第　2　部　第1章

ブロックチェーンによる分散型台帳技術の解説

小林 直人　宮田 大輔

目　次

１．はじめに

ブロックチェーンとは、ビットコインを始めとした暗号資産（仮想通貨）の根幹をなす技術である。分散型台帳技術の一手法であり、中央集権的な管理者が不在のもとで、信頼性高く情報を記録するための方法である。2008 年にサトシ・ナカモトが暗号技術のメーリングリストに投稿した論文［1］にて初めて提唱され、2012 年頃からビットコインが実用化され始めたのをきっかけに、様々な分野において、その応用が検討されている。

ブロックチェーン自体は、真新しい手法によるものではなく、既存の情報技術の組み合わせにより実現された複合技術である。それ故、その仕組みを容易に説明しづらいことから、誤った解釈で紹介されることもある。

本章ではその技術的側面について、なるべく平易な形で、つまり暗号技術をはじめとした情報通信技術をなるべく交えない形での解説を試みる。

２．ブロックチェーンとは

２－１　ブロックチェーンに適した情報システム

前述したように、ブロックチェーンとは分散型台帳技術の一手法であり、広く言えば情報の記録・管理を行う方法（データベース）のひとつである。一般的に台帳とは「売買の金額などの取引情報を記録する帳簿」を指すが、これはブロックチェーンがビットコインという仮想的な通貨実現のため提案されたことに由来するものであり、台帳に限らず、どのような情報でも記録できる。

ブロックチェーンは、実現したい情報システムが次の要件を満たす場合に、必要なデータを記録するデータベースとして適していると言える。

・中央集権的な管理者（サーバコンピュータ）の存在しない、つまり平等な複数の管理者によって運用される情報システムの実現
・ただし、その管理者の中に信頼できない者が存在するという状況を想定する
・その下で、不正な記録の防止や、記録された情報の改ざんの防止の実現

逆に、信頼できる中央集権的な管理者が存在する場合や、複数の管理者がいてもお互い

に信頼できる場合においては、既存の技術で事足りることも多いという事実は、ブロックチェーンを理解する上で認識しておく必要がある。

そもそもブロックチェーンとは、その第一の応用事例であるビットコインが「国家から独立し誰でも（システム管理者として）参加でき、記録した情報に通貨のような価値を持たせて、それを直接譲渡できる仕組み」の実現を目指して開発されたために必要となった技術である。上記の要件は、この実現のための要件に他ならない。ビットコインのような仮想的な通貨の実現以外にこの要件を満たす状況としては、不特定多数が管理者として参加できる情報システムや、同業他社のように特定の利害関係にある者同士で共同管理する情報システムが考えられる。具体的な例については第 3 部で紹介する。

なお、一般的な電子マネーは、その運営企業のサーバコンピュータで中央集権的に情報管理されるものであり、通貨のように利用者から利用者へと価値を直接譲渡できるものではない。この点で、一般的な電子マネーと暗号資産は実現方針がまったく異なる。

2－2　ブロックチェーン（ビットコイン）開発の動機

サトシ・ナカモトの正体は 2021 年時点でも謎に包まれており、その開発動機などについては分かりかねる。しかし、サトシ・ナカモトに限らず、古くからコンピュータ技術者（geek）たちが、中央集権的な管理不在のシステムを作りたがる傾向があるという点を、前提とすることで、ブロックチェーン（ビットコイン）の開発動機を想像することができるのではないだろうか。開発当時から実用に至るまでの話や、情報技術的な解釈については［2］に詳しい。以下、一部を引用する

2009 年 1 月 3 日に、サトシ本人によって書かれた最初のコードから、ビットコインの最初のブロックが生成された。基本的に、ビットコインに関心を持っているのは一部の geek だけだった。彼らは、ビットコインの趣旨に賛同し、自らの PC の計算機資源を供出してマイニングを行い、ビットコインの取引を支えたのである。

そこには明示された契約も、法人化の仕組みもなく、コード（コンピュータのプログラム）だけが存在する。そのコードもまた、自主的に集まった技術者が、相互にレビューしつつ、自由に書き換えることができる。そのコードが、重要な経済的な帰結（たとえば、暗号資産の価格変動や、業者間の主導権争いの決着）を生じさせる。このような、「コードが支配する世界」が到来することは、インターネットが出現した当初から予想はされていた。しかし、それが予想されたよりも早く、数十兆円規模の暗号資産という形で実現す

