第1回 ビットコインとブロックチェーン・分散台帳

セコム株式会社 IS研究所
コミュニケーションプラットフォームDiv.
暗号・認証基盤グループ
主任研究員 佐藤 雅史（さとう まさし）

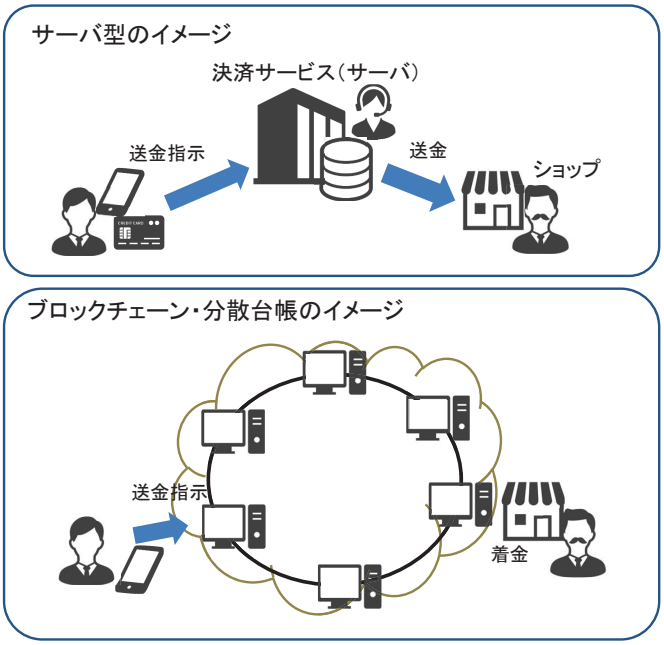
はじめに

2010年代の中頃から仮想通貨と共にブロックチェーン・分散台帳の熱狂的なブームが沸き起こり、多くの資金や人材が投入され数々の開発プロジェクトや実証実験が立ち上がった。2010年代も残り僅かとなった現在において熱風は穏やかになりつつも、ブロックチェーン・分散台帳を用いたサービスも出始め、さまざまな分野や業界でたびたび話題にあがるように人々の関心は未だ根強い。ブロックチェーン・分散台帳の技術を仮想通貨以外のデジタルデータ管理にも適用することで、業務改善や事業者間連携、新たなビジネス創造などに繋げたいという期待の声がある。このような期待の声は昨今のデジタルトランスフォーメーションの議論にも通じるものがあり、情報技術を基礎にデジタルデータを中心とした社会変革を目指す傾向は今後もますます強まることは疑いがない。しかし、これまでもそうであったように、万病に効く全能な技術というものはなく、どの技術にも特徴があり適切な使い方がある。ブロックチェーン・分散台帳も同じく、どのような特徴があるかを理解しておくことが重要である。

本連載では数回にわたり、ブロックチェーン・分散台帳の仕組みと特徴、最近の動向について紹介し、ブロックチェーン・分散台帳によるデジタルデータ管理の考え方を示したい。第1回となる今回はブロックチェーン・分散台帳ブームの元祖といえるビットコインを紹介する。

ビットコインの登場とブロックチェーン技術

ビットコインは2009年頃にSatoshi Nakamotoと呼ばれる仮名の者によって考案された電子決済システムである[1]。この電子決済システムの最大の特徴は、決済に用いる通貨の発行と通貨の移転（送金）に関わる一連の処理を中央の機関や事業者によらず実現する点にある。ビットコインでは、電子決済システムを管理する人や組織やサーバはいない。世界中の利用者が自身のコンピュータ上でソフトウェアを実行し、それらがネットワークを形成し、協調動作することで全体の決済システムが機能するようになっている。現在、このビットコインのプラットフォームとなるソフトウェアは有志の開発者コミュニティによって開発・保守されている。



従来型の決済サービスとブロックチェーン・分散台帳の決済サービスの違い

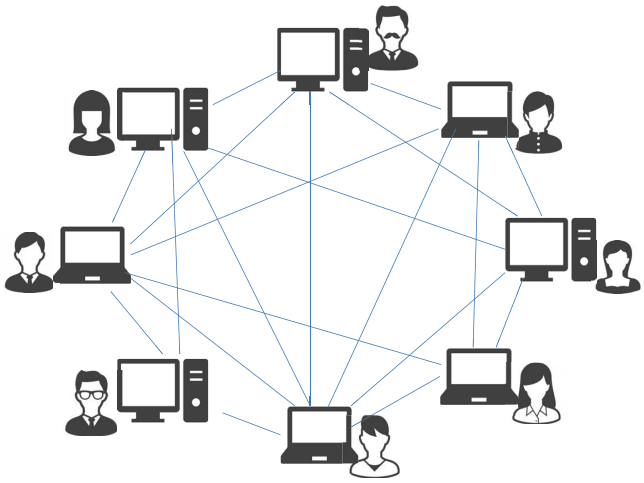
このビットコインの仕組みの要がブロックチェーンと呼ばれるものである。近年では、ビットコイン以外にもブロックチェーンの技術を発展させたプラットフォームが多く登場している。それらのプラットフォームの中には決済以外のデジタルデータ管理にも応用しようという動きがあるものもあり、また仕組み上の違いからブロックチェーンとは区別し、分散台帳と呼ぶものもある。

1 Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

ビットコインを実現するコンピュータネットワーク

従来の決済サービスは運営主体となる機関や事業者が介在し、それらの組織の管理下で決済に関わる一連の処理を実行し、整合性を維持している。例えば、利用者の口座番号などの情報を管理し、指示された金額を送金者の口座から減額し、同額を送金先の相手の口座へ移動する、などである。このような処理を適切に実行しなければ、流通している通貨量と不一致を起こし、通貨全体の機能を失ってしまう事態にもなりかねない。ビットコインは、このようなシステムを管理する機関やサーバがなくても、世界中の利用者が保有するコンピュータだけのネットワークで維持できる仕組みを目指している。

