺度」の 3 つの機能を持つ貨幣を発明することで、部族を超えて、大陸を超えて、巨大な経済を発展させてきた。美しい貝殻を、巨石を、貴金属を媒体とし、近代においては信用を礎とした持ち運びにも便利な紙幣を発行した。偽造貨幣の弊害が広く認知される中、いよいよその最終形といわれる暗号貨幣がその片鱗を現しつつある。

1960 年代に発明されたインターネットは、1990 年代に商用利用可能となり、1993 年に World Wide Web（WWW）※1 と最初のブラウザーである Mosaic※2 の利用が解放された。続く 1995 年に世界中で最も多くの人々が使用する MS-DOS が Windows95 にアップグレードされると、インターネット上での商取引が爆発的に増加することを見越した多くの先駆者たちが、今度はインターネットで使用できる貨幣（価値を持つ疑似有体物としてのデータ）の発明に乗り出した。1995 年までには百を超える新しいアイデアが紹介され、そして事業化された。しかし新しい世紀を迎えることができた事業は 1 つもなかった。まだ貨幣を作れるほど暗号技術は成熟していなかったのである。人類は真の暗号貨幣の出現のために、暗号技術の完成を待つこととなった。

20 世紀最後の年、すでに脆弱性が見過ごせないレベルに達した暗号技術の新しい標準※3 が決められたが、それでも暗号貨幣を創造できるレベルには届かなかった。ところが、2009 年、人類への寄与などとは全く異なる目的のために、90 年代の技術を使い、従って大きな脆弱性を包含する前近代的な実験的試みが紹介された。貨幣自体を創造することを放棄し、プライドの高い 90 年代の研究者にとってはタブーとされた台帳方式という苦肉の策を用いた。これがブロックチェーンを用いるビットコインであり、一般には暗号貨幣ではなく暗号通貨の変種と考えられている。古典的な貨幣はその交換と同時に決済を完結する。いちいち記帳の必要はない。一方ビットコインは記帳した台帳の正確性にその価値が依存する。したがってこの台帳をいかに正確に記帳・保持するかだけが重要で、正確な台帳維持のためには、即時決済は犠牲にされ、一旦終了した決済自体が覆されることもある。このように不完全な仕組ながら暗号通貨を全世界に知らしめた功績は大きかったが、2017 年 8 月に筆者がサンフランシスコにて行ったブロックチェーン崩壊の講演から間もなく、翌月の中国をはじめとして各国がビットコインを禁止することで、壮大な実験は終焉を迎えた。



＜ブロックチェーン（Blockchain）とは＞



ブロックチェーンは、ハッシュチェーンを利用するデータ保存部分と、PKS（公開鍵方式暗号）を利用する入出力部分から成る。ハッシュチェーンとは、あるデータの塊のハッシュ値を計算し、次のデータの塊の一部とし、これを繰り返すことで連続するデータ塊列を作成し、途中からまたは反対からの改竄が不可能なデータベースを作る古くからある技術をいう。

ブロックチェーンは、以上の基本構造に加え、以下の機能を追加したものである。

① 過去の取引を覆されないようにするため、ハッシュチェーンの大量の同一コピーを常に更新する。

② 二重取引を防止するため、取引情報の追加は 1 度に 1 人だけが行う。

③ システムを稼働するために報酬を与える。

ちなみに、ここで用いられるハッシュ関数は、あるデータが与えられた場合にそのデータを固定長の数値に変換する関数で、以下のような特徴を持つ。

① どんな大きさのファイルもすべて固定長の数値に変換される。

② 同じデータからは必ず同じハッシュ値が得られ、少しでも異なるデータから得られるハッシュ値は全く異なるものになる。

③ 変換は一方向であり、ハッシュ値から元のデータを導き出すことは不可能である。

ハッシュ関数は、例えば、電子署名では、署名対象の容量削減と改竄検知にハッシュ関数が用いられ、またインターネットの標準プロトコルである TCP では、通信データの欠落を確認するチェックサムに用いられている。