ることになったことは、人々を驚かせるのに十分であった。

３．取引情報の分散管理

本節では、ビットコインのような「記録した情報に通貨のような価値を持たせて、直接譲渡できるシステム」を実現することを想定し、前節で述べた要件を満たすためにはどのような仕組みを導入すれば良いかを説明していく。なお､本節では簡単のため､コンピュータの利用は想定せず、管理者が人手で情報の記録・管理を行うこと、つまり人力システムとでもいうべきものを想定する｡通貨の単位はコインとする｡なお､本節で説明する方法は､ブロックチェーンの実現方法を踏まえて記載しているものの、あくまで一例であり、別の選択も考えられる。

３－１　管理者が１人の場合

まず管理者が１人で取引情報を記録・管理することを考える。システムの利用者は取引の内容を何らかの連絡手段で管理者に伝える。管理者はノートなどの記録媒体に手書きで情報を書き込んでいくものとする。なお、この状況は一般的な電子マネーのように中央集権的に（サーバークライアント方式）行われている方法と同様である。

利用申請とコインの発行

まず利用者に何かしらの形でコインを与えないと取引はできない。様々な方法が考えられるが、例えば、利用者が申請をした時点で 500 コインを与えるものとする[1]。管理者は申請があった時点で、台帳に次のような情報を書き込む。

1 行目	20/12/1 10:00:00		小林	500
2 行目	20/12/3 11:00:00		宮田商店	500

取引情報の伝達

コインを使った取引を行うときに、利用者はルールに従って取引情報を管理者に伝える

1　このルールで運用する場合、この仮想経済圏のコインの全量は（利用者× 500）となる。なおビットコインは、このルールで運用されているわけではなく、後述するマイニングによりコインが新規発行される。その発行額を経過時間により調整することで、コインの全量を調整している。

(2 人で伝えても良いし、1 人が代表で伝えても良い)。ここでは「誰が、誰に、いくら送るか」を伝えるように決める。例えば､小林が宮田商店で 200 コインの買い物をした場合、「小林、宮田商店、200」という情報を管理者に伝える。

管理者は現在の時刻を確認し、最終的に次のような情報を台帳に書き込む。

3 行目	20/12/9 14:15:00	小林	宮田商店	200

正当性の検証

取引情報を台帳に書きこむ前に、管理者は次の点を検証する必要がある。

・(本人認証) 利用者のそれぞれに対し、その情報を送ったのが本人であるかどうかを確認する。例えば、管理者と利用者の間で事前に共有したパスワードを知っているかどうかなどで行える
・(残高確認) 送金元の利用者が取引額以上のコインを持っているかどうかを確認する。これは、台帳を最初から順に追っていき、その利用者の残高を計算していくことで行える[2]
・(二重取引の防止) 取引の作業を完了させる前に､同じ利用者から別の取引の連絡があった場合、作業手順によっては、残高が足りないにも関わらず、両方の取引を成立させてしまうということが起こり得る。ただし管理者が 1 人の場合は、作業途中で連絡があった場合でも、今の作業を完了させてから、次の連絡に対応することでこのような二重取引は起こらない[3]

これらの確認が終了した時点で、台帳に書き込み､「取引が正常に完了した」ことを利用者に伝える。

また、台帳が破損したなどの障害に備え、定期的に台帳のコピーを取るなどの対策が必要となる。ただし、この方法だけではコピーした時点から障害の起きた時点までの取引に

2　利用者の口座情報を別に作成し、そこに残高を記録することで再計算の手間は省けるが、記録すべき情報が増えるほか、整合性の問題が生じる。
3　コンピュータが処理する場合、台帳（データベース）が 1 つでも、作業者（プロセス）が複数いることが一般的なので、このようなことが起こり得る。この場合、作業中の読み書きを禁止する（ロック）することで対応できる。

ついては、復旧できないため、複数の台帳とそれぞれに作業者を準備して、常に同じ作業を行わせるなどの対応を併用すると盤石となる。

３－２　複数人で管理する場合（お互いに信頼できる場合）

台帳の管理を１人ではなく、遠隔地にいる複数人で平等に行うことになったとする。平等とは、上下関係がなく、すべての管理者が同じルールに従って作業をし、同一の情報を管理するという意味である。この管理者たちは全員不正を行うこともなく、お互いに信頼しているものとする[4]。

この状況においては、すべての管理者が原則として３－１の手順に従って台帳の記録・管理を行うことで実現できるが、複数人が管理することによって生じる次のような問題に対応しなければならない。

取引情報の伝達方法が一意でない

管理者が１人ではないため、利用者がどの管理者に取引情報を伝達するか、また管理者同士がどの順番でその取引情報を伝達しあうかは様々な方法が考えられる。ここでは、利用者の利便性などを考慮し、利用者がどの管理者に取引情報を送るかは、その利用者が自由に選べるものとする。また、取引情報を受け取った管理者は他のすべての管理者にその取引情報を伝達するものとする。こうすることで、何らかの理由で一部の管理者が作業できない状態にあっても、他の管理者たちで作業をまかなうことができる。