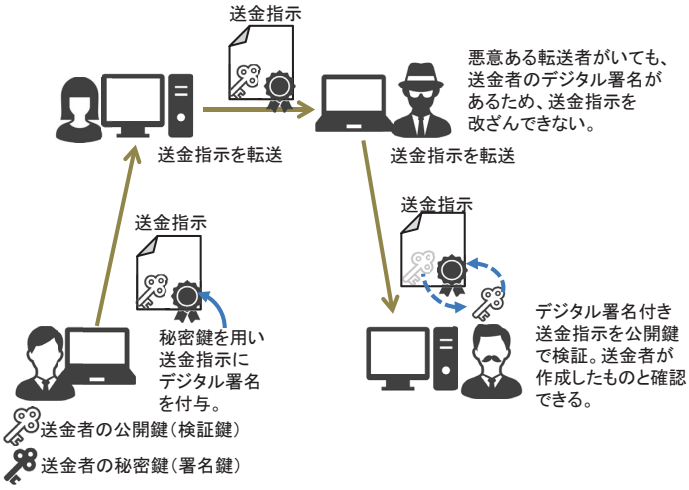
ビットコインのプラットフォームは主従関係のないコンピュータが網目のように接続される、いわゆるピアツーピアネットワークと呼ばれる形態である。このようなネットワークでは、ビットコインの送受を行う当事者のコンピュータ同士を直接結んで送金指示のやりとりを行うわけではない。送金者からの送金指示は、その者のコンピュータから送信され、そこと接続しているコンピュータが順次バケツリレーのように転送しあうことで、ネットワーク上のコンピュータに伝搬し、やがて受領者の知るところとなる。ちなみに、現時点では全世界で1万以上のコンピュータがネットワークに接続され、一つのビットコインプラットフォームを形成している状況にある。どのコンピュータもいつでも接続して良いし、また、不要であればいつでも切断できる自由な世界である。しかし自由な世界の中には、悪意ある者が稼働するコンピュータもいるだろう。伝搬されてくる送金指示の送金先や送金額を途中で不正に書き換える者もいるかもしれない。したがってこのような環境下でも決済のシステムを維持する仕組みが必要となる。この仕組みの代表的な技術的要素に、デジタル署名と、台帳作成メカニズム（ブロックチェーン作成）が挙げられる。次に、これらの要素を簡潔に紹介したい。



ピアツーピアネットワークのイメージ

送金指示の改ざんを防ぐデジタル署名

デジタル署名は、前述した課題の一つ、送金指示伝送の途中経路での情報改ざんを防ぐ（検知可能にする）暗号技術である。ビットコインの送金を行う送金者が秘密裏に管理する暗号の鍵（秘密鍵）を用いて、送金指示にデジタル署名という暗号データを添付する。送金指示を受領者は、送金者の秘密鍵と対となる公開鍵を用いてデジタル署名を検証する。デジタル署名を検証することで、送金指示がその送金者から出されていること、そして、指示内容が他者により改ざんされていないことを確認できる。デジタル署名は従来からある暗号技術で電子署名と呼ばれることもある。電子署名法などで聞き覚えのある読者もおられるだろう。ちなみに、ビットコインでは、電子署名法で規定されているような秘密鍵所有者に対する本人確認（認証事業者による本人確認）は行われず、送金者が自身で作成した公開鍵を告知するのみである。すなわち、ビットコインプラットフォームの通信上では、公開鍵や送金指示から実際の人物（例えば氏名や住所など）を特定することはできない。

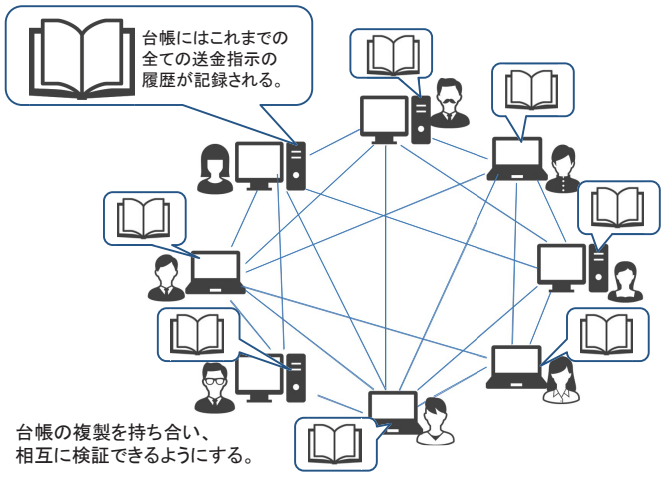


デジタル署名による送金指示の改ざん対策

取引が記録された台帳データの共有（複製）

次の課題は、さまざまな送金者から逐次出される送金指示をどのように処理していくかである。ビットコインのようなピアツーピアネットワークでは送金者から出された送金指示がどの通信

経路を辿るかは保証されず、各コンピュータに送金指示が到着する時間も順序もバラバラになる性質がある。バラバラな情報を元に各コンピュータがそれぞれ勝手に処理を進めると、各コンピュータでの決済処理の実行結果に食い違いが出てしまうことがある。この課題への対策として、ビットコインでは送金指示の履歴（送金の実行記録）を一つの台帳データに記載し、その台帳データの複製を各コンピュータで持ち合う仕組みを採用した。台帳データには正しく検証された送金指示だけが記録される。例えば、デジタル署名により改ざんがないこと、残高より多くの支払いをしていないか、同じ送金指示を過去に実行していないか等の検証である。台帳データ上では送金指示の順序は一意となり、各コンピュータで整合性の取れた処理を実行することができる。