＜仮想通貨を支えるブロックチェーンの崩壊＞

ブロックチェーンは、中央管理者がいなくても機能する改竄不能な記帳システムとして注目されてきた。ときに分散台帳と説明されることがあるが、実態は 1 つの台帳を分散して構成する分散台帳ではなく、同一内容の台帳が複数存在する多数同一複製台帳である。改竄をできなくするには、台帳自体を改竄できないようにしなければならない。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。しかしこれだけでは不十分である。台帳全体を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、台帳全体の改竄も不可能にするという。それでも、取引自体をある時点以降からなかったことにするブロックチェーンの巻き戻しやブロック追加時間を利用する攻撃などの問題が報告されている。

そもそもこのように多数複製が必要となってしまったのは、取引の 1 つ 1 つが台帳に記録されて初めて有効となるため、すべての過去の取引を調べることでしか、現在の状況を証することができないという、台帳方式最大の欠陥に起因する。

その結果、現在このブロックチェーンについて、以下のような内部問題が報告されている。

① 台帳（ブロックチェーン）が 100 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。

② 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、現在は全複製を基本としている。
③ その結果、同一台帳の複製に莫大な通信量及び電気量が必要で、多数の複製台帳の維持が困難になりつつある。
④ 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。
⑤ 日々の取引記帳だけでも莫大な電気量、通信量が必要となっている。

一方、ブロックチェーンへの読み書きを担う公開鍵方式に起因する事件（外部攻撃）は大別して以下のとおり 3 つある。

① Wallet または預け先からプライベートキーを紛失または盗まれる。
② 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。
③ 中間者攻撃（man-in-the-middle-attack、MITMA）により取引内容が改竄される※4。

さらに最近は、運用にかかわる大問題が指摘されている。

① 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）、台帳を全部消せば、別のコイン（フォークコイン）となり得る。
② 空マイニングできる。

取引情報を記録するためには、取引数が一定量たまった段階で「マイニング」が行われるが、取引がほとんどない状況では、取引が記録されるために膨大な時間がかかる場合がある。これを避けるため、決められた時間が経過すると取引数が十分でなくてもマイニングが行われることがある。これを「空マイニング」という。その結果、必要量を大幅に上回る大量のコインが出回ることになり、コイン自体の価値を損なう。

このように多くの問題が指摘される現在でも、暗号通貨（Crypto Currency）への熱気は続いている。世界各国が規制を強める中、厳格な基準をクリアした新たなコインが続々と生まれている。これまで各国政府ないし政府公認の銀行だけが発行してきた貨幣を、民間が発行し民間が管理する。中央管理者は存在せず、参加者全てが対等に貨幣の恩恵を受けると同時に責任を持つ。このブロックチェーンという実験の理想の部分が今も人々の心を突き動かしている。脆弱な暗号技術に因るが故に盗難が頻発し、巨大な台帳の大量複製が困難になり、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。必要なのは、人類が 1990 年代に夢見た台帳を必要としない暗号貨幣（Crypto Cash）であり、これを可能ならしめる暗号技術なのである。