各管理者の受け取る取引情報の記帳順序が異なることが起こり得る

ほぼ同時に複数の管理者が取引情報を受け取った場合、伝達にかかる時間遅延により、各管理者に届く取引情報の順序が管理者ごとに異なることが起こる。そのため、各管理者が取引情報を受け取った順序で処理してしまうと、取引の前後関係が異なった台帳を記録してしまうことになる[5]。また、この遅延を利用して、悪意を持った利用者が異なる複数の管理者に対してほぼ同時に異なる取引情報を伝達することで、二重取引の不正も容易に行えてしまう。

4　この方法が３－１の方法に対して優位性があるわけではないことに注意する。

5　取引情報を最初の管理者が受け取った時刻順で記帳していくという方法も考えられるが、これを実現するにはどこにいてもまったくズレの存在しない時刻を指す時計システムが必要となる。

これを防止するためには、各管理者が受け取った取引情報について正当性の検証を行った後、すぐに完了処理を行うのではなく、一定時間、未完了情報として保留した後、例えば「10分ごと」といったように事前に時間を定めておき、その時刻になったタイミングで保留した情報をまとめて完了処理をする方法が考えられる。

このひとまとまりの取引情報を「ブロック」と呼んで管理することにする。正当性の検証を行っているため、このブロックの中では二重取引などの不正は存在しない。

ただし、あるブロックの完了処理を行う時刻の前後で取引情報が伝達された場合や、ある管理者が台帳の記入を間違えてしまった場合には、ブロックの内容が管理者ごとに異なってしまうことが起こり得る。そこで、完了処理を行う前に、各管理者が作成したブロックを、すべての管理者がお互いに確認しあう必要がある。そのときに内容の異なるブロックが見つかった場合、何らかの合意形成を行って、ブロックの内容を確定させる。

このケースでは、管理者たちはお互いを信頼しているので、話し合ったり、多数決を取ったりして、平和的に解決することができる[6]。ただし多数決の場合は、半数以上の管理者がまったく同じ記帳ミスをしてしまった場合は、誤った情報が記録されてしまうことは当然ながら避けられない。また、管理者の数が多い場合は、多数決を取るにしても、すべての管理者が作成したブロックをすべての管理者の間で伝達しあう必要があり、さらにその結果の連絡にも時間を有する。代表者を決め、すべてのブロックをその代表者の元に集めることで解消することはできるが、これは「平等」という趣旨には反するため、それを許容するかの検討が必要となる[7]。

3－3　複数人で管理する場合（お互いに信頼できない場合）

3－2と同様、台帳の管理を1人ではなく、遠隔地にいる複数人で平等に行うことになったとする。ただし、各管理者が不正を行う可能性は捨てきれず、お互いに信頼しているわけではない。さらに、希望すれば誰でも管理者になれるものとする。

この状況において、すべての管理者が3－1と3－2の手順に従って、台帳の記録・管理を行うとすると、次のような解決が難しい問題が起こり得る。

6　実際のブロックチェーンの運用においてはPBFT（Practical Byzantine Fault Tolerance）などの方法が用いられている。これらの方法では、基本的に多数決による合意形成が行われているため、後述する「結託による不正」に対応することができない。

7　コンピュータシステムの場合、この代表者が単一障害点（ここが故障すると、システム全体に影響を及ぼす箇所）となってしまう。

情報漏洩が起こり得る

管理者が悪意を持って台帳を他者に公開する可能性がある。従って、台帳は公開することを前提とし、そこに記録された情報は、第三者に見られても構わないことを前提としなければいけない。

単純な本人認証の方法が利用できない

パスワードによる認証は、パスワードリストをすべての管理者が持つ必要があるため、この状況では利用しづらい。そこで、取引を行う際に利用者が、署名やハンコを一緒に伝達することで、その取引が本人により行われたものであることを証明するという方法を採用する。もちろん、この署名やハンコは偽造が難しく、かつ、本人であることを誰もが正しく検証できるようなものでなければならない[8]。台帳は公開されているため、この仕組みを利用する場合、誰がどのような取引を行ったかは、誰でも確認できるということが前提となる。

各管理者の台帳内容が同一であることが保証されない

悪意を持って、もしくは何かしらのトラブルによって、過去の記録が改ざんされるということが起こり得る。そのような改ざんを困難にするために、あるブロックを作成するときに、時系列的に１つ前に作成したブロックの内容を要約した情報を、そのブロックに記録するということが考えられる。