台帳共有（複製）のイメージ

台帳データの作成方法と改ざん対策

しかし、ここでまた新たな疑問が浮上する。台帳データを誰が作るのだろうか。そして、台帳データもまた何者かによる改ざんの脅威にさらされないのだろうか。この台帳データの作成の役割を特定のコンピュータに任せてしまっては、そのコンピュータが従来の中央管理型のサーバの役割と変わらなくなってしまう。そこで、これらの課題に対し、ビットコインではプルーフオブワーク（Proof of Work）とよばれる台帳作成メカニズムを採用した。このメカニズムでは台帳データの作成は各コンピュータの競争によって行われる。この競争ルールは、台帳の新しい1ページを完成させるためにクジ引きを行うようなものである。この台帳作成の競争に参加する各コンピュータはアタリとなる数値を引くため、ひたすら大量に計算を繰り返す。晴れてアタリを引けたコンピュータは作成した新しい1ページを他のコンピュータに配信するとともに、自身は報酬として新たに発行されたビットコインを獲得できる。新しいビットコイン獲得のために大量計算を行う行為を発掘行為に見立ててマイニング（mining）と呼ぶこともある。この台帳の1ページはブロックと呼ばれ、各ブロックにさまざまな送金者の送金指示のデータが格納されることになる。ブロックはおおよそ10分間隔で順次作成されていく。作成過程ではハッシュ関数と呼ばれる暗号技術を使用し、各ブロックは前のブロックと順次結合されていくことで各ブロックに対する改ざんを防止している。台帳の1ページ1ページ（ブロック）が外せない鎖で閉じられているようなイメージである。ブロックの連鎖（チェーン）、すなわちブロックチェーンというわけである。

ビットコインの一連の処理や取り決め（通貨発行量やマイニングのアタリ設定など）は全てソフトウェアに組み込まれており、人手を介さず各コンピュータによって実行される。誰かが取り決めを無視して不正を働こうとしても、一部のコンピュータで実行されるソフトウェアを書き換えるだけでは、その他の多勢から無効なものとして無視されるだけとなる。自分にとって都合のよいルールに改変するためには世界中の大多数のソフトウェアを書き換えることとなり、それはほぼ不可能である。

経済的な動機付けによって台帳データは更新が続けられ、明確な管理者や運用者がなくとも整合した決済システムを維持するという発想はビットコインのユニークな点である。ビットコインのメカニズムは多くの者を惹き付けた一方で、さまざまな課題があることも判明してきた。ビットコインが抱える課題を解決するさまざまな手段が提案されており、現在も中核の開発コミュニティによってソフトウェアの修正や拡張が進められている。また、ビットコインから着想を得て、ビットコインとは別のプラットフォームの開発プロジェクトも多く立ち上がり、進展している。

第1回のまとめ

今回はブロックチェーン・分散台帳の源流であるビットコインについて紹介した。ビットコインは決済機能に特化しているため、汎用的なデジタルデータ管理にはそのまま応用しにくい。しかし、ビットコインの仕組みを基本として理解しておくことで、他のブロックチェーン・分散台帳の特徴を理解する手助けとなるだろう。次回以降の連載を通じて、ブロックチェーン・分散台帳の特徴、課題について述べ、デジタルデータ管理に適用する際の考え方を示していく。

第2回 ブロックチェーン・分散台帳とは

セコム株式会社 IS研究所
コミュニケーションプラットフォームDiv.
暗号・認証基盤グループ
主任研究員 佐藤 雅史（さとう まさし）

はじめに

ブロックチェーン・分散台帳は仮想通貨を実現するための技術的基盤として登場したが、仮想通貨以外にもさまざまな応用が検討されている。既存システムからの変革や新しいビジネスの創造など期待されており、それは昨今のデジタルトランスフォーメーションの議論にも通ずるものがある。情報技術を基礎にデジタルデータを中心とした社会変革を目指す傾向は今後もますます強まることは疑いがない。しかし、どんな技術にも当てはまるように、ブロックチェーン・分散台帳にも特徴があり、適切に扱うためにはその特徴をよく理解しておく必要がある。

本連載では数回にわたり、ブロックチェーン・分散台帳の仕組みと特徴、最近の動向について紹介し、ブロックチェーン・分散台帳によるデジタルデータ管理の考え方を示していく予定である。前回はブロックチェーン・分散台帳の源流であるビットコインの概要について紹介した。今回はビットコインの概念から派生したブロックチェーン・分散台帳の特徴と、検討されている利用例を紹介する。

ブロックチェーン・分散台帳が目指すもの

明確な管理者や運用者がなくとも整合した決済システムを維持するというビットコインの発想は、従来の決済システムとは異質なものであった。ソフトウェアをオープンソースとし無料で配布したことで、利用者に広まり、さらにさまざまな事象が追い風となり、ビットコインのプラットフォームを構成するコンピュータネットワークは大規模なものとなった。このように、ビットコインの概念を論文として公表しただけでなく、実際にソフトウェアを普及させ実証したところが注目に値する。

ビットコインは多くの技術者や新興企業などを惹き付け、ビットコインに触発されたブロックチェーン・分散台帳プラットフォームの開発プロジェクトも数多く立ち上がった。その中には、ビットコインのような新たな決済手段（いわゆる仮想通貨）のためのプラットフォームもあれば、その他の用途のためのデジタルデータ流通や管理のためのプラットフォームもある。それぞれ目的や仕組みに差異はあるが、ビットコインの概念に多かれ少なかれ影響を受けている。