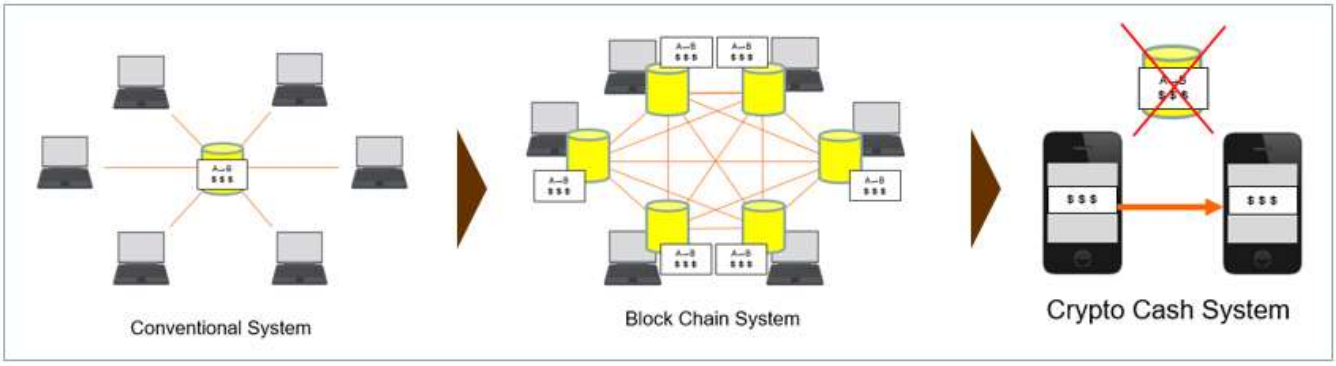
＜暗号貨幣（Crypto Cash）とは＞

世界最初の暗号貨幣である“Crypto Cash”は、価値の交換を行う際に交換される代替物としての疑似有体物（或いは実体）として記号列を用いる貨幣であり、暗号技術の完成とともに、法定通貨を発行する基本技術として世界で初めて開発された。貨幣の発行者情報や価値情報は、完全暗号化した記号列と一意対応するので、改竄、偽造、偽使用を不可能にする。また、信用情報、使用条件、利息、期限などの条件も合わせて暗号化することで、様々な機能を持つ暗号貨幣を作ることができる。記録媒体を問わないので、電子的に送信／保存することが想定され易いが、金属に刻印されたり、紙に印刷されたりすれば、暗号金属貨幣や暗号紙幣として使用することも可能である。従来の貨幣と同様、記号列という実体を持つので、実体のある貨幣として、「決済手段」、「価値の保蔵手段」、「価値尺度」の 3 つの基本機能を有する。

Crypto Cash は、金属や紙をベースとした通貨と同様、国家の信用をベースにした法定通貨としても、他の法定通貨との兌換券としても発行され得るが、香港などの法定紙幣のように、銀行やグローバル企業などの発行者または発行グループの信用で発行されてもよい。また信頼の保証として、金や銀などの貴金属だけでなく、天然資源の価値を担保として発行されることも考えられている。

そもそも貨幣は、間接的に価値の交換ができる代替物であるので、価値の交換の最小単位である二者の間で、コンセンサスが取れれば十分であり、お互いが信用する価値（または信用）または価値の保管者（または信用の提供者）が保証する価値と、一意対応する代替物を交換することで、価値の交換を行うことを可能とする。そのため現在の通貨のほとんどは、予め発行量とスケジュールを決めて発行し、一般には国或いは中央銀行が貨幣を保管・管理しながら市場に流通させる。暗号貨幣の場合は代替物が暗号化された記号列というだけで従来の貨幣と何も変わらない。偽造、偽使用ができない上に、媒体を選ばないという従来にない特長をもつ、より優れた代替物である。Crypto Cash は通常、法定通貨として、国の信用（国力）に加えて、既発行の法定通貨や資源を担保として発行される。

下図に示すように、従来中央集権的に中央のサーバ通貨情報などのすべてのデータを保管、計算、管理していたが、ブロックチェーンの出現により、すべてのノードがすべてのデータを複製所有する一見すると対等に見えるシステムに進化した。しかし、前述の通り脆弱な暗号技術と原理的な欠陥により崩壊寸前である。一方、Crypto Cash は、1 対 1 の価値交換システムであり、すべての Cash は台帳を必要としない。現在の現金と同様、財布から直接お金を出して渡すことで価値の移転が行われるのである。