ビットコインや多くのブロックチェーン・分散台帳の概念の一つとして、システムを支配できる立場にある機関や事業者などの関与を極力排除しようとするものがある。その背景には、例えば、各国の中央銀行が行う通貨発行への問題提起や、管理主体となる機関や事業者が大きな支配力を握ることへの懸念、機関や事業者のサービス停止や廃業などによる機能不全の回避などがある。さらには、利用者中心の経済圏を作ろうという思想もあり、その思想を実現するために、どのコンピュータでも機能が肩代わりできるような分散型モデルを採用している。

また、人間の判断に基づく運用を軽減しようという概念もある。人は間違えることもあれば、意識的にも無意識的にも恣意的な判断をしてしまうことがある。ビットコインや多くの後続プラットフォームではさまざまな処理や取り決めをソフトウェアに組み込み自動実行する仕組みを採用している。そのソフトウェアもオープンソースで公開することで処理内容の妥当性も外部から検証可能にすることができ、台帳データ（ブロックチェーンデータ）の記録を辿ることで処理結果についても検証可能にする、というように透明性の確保を重視している。

上記のような概念は賛否ともどもさまざまな議論がある。また、現状のブロックチェーン・分散台帳のプラットフォームの機能や性能を考えた場合、実際にこのような世界を実現できたとしても、社会で一般的に運用していくにはまだ時間がかかるように思える。しかし、これらの概念は多くの人々を惹き付け、ブロックチェーン・分散台帳による既存システムへの破壊的イノベーション（変革）を目指す大きな原動力の一因になっている。

ブロックチェーン・分散台帳の傾向

ブロックチェーン・分散台帳のプラットフォームは多種多様で

あり、技術的な観点でひと括りにすることは難しい。実は、ブロックチェーンや分散台帳といった言葉も明確な定義がなされているわけではなく、関係者の間でもそれぞれの解釈で用語を使い分けていることが多い。ブロックチェーンと分散台帳の相違点として、台帳のデータ形式の違いがある。ビットコインのように、台帳のデータ形式がブロックと呼ばれる、ひとかたまりのデータを連ねていく形式（本連載第1回を参考のこと）であるものをブロックチェーンと呼び、そうでないものを分散台帳と呼ぶ傾向がある。データ形式の違いから台帳作成と共有（複製）の方式も異なっている。形式の違いはあるものの、ブロックチェーンも分散台帳も大きな視点では、複数のコンピュータ間で台帳を共有し、相互に台帳の正しさを確認しながら、台帳の改ざんを防止するという考え方は同様である。

台帳データに書き込める情報に着目すると、ビットコインの場合は決済機能に特化しているため、台帳データに書き込める情報は決済に関わる取引情報（仮想通貨の送受の情報）であり、それ以外の情報を記載することには適していない。一方で、後発のブロックチェーン・分散台帳のプラットフォームの中には、取引情報以外にも利用者が定義したさまざまな情報を台帳データに書き込めるものも登場している。さらに、台帳に記録され、台帳の情報と連動して駆動するプログラムを組み込めるものもある。このような台帳と連動したプログラムはスマートコントラクトと呼ばれている[1]。このように、台帳データにさまざまな情報を記載できる機能や、プログラム実行を伴うスマートコントラクトの機能によって汎用性や拡張性が高まり、決済以外の用途にも応用できる可能性が出てきた。この可能性に着目した多くの業界やコミュニティ、組織が多分野のデジタルデータ管理への適用を検討している。応用先として検討されている例を次に紹介したい。

ブロックチェーン・分散台帳の応用検討例

決済等

仮想通貨を媒体とした決済を行う。ビットコインと同様に、決済に関わる情報をブロックチェーン・分散台帳で記録する。仮想通貨の発行と仮想通貨の送受の履歴をブロックチェーンに記載することで、発行量や流通に対する透明性を確保する。仮想通貨の利用は取引時の決済以外にも、ソーシャルメディア等において個人が発信する情報や記事・コンテンツに対する評価や支援として送付するといった使われ方もある。昨今、仮想通貨は交換レートの乱高下が激しく決済として扱いにくい状況にあるが、安定した交換レートを実現する方法も検討されている。

個人間取引

オンラインのフリーマーケットにおける個人間の物品売買や、ゲームで用いるデジタルデータ（例：ゲームキャラクターのトレーディングカードデータ）の売買情報をブロックチェーン・分散台帳で管理する。ブロックチェーン・分散台帳には物品やデジタルデータの識別番号と保有者の識別番号の履歴が記録され、識別番号と実際の物品やデジタルデータとの関連付けはブロックチェーン・分散台帳とは別の仕組みで行う。この他、電力の個人間取引の仲介を行うことも検討されている。個人の家庭で発電した余剰電力を別の者に与える際の売買記録をブロックチェーン・分散台帳で管理する。ブロックチェーン・分散台帳に記録された売買情報に連動した装置によって、実際に送電が行われることになる。

権利等の管理

IoT[2]など機器や装置の使用権に関する情報をブロックチェーン・分散台帳で管理する。ブロックチェーン・分散台帳の情報を元に、機器・装置への操作の権限、または、機器や装置から出されるデータの利用を他の者へ許諾したり、利用権の売買を行ったりする。ブロックチェーン・分散台帳は権利の保有者や権利の譲渡先などを記録するために用いられる。別の例では、音楽などのデジタルコンテンツに対する権利の管理を行うケースもある。その他にもデジタルデータで表現されるさまざまな権利関係の移転などを管理することが検討されている。

サプライチェーン

製造や食品流通の各工程や物流において、関係する事業者が商品の状態や配送状況などの情報をブロックチェーン・分散台帳に記録する。企業や業種をまたがった横断的なトレーサビリティを実現するため、ブロックチェーン・分散台帳の導入が検討されている。

組織間の情報連携

銀行や証券会社などで実施している本人確認業務に付随する情報をブロックチェーン・分散台帳に記録する。各社が連携し、本人確認手続きを共同で実施することで手続きの省力化や安全性の強化を目指す。その他にも公共サービスに関わる異業種の企業間で顧客に関する情報をブロックチェーン・分散台帳に記録し、連携することでワンストップサービスを実現しようという試みもある。

1　ブロックチェーン・分散台帳のプラットフォームによっては同種の機能に別の呼称をする場合もあるが、一般的にはスマートコントラクトという呼称で分類されている。

2　Internet of Things：インターネット通信機能を備えた多種多様なセンサーや機器

上記以外にもさまざまな利用例が検討されているが、いずれにおいても、ブロックチェーン・分散台帳はデジタルデータ管理の部分に用いており、全体のシステムはその他の技術や運用と組み合わせて実現されている。上の例で言えば、装置や機器で備えるべき機能や、送電のための施設、金融機関における顧客本人確認の手続きなど、ブロックチェーン・分散台帳以外のメカニズムや処理が必要である。ブロックチェーン・分散台帳が活躍する場面は、例えば権利関係などで矛盾する二重の譲渡が行われていないかを記録上で確認するといった、デジタルデータ上の整合性の確認である。

また、上記の例以外も含めたさまざまな利用検討の中には、実証実験の段階でまだ実用に至っていないものも多い。また、ブロックチェーン・分散台帳の技術的な検証を目的としたものもあり、ブロックチェーン・分散台帳が適している利用例とは言い切れないものもある。

次回の連載で、ブロックチェーン・分散台帳におけるデジタルデータ管理の考え方について踏み込みたい。

コラム

仮想通貨（暗号資産）

ビットコイン以外に膨大な種類の仮想通貨が存在する。その多くは何かの資産（ゴールドや円など）等に基づいて発行される仕組みではなく、仮想通貨の価格や価値を決める基準というものがない。仮想通貨に価値を見出した者同士で売買が行われる中で、急激な需要やさまざまな問題の発生など、なんらかのきっかけで仮想通貨の交換レートが暴騰 / 暴落することがある。例えば、ギリシャやキプロスの金融危機では、同国の銀行の預金者が引き出しや送金の制限、預金課税などを回避するために、ビットコインに交換し保有する者たちが現れ、そのためビットコインの相場が急騰したと言われている。あるいは、各国で仮想通貨に対する規制に関する言及がなされると相場が急落するといった状況も見られた。現在は落ち着きつつあるものの、ここ数年の仮想通貨ブームで相場変動も激しく、決済手法として登場したものの決済に使われにくいという状況に陥っている。決済用途よりも投機目的として仮想通貨交換所で売り買いする人や、資産価値として保有している人が多いのが現状である。こうした現状を背景とした国際的な議論により、仮想通貨という呼称から暗号資産 (Crypto Assets) に変更しようという動きがある。また、交換レートの問題を解決するため、円やドルといった法定通貨に紐づけるなど、より安定的な価値を維持する仮想通貨（暗号資産）発行の仕組みも提案され検証が行われている。

また、別の問題として、仮想通貨（暗号資産）の仕組みそのものは利用者の本人確認もなく、通信上でも本人を特定できるような情報はやり取りされないため、ブラックマーケットでの決済手段やマネーロンダリングなど反社会的な用途に使われやすい傾向がある。仮想通貨（暗号資産）を入手するための一般的な入口は仮想通貨交換所と呼ばれる事業者である。法改正により、日本で事業を行う仮想通貨交換所は 2017 年から登録制となっている。日本の仮想通貨交換所では本人確認が実施されており、仮想通貨交換所を通じて行われた送金については送金者の身元が確認できるようになっている。

このコラムで述べたように仮想通貨（暗号資産）にはさまざまな課題があり、今後も技術的な仕組みと制度など社会的な取り組みによって解決していくことになるだろう。

第3回 ブロックチェーン・分散台帳における デジタルデータ管理の考え方

セコム株式会社 IS研究所
コミュニケーションプラットフォームDiv.
暗号・認証基盤グループ
主任研究員 佐藤 雅史（さとう まさし）

はじめに

前回はブロックチェーン・分散台帳の共通的な特徴と検討されている応用例の一部を紹介した。世の中の応用例の中には、ブロックチェーン・分散台帳の技術的な課題を洗い出すことを目的とした実証実験の場として考えられているものもあり、すべての応用例がブロックチェーン・分散台帳の特徴を効果的に活用したものであるとは限らない。ブロックチェーン・分散台帳の適用を考える場合には、その技術の特性をよく考える必要がある。連載最終回となる今回はこれまで述べてきたブロックチェーン・分散台帳の特徴や性質を振り返り、デジタルデータ管理を行う場合の考え方を示したい。

ブロックチェーン・分散台帳の機能

ここでは、これまでの連載で述べてきたブロックチェーン・分散台帳の共通的な特徴を振り返り、ブロックチェーン・分散台帳の主な機能を整理したい。

ブロックチェーン・分散台帳の主な狙いは、データ管理や処理に関して特定の機関や管理者などへの依存性を抑制することにある。それは、特定の機関や管理者がデータ管理や処理において不正を働くこと、恣意的な操作を行うこと、経済的理由などでデータ管理や処理を維持継続できなくなること、なんらかの障害で一時的に機能停止するなどといった懸念が背景にあるからだ。

ブロックチェーン・分散台帳が採用したアプローチは、データ管理や処理を異なる者が管理する複数のコンピュータ間で協調動作させ、一部の者やコンピュータが異常な行動や機能停止しても、システム全体として正しく動作できるようにすることである。