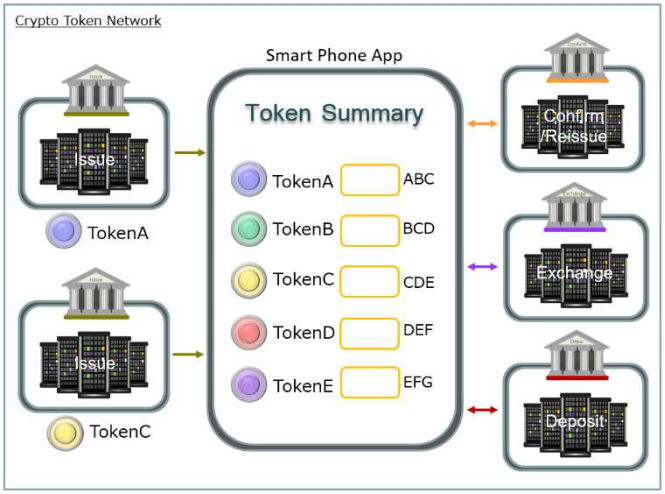
＜現在のコインと ICO＞

そもそもビットコインは実験的試みとして、この試みに参加するすべての人々のコミュニティの中で価値を認められ成長してきた。現在では、時価総額 1 兆円を超えるコインだけでも（2018 年 2 月 25 日時点／1 ドル=107 円換算)、ビットコイン（BTC)、イーサリアム（ETH)、リップル（XRP)、ビットコインキャッシュ（BCH)、ライトコイン（LTC）の 5 つがあり、1600 以上のコインが報告されている。

時価総額最大のビットコインを例にとると、余分な手数料を必要とし、取引記録に 10 分以上もの時間がかかるので実際的ではないものの、理論的には決済が可能ということで、「通貨のようなもの」として扱われることもある。しかし、「決済手段」、「価値の保蔵手段」、「価値尺度」の 3 つの機能を考えると、決済機能としては不十分で、他の法定通貨との相対価値は乱高下し価値の尺度とはならず、その結果保蔵手段としても危ういと考えられ、決して通貨とは認められていない。多くの国ではコモディティ（先物取引の対象となる商品）と見做されている。ところが、他のコミュニティの認める通貨との間における価値の乱高下が投機の対象として、想定外の人気となった。保蔵手段というよりも、持っているだけで価値が上がる投機の対象そのものとして買われたのである。しかしそれも 2017 年 9 月に中国が禁止すると、それまでほとんどの交

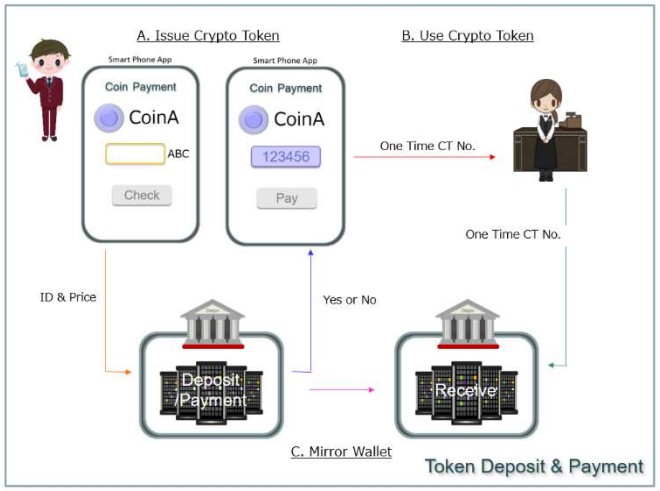
換貨幣であった中国元によってビットコインを入手していた両替屋（取引所）が慌てて、翌年１月にかけて自己所有分を仕手戦を仕掛けてすべて放出し、日本円で入手した一般の投機家の手に移り順調に値を下げ、現在は小康状態を保っている。
参加するメンバーのコミュニティの中だけで価値があるもの、それがコインである。地域であれ、会社であれ、ボランティアサークルであれ、誰でも発行できる。あるコミュニティにとって価値があっても他のコミュニティにとっては必ずしも価値があるとは限らない。コミュニティの垣根を超えたそれぞれのコインの交換は、現在のところコミュニティの相場に対する力関係のみによると推測され、何の根拠も見られない。
このように様々なコインが発行されてきたが、このコイン発行という行為が会社の株式公開に近いと考える人が現れ始め、ICO（Initial Coin Offering）と呼ばれるようになった頃から、会社や団体のための資金調達の手段として利用されることが多くなった。この新しい特定の目的を持つコインはトークンと呼ばれることが多い。そもそもこれらのトークンはほとんど既存コインのカラードコイン（ビットコインの場合）など既存のコインのシステムに乗った応用のコインとして発行される。以上の通り、コインはコインそのものと、資金調達を目的とする社債的なものの２つに分化してきたのである。今後後者は、様々な規制が課せられるものの、トークンを手に入れることで得られるサービスなどの価値を高めることで、より多くの参加者がコミュニティの一員となり、資金を提供するという最新の資金調達の手段として世界中で認知されていくと思われる。トークン発行者は、少しでも価値あるトークンにすることで多くの人々が参加し活発なコミュニティを作ることが重要になる。中身を充実させることが重要だということだ。