そして、そのようなシステムを実現するために、以下のような機能や性質を求めている。

複数のコンピュータ間でのデータの共有と相互検証

複数のコンピュータ間で同じ台帳データを複製し持ち合う。台帳データに記録される情報の妥当性を複数のコンピュータで検証する（検証できるようにする）。同じ台帳データとなるようにコンピュータ間でのデータ同期方法についてさまざまな手法[1]が提案されている。

データに対する改ざん耐性

管理者の異なる複数のコンピュータ間でデータの送受、処理や管理を行うため、途中の過程でデータが改ざんされないことが必要となる。そのため、個々のコンピュータから送信されるデータ（取引情報など）への改ざん対策としてデジタル署名技術を採用している。また、それらのデータが記録される台帳データにも暗号学的ハッシュ関数を応用した改ざん対策が行われている。

データ検証や処理の自動化と透明性

ブロックチェーン・分散台帳が目標とする究極の世界は、人手を介すことなく、台帳データと連動したプログラムが中心となって自動実行される世界である。プログラム実行の監督を行う機関や管理者もない世界であるため、プログラムが正しく実行されているかどうかについても、複数のコンピュータ間でチェックできることを求めている。このような台帳のデータと連動して動作するプログラムはスマートコントラクトと呼ばれている。スマートコントラクトは処理の内容と実行結果を台帳データに記録し、各コンピュータでプログラム実行を再現できるようになっている。実行結果を複数のコンピュータで検証可能にするといった透明性への要求がスマートコントラクトと従来のプログラムとの違いといえる。

さまざまなブロックチェーン・分散台帳のプラットフォームはそれぞれ詳細な仕組みは異なるが、上記の機能や性質を要求している点は共通的といえる。さらに、複数のコンピュータ間での

1 ブロックチェーン・分散台帳の分野で、これらの手法はコンセンサスアルゴリズムと総称されている。

データ共有に対する考え方について、2つの大きな分類ができる。連載第2回で示した応用例を振り返ってみよう。ソーシャルメディアでの仮想通貨の利用や個人間取引といった例では、できる限り分け隔てなく誰でもブロックチェーン・分散台帳のコンピュータネットワークに参加できる仕組みのほうが参入へのハードルが低く、より広く参加者を募ることが期待できよう。参入へのハードルが低くなることで、新たな応用例のアイデアが生み出される機会が増える可能性もあるだろう。一方で、サプライチェーンや組織間の情報連携といった例では、特定の業界内や企業間での利用を想定しており、このような誰でも自由に台帳データにアクセスできる環境は必ずしも必要ではないし、好ましくない場合もある。

これらのためにブロックチェーン・分散台帳のプラットフォームには、利用者やコンピュータのアクセス制限の有無によって、プライベート（Private）/パブリック（Public）、さらに、パーミッショナド（Permissoned）/パーミッションレス（Permissonless）という用語で分類されることがある。これらの用語もまた明確な定義がなされているわけではなく、人により解釈が微妙に異なる。ここではパーミッショナド/パーミッションレスという用語で区別することとする。最初にパーミッションレス型を紹介し、次にパーミッショナド型を紹介したい。

パーミッションレス型のブロックチェーン・分散台帳

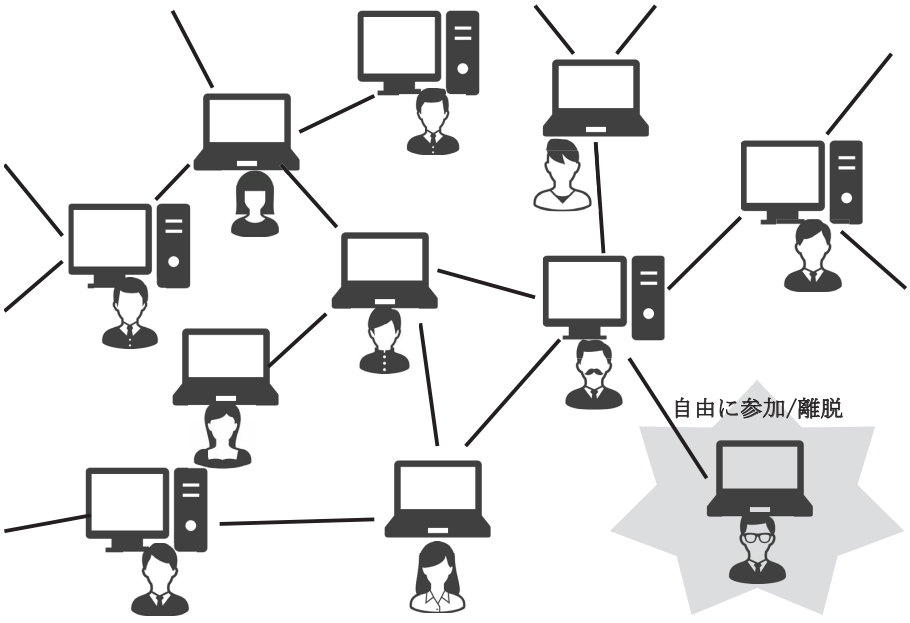


図1　パーミッションレス（パブリック）型のイメージ

パーミッションレスやパブリックと呼ばれるブロックチェーン・分散台帳のプラットフォームは、誰でも使え、利用のための資格や条件、承認等は不要である。利用する場合には、インターネットに接続したコンピュータでソフトウェアを起動するだけでよい。前回の記事で紹介したビットコインや、ビットコインと並び著名なプラットフォームであるイーサリアムがこの代表格である。イーサリアムは汎用的なデータ記録やスマートコントラクトの機能を持ち、決済以外の用途にも対応している。この形態のブロックチェーン・分散台帳は誰でも自由に参加でき、参加する目的もさまざまである。ある利用者は決済情報の管理に使用したいと考えるかもしれないし、また別の利用者はある商品通流の記録（商品番号の追跡など）に使いたいと考えるかもしれない。目的は違えども、皆が同じ台帳データを共有し、誰もが更新・参照できるのが、この形態の特徴である。