＜コインはキャッシュに進化する＞
トークンの発展には、プラットフォームとしてのコインそのものがしっかりと発展していかなければならない。しかし、前述の通り、バベルの塔は崩壊し始めている。トークン自体が最早砂上の楼閣といってよい状況である。
すでにブロックチェーン系のコインのプラットフォームの崩壊が始まっており、これに代わるプラットフォームの提供が待ち望まれている。従来のブロックチェーン型のコインプラットフォームも度重なる改善を施されてきたが、構造的欠陥を克服することはできないことが分かっており、抜本的解決可能な最有力候補として注目されているのが暗号貨幣技術をベースにしたプラットフォーム、暗号トークン（Crypto Token）である。すでにブロックチェーン系のコインをベースに発行されたトークンについても、コミュニティが存続を求めるものについてはその多くが順次 Crypto Token プラットフォームに変更されていくであろう。
従来通りトークンは、コミュニティの中で、トークン名（トークンシンボル）、トークンの総量管理（追加・減少）機能、トークン管理権限設定、トークン交換（送金）基本機能などのルールを決めて、コミュニティによって決められた代表者によって発行される。トークンは従来の貨幣と同様、記号列という実体を持ち、「決済」、「交換」、「保蔵」などに使用される。



Crypto Token プラットフォームでは、スマートフォンなどのアプリケーションで提供されるユーザーアプリ（Wallet）と、それぞれのトークンを発行するコミュニティ専用の①トークン発行機能、②トークン確認・再発行機能、③大きい単位または小さい単

位への両替機能、④トークン貸金庫機能の４つの基本機能から構成され、コミュニティによって運営される。これらのシステムはトークンの発行時／両替時／使用時などのタイミングで手数料を収受することで運用費を賄う。



トークンは従来の貨幣と同様に紛失しないよう注意深く保管しなければならない。大きな金額であれば金融機関や貸金庫のような自分が安心と考えるところ（Deposit）に預けることもできる。またトークンはそのまま相手に渡せば、金銭の譲渡や支払いに使用できる。トークンの受け渡しは、QR コード決済などの従来のペイメント方式を利用することもできるが、図のように預けたままその一部のトークンを使って決済を行うことができる。例として、「シックスペイ」という方法を説明する。Wallet から決済したい金額情報を Deposit に送信し、残額を確かめたうえで、Wallet アプリが暗号技術を使って 6 桁の数字を作りこれを決済先に渡して、決済先が自身の Deposit にブラウザーを通して 6 桁の数字を送れば決済は完了する。専用線（秘匿通信）や専用の読み取り機は必要ない。トークンを安全な場所に保管したままなので紛失のリスクを減らせるうえ、手持ちのトークンが決済額丁度でない場合など両替の手間を省くことができる。