この形態の利点は、利用のためのハードルが低いため、数多くの利用者が台帳データを用いたアプリケーションの開発者になり得ることである。さまざまな開発者が発案する多種多様なアイデアの中から革新的なアプリケーションやサービスが登場するかもしれない。このようなイノベーションの可能性の一方で、誰もが参加できることの負の側面として、悪意ある者も参加できるという点がある。悪意にもさまざまあり、皆が共有する台帳データを破壊しプラットフォームを機能停止させようとするものもいれば、プラットフォームの機能を使って反社会的な目的に利用するものもいるだろう（連載第2回コラム参照）。

プラットフォームへの攻撃の一部については、連載第1回で述べたビットコインの台帳データの改ざん対策のように、プラットフォームの機能で対策が講じられているものもある。一方で、プラットフォームを不適切な目的で悪用する者については問題が複雑だ。例えば、誰から誰へ支払ったという決済情報だけでなく、その支払いで何を購入したかという購買情報までも台帳データに書き込んでしまった場合、その台帳データに記載された購買情報の傾向から詐欺などの悪用のための情報源として利用されてしまうかもしれないのだ。

この形態のプラットフォームを利用する場合は、誰もが台帳データを参照できるという前提で情報漏えいやプライバシー侵害の可能性と、台帳データが悪用され

る危険性を考慮し、台帳データに書き込むべき情報を精査する必要がある。最近では、高度な暗号技術を用いて、台帳データを秘匿しつつ、台帳データの不整合を確認できる機能についても研究が進められており、将来、実用に達することが期待される。しかし、いずれにせよ、このような誰彼構わず台帳データを共有する仕組みでは、特定の業界や組織・分野に限定したい用途では機能的にも性能的にも限界がある。そこで、登場したのが、プライベート・パーミッションド型のブロックチェーン・分散台帳のプラットフォームである。

パーミッションド型のブロックチェーン・分散台帳

パーミッションドやプライベートと呼ばれるブロックチェーン・分散台帳のプラットフォームは、コンピュータのネットワーク接続制限や、事前に利用者やコンピュータに対して登録や承認などの手続きを行うなど、アクセス制限を行う形態である。

パーミッションド型の特徴は、企業や組織間など管理が異なるシステム間で台帳データの複製を持ち合うことができ、また、アクセス制御等により台帳データの利用をコントロールすることができることにある。パーミッションレス型が一般利用者による一般利用者のためのプラットフォームを目指す傾向にあるのに対し、パーミッションド型は主に特定の業界や分野において組織間の連携を行うためのプラットフォームを目指している。

この形態では、登録や承認などの手続きを行うためのサーバや運営者を必要とする場合がある。また、利用者やコンピュータに一定の基準や信頼を置くことを前提するため、ビットコインのような競争に基づく台帳データ作成の仕組みは採用せず、台帳データ作成の役割を分担する複数のサーバを設置することで、より高速で大量のデータ処理を実現しているものがある。このように、特定の機能や役割を担うサーバや管理者が置かれる場合があることから、パーミッションレス型に見られるような機能、役割の分散化や、特定の機関や管理者による関与の排除といった構想からは遠ざかる傾向にある。

この形態を適用する場面では、パーミッションレス型のような利用者をも巻き込んだイノベーション創発への期待よりも、企業や組織間の業務上の課題解決を重視する側面があり、システムの全体構成も従来型のシステムに類似した傾向になる。連載第2回の利用例で記載したサプライチェーンでのデータ管理や金融機関のデータ連携などのようなケースで用いられる場合が多い。

ブロックチェーン・分散台帳におけるデータ管理の留意点

上記のパーミッションレス型とパーミッションド型の違いで、一口にブロックチェーン・分散台帳といっても、ずいぶんと性格が異なることが理解していただけたと思う。デジタルデータ管理を行う対象や目的に照らし合わせてブロックチェーン・分散台帳のプラットフォームの適合性を考え、利用すべきである。