今後この Crypto Token プラットフォームは、従来の株式（Crypto Stock）や債券（Crypto Bond）などにも応用されていく。

＜ブロックチェーンの目指したもの＞

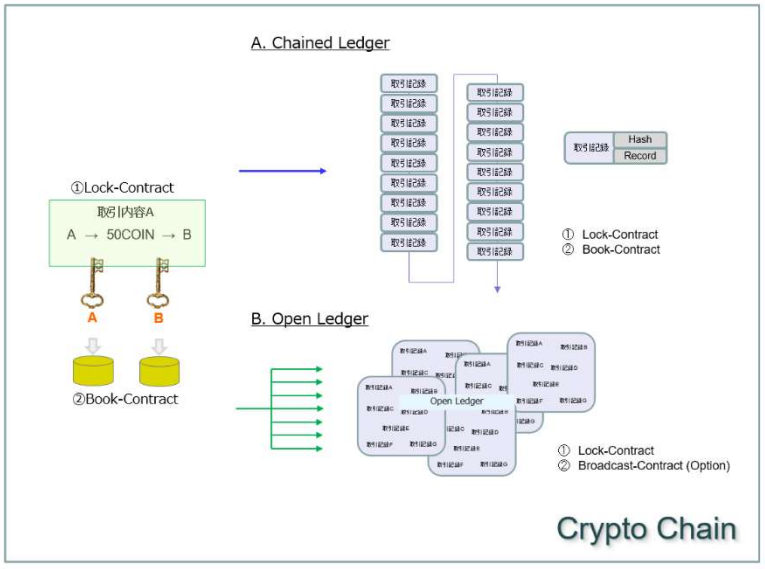
最後に、ブロックチェーンとビットコイン（またその類似技術）によって作り出される未来図について考察する。

ブロックチェーンは暗号通貨を構成するには役不足であったが、記帳システムとしての期待は依然大きい。特に、マイニング過程でコミュニティ全体のコンセンサスを形成できる点に注目する人が多く、この特長を利用した非中央集権的なシステムの可能性に焦点を当てた、DAO※5 や DApps※6 など様々な応用が考えられている。

現在のブロックチェーンは、ネットワークの維持のための報酬システムが組み込まれていることを特徴としており、自律的に非中央集権的に維持されているところも面白い。多くの人が報酬のために自らブロックチェーン維持のために志願する。逆に報酬が不十分となってしまえばそれ以上維持できないという問題を抱えている。構造上次々に増える志願者によってネットワークは巨大にならざるを得ないので、ある時点で維持コストが報酬を凌駕する。また、脆弱な暗号技術と構造的な脆弱性によってもいずれ確実に破綻する。

実は、ブロックチェーンによって作り出される未来図を実現するのに、これほど複雑なシステムは必要ではない。コンセンサスは関係者（ステークホルダー）の間だけで取れればよく、新しく開発された Crypto Chain を用いれば、同じ目的をはるかに簡便な方法で実現できる。

先にブロックチェーンでは、取引の１つ１つが台帳に記録されて初めて有効となるために、すべての過去の取引を調べることでしか、現在の状況を証することができないという、台帳方式最大の問題が内在していると述べた。例えば、ブロックチェーンによるBitcoinを現在Aさんがいくつ持っているかは、ブロックチェーン全体を限なく調べて、その残高を把握しなければならない。そのためハッシュチェーンが持つそれ自体の改竄不可能性だけでは不十分で、多数の複製を用意してこれを維持することが不可欠であると説明した。



もし、その時点で取引が確定しており、取引情報の１つ１つが改竄不可能ならば、それら１つ１つの取引情報を関係者だけで互いに複製を保存しておけば、関係者全員が揃わない限り改竄は不可能になる。この時点ですでに関係者間のコンセンサスは取れている。補助的に取引情報をまとめて記録するために、ハッシュチェーンを使って記録してもよい。これが「Crypto Chain」であり台帳を「Chained Ledger」と呼ぶ。また、関係者全員が結託して１つ１つの取引情報を改竄する恐れを回避するためには、これら１つ１つの取引情報をインターネットにブロードキャスティングすれば十分である。これを「Open Ledger」と呼ぶ。