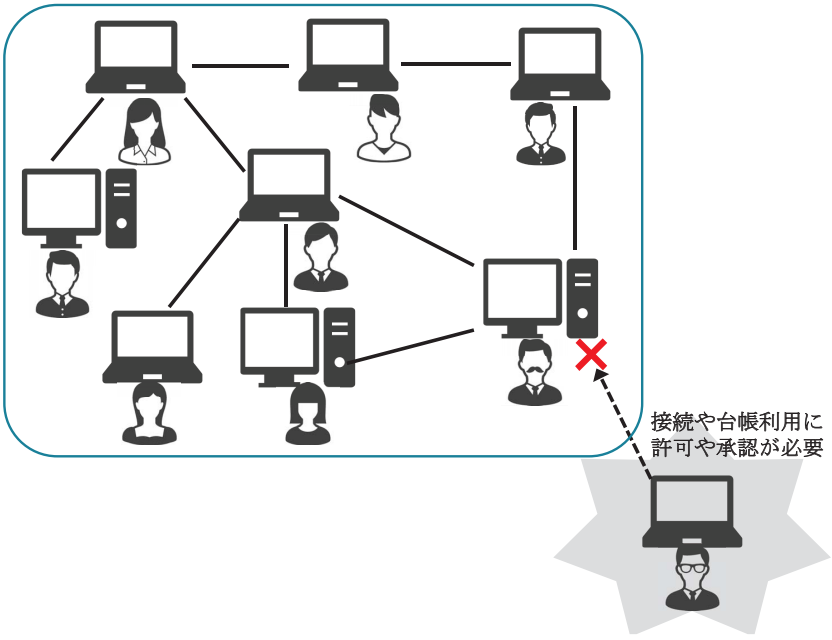


図2　パーミッションド（プライベート）型のイメージ

目的はなにか

ブロックチェーン・分散台帳では、前述したデータ共有やデータの改ざん耐性、プログラムの実行といった機能はそれぞれが独立した技術によって実現されているのではなく、複数の技術が組み合わされて実現されており、複雑な傾向がある。ある目的を達成するために必要な機能が、データの共有だけ、あるいは、データ改ざん耐性だけといったように、特定の機能だけである場合には、ブロックチェーン・分散台帳のプラットフォームがもたらす種々の機能を持て余してしまうことにもなる。さらには、プラットフォームの機能や性能などの制約がかえって足かせになってしまうことにもなりかねない。

例えば、同一組織内で管理するデータについて考えた場合には、これまで述べてきたブロックチェーン・分散台帳が前提とする環境とは異なり、処理性能と引き換えとなる複雑なデータ複製メカニズムは過剰なこともある。目的を果たすための前提としている環境が、先に述べたブロックチェーン・分散台帳の背景にある考え方と合致できるかどうかという点は重要だろう。そうではなく、データ共有やデータ改ざん耐性など単体の機能だけに関心があり、特定の機関や管理者にシステム構築や運用を任せてもよい等といった場合には、データベース技術や、電子認証局に基づくデジタル署名、デジタルタイムスタンプ技術などこれまでの成熟した技術と比較検討することも必要となる。

ブロックチェーン・分散台帳を使う場合には、さまざまな人や組織の間で台帳データを共有し、台帳データについて取り決めたルールの実施を相互に検証できる（監視できる）ことが重要なカギになると考えられる。どのような者や組織を巻き込んでどのような価値を生み出すことを期待しているかに振り返り考えることが必要だろう。

共有すべきデータとは

パーミッションレス型は、基本的に台帳データが他の利用者からも閲覧可能になるため、特定の利用者間だけで秘密にしたい情報を記録するのには適さない。一方で、パーミッションド型であっても、情報が他の利用者（例えば、別の企業や組織など）と共有されるという前提は念頭に置いておくべきである。

どの情報を誰と共有するかしないかというように、情報の区分とアクセス制御を事前に設計しておくことが必要となる。また、パーミッションレス型にしろ、パーミッションド型にしろ、他の利用者と台帳データを共有するため、冗長な情報を台帳データに記載することは台帳データサイズの無用な肥大化を招くこととなり、他の利用者に対しても負担をかけることとなる。台帳データの無用な肥大化を招かないためにも、台帳データに記載する情報の選別は重要である。実は、台帳データに記載できるデータ量や一度に処理できる量には制限がある。

例えば、大きなサイズの画像や動画データなどの台帳データに記載することは現実的ではない。よくある適用方法としては、実際の画像などのサイズの大きなデータはブロックチェーン・分散台帳外で保存し、ブロックチェーン・分散台帳の台帳データにはその画像を参照するための情報を記載するといったものがある。他にもメタデータの管理も考えられるだろう。

このようにブロックチェーン・分散台帳はなんでも管理できる汎用的なデータベースではなく、あくまでも、台帳データに記載されたデータの正しさや、スマートコントラクトで実行された処理結果の正しさを検証するためのものとして考えた方が良い。

入力前のデータに対する管理

ブロックチェーン・分散台帳のプラットフォームは台帳に記載されたデータについては改ざんを防止するが、プラットフォームに入力される前のデータが正しいかどうかは関与しない。例えば、サプライチェーンでの利用において、台帳に商品番号による流通過程を記録するケースを考えてみよう。

流通の各拠点で台帳に商品番号と所在地、商品の状態などのデータを入力し記載することになるだろう。そして基本的には、台帳に記録された商品番号に基づいた履歴は改ざんされることなく維持される。しかし、実際の商品と商品番号の紐づけが正しいかどうか（例えば、流通の過程で入れ替えられていないか）は台帳だけでは分からない。実際の商品と商品番号の紐づけをどのように管理するのかをブロックチェーン・分散台帳のプラットフォームとは別に検討する必要がある。入力前のデータの正しさをどう担保するかという課題は、データベースやデータ記録管理システムで共通の課題であり、ブロックチェーン・分散台帳であっても例外ではない。

ブロックチェーン・分散台帳の今後

ブロックチェーン・分散台帳のプラットフォームやプラットフォームを支える周辺技術の環境は日々更新され、新しい技術の研究開発が盛んに行われている。現在抱えている機能や性能、安全性に関するさまざまな技術的な課題も将来的にはさまざまな手法で改善されていくだろう。現在は乱立状態にあるプラットフォームも将来的には淘汰されていき、代表的なプラットフォームに関する開発環境はさらに拡充し、対応アプリケーションや対応システム開発のノウハウが蓄積されていくとともに、より広範な利用者や開発者にも扱いやすい環境が整備されていくと考えられる。そのような状況になれば、ブロックチェーン・分散台帳がデジタルデータ管理の基盤を支える、リーズナブルで十分な機能や性能を備えた技術要素として、より大きな存在感を示すことになるかもしれない。

ブロックチェーン・分散台帳の背景にある考え方を理解し、来るべきデジタルトランスフォーメーション時代におけるデジタルデータ管理のあるべき姿を考えることが、今求められていることだろう。