このように、Crypto Chainを用いれば、改竄を防止するために、多数同一複製台帳は必要ない。極めてコンパクトなCrypto Chainで十分である。これを用いれば、ブロックチェーンの内在する問題を考慮する必要はなく、ブロックチェーンを用いることだけで実現されると信じられている未来が、ブロックチェーンなしに実現できるのである。

※1. World Wide Web （WWW）

インターネット上に蓄積されている情報を組織だった形式で，共有，検索，閲覧，利用できるように構築したシステム。単にウェブとも呼ぶ。マウスなどのクリック操作一つで，テキストや画像などの個別情報に関係づけられた別の情報を即座に参照できるハイパーテキスト形式が使われ，まるで蜘蛛の巣（web）のように情報の網を世界中のネットワークに張りめぐらせることができるため，この名がついた。スイスのジュネーブにあるヨーロッパ原子核研究機関 CERNに勤めていた物理学者ティム・バーナーズ＝リーが，1989年に研究情報共有のために開発したシステムで，テキストに文字，写真，動画，音声などを埋め込むツールがその中核であった。

（出典：ブリタニカ国際大百科事典 小項目事典　https://kotobank.jp/word/ワールド・ワイド・ウェブ-156029/）

※2. Mosaic

NCSAが開発したWebブラウザーのひとつ。Mosaicの登場によって、WWWの利用が容易になり、インターネットが加速度的に普及した。なお、米Netscape社のNetscape Navigatorは、Mosaicの開発メンバーによって開発された。

（出典：ASCII.jpデジタル用語辞典　http://yougo.ascii.jp/caltar/Mosaic/）

※3. 暗号技術の新しい標準

旧規格 DES（FIPS 46）の「DES」は、、時代の経過による相対的な強度の低下、NSAの関与があるその設計の不透明性（詳細はDESの記事を参照）が問題であることから、1997年9月にNIST（アメリカ国立標準技術研究所）が後継の暗号標準AES（Advanced Encryption Standard）とすべく共通鍵ブロック暗号を公募した。

(出典：Wikipedia https://ja.wikipedia.org/wiki/Advanced_Encryption_Standard/)

※4. 中間者攻撃による取引内容の改竄

中間者攻撃による取引内容の改竄については、以下のような攻撃が報告されている。

① 取引所に成りすました攻撃者にログイン情報を盗まれる。

② マイイーサウォレットのようなシステムでブロックチェーンの API を叩くまでに取引内容を改竄される。

また、中間者攻撃には分類されないが、ウォレットに侵入したマルウエアによって以下の攻撃を受ける可能性が指摘されている。

③ 手元にあるフルブロックチェーンのウォレット(ブロックチェーン P2P に直接アクセス)から送金処理をする

※5. DAO

Decentralized Autonomous Organizarion（分散自律組織）- 価値の交換を含む社会活動を、既存の価値体系での信用を用いずに行う組織であり、ビットコインやその発展系の共同体を表す基本概念。もしくは、クラウドファンディングの世界記録を持つ「The DAO」のこと。

(出典：Wikipedia https://ja.wikipedia.org/wiki/DAO/)

※6. DApps

DApps(分散型アプリケーション)とは『Decentralized Applications』のことで、日本語に訳すと「分散型アプリケーション」となる。これを言い換えれば『ブロックチェーン技術を用いた非中央集権的なアプリケーション』ということになる。

DApps(分散型アプリケーション)の定義として以下のものが挙げられる。

- オープンソースのアプリケーションで、特定の管理者に制御されず自動化されていること
- 暗号化されたトークンを持ち、参加者にはトークンで報酬が支払われること
- ユーザーの同意によってプロトコルが改善（例えばハードフォーク）されること

多くのサービス（アプリケーション）は株式会社のような中央管理者から提供されている。しかし、DApps(分散型アプリケーション)は、ブロックチェーン技術によりインターネット上に解き放たれて非中央集権的に分散している。

今後 DApps(分散型アプリケーション)が台頭してくれば、あらゆるサービスが非中央集権的に分散していくものになる。

(出典：Coin News https://coinnews.jp/articles/9450/)