これは例えば、あるブロックに記録されている数値すべての平均値を計算して、次のブロックにも書き込むという方法で実現できる。ここでいう数値とは、そのブロックに記録された取引金額の他、前のブロックの平均値自体も含まれる。このように記録されたブロックに含まれる数値を１つだけ改ざんしたとする。するとそのブロックの平均値も変わる。この平均値が次のブロックに記録していた値と異なることを誰かに確認されてしまえば、改ざんしたということがばれてしまう。そこで次のブロックに記録した平均値も改ざんしようとすると、さらにその次ブロックの平均値も変わっていくため、結局、一番新しいブロックまで計算しなおさなければ、改ざんが成功しない。

このような記録方法は、要約情報を通じてブロック同士が次から次に鎖状に連結しているように見えることから「チェイニング」と呼ばれることがある（図１）。なお、これがブロックチェーンの名前の由来である。

8　後述するように「公開鍵暗号方式を利用した電子署名」を利用することで、これを解決できる。

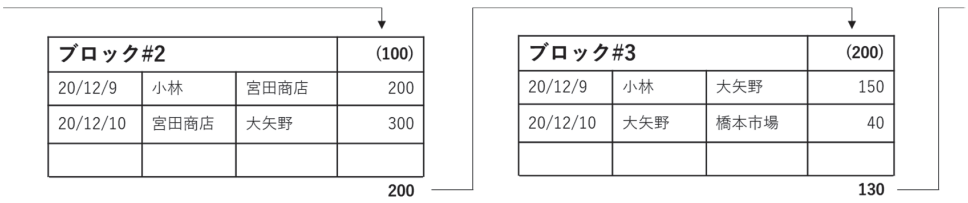

図１　要約値によるブロックの連結

ただし、単純な平均値の計算では、同一ブロック内の複数の数値を改ざんすることで、元の平均値と一致させることは容易であるため、実用的ではない。そこで少しでも改ざんを行うと、その要約情報が予測できない形で大きく変化するものが必要となる。さらに、その計算自体が困難で時間を要するものを利用することで、改ざんそのものを困難することができる。ただし、改ざんの検証に時間がかかってしまうのは良くないため、計算結果が正しいかどうかの確認は容易に行えるものにしなければならない[9]。

改ざん以外にも様々な不正が考えられる

例えば「取引情報をわざと受け取らない」「誤った情報をわざと伝達する」などである。これについては次の項目であわせて説明する。

ブロックの内容が異なった場合の合意形成が容易に行えない

ブロックの内容が異なった場合の合意形成を、３－２で述べたような単純な多数決で行ってしまうと、管理者の半数以上が結託する（不正を行いたい者が仲間を集め、管理者として参加させる）ことで、常に同じ者たちによる決定がなされてしまう。このような「結託による不正」は容易に解決できず、本節で実現したいシステムにおいて、最大の問題となる。そこで多数決を取ることをせず、代わりにすべての管理者の中から「代表者」を１人決めて、その代表者の作成したブロックについて全員で正当性の検証を行い、問題がなければ、そのブロックを採用するという方法を考えてみることにしよう。

常に代表者が同じ管理者だと、「平等」という趣旨に反するため、例えば、毎回くじ引きでこれを決めるものとする。ただし、くじ引きでは仲間が多い方が当たりやすいというのは変わらないため、「結託による不正」は解決しない。

9　後述するように「一方向性ハッシュ関数」を利用することでこれらすべてを解決できる。

そこで、くじが当たりだった場合、その代表者のブロックを採用することに加え、「その代表者にコインを与える（その代表者に新規のコインを発行する、もしくは利用者から台帳利用の手数料を徴収する）」というルールを導入する。つまり代表者になればなるほど「コインが儲かる」ことになるのである。ただし、コインを多く所有したとしても、この台帳システムが破綻した場合は、そのコインに一切の価値はなくなってしまう。するとどうなるか。破綻させないために、すべての管理者たちは必然的に「不正を行わず、正しく作業を行う」ことが望まれるのである。

ただし、単純なくじ引きでは、結局のところ、人を集めるほど当たりやすくなるという「数の原理」は変わらない。そこで他の要因を導入することにより「くじの当たりやすさを変える」方法を考えてみる。他の要因とは、例えば「持っているコインの総量」「信頼性」、そして「計算力」などであり[10]、これらが高いほど「くじが当たりやすくなる」仕組みを導入する。「計算力」であれば、何かしらの難しい計算を全員で同時に行い、正しい結果を一番早く求めたものが代表者に選ばれるという方法で実現できる。これらを高めることは、人を集めるほど容易でないだろう[11]。この手順は「ひたすら掘る（計算する）ことでコインを発掘できる」ことに例えて「マイニング」と呼ばれる。また「計算（仕事）を多くした者に対して、ブロックを作る権利を与える」という基準は「プルーフオブワーク」と呼ばれる。

このような仕組みを導入することで「その要因を上げれば、コインが儲かる」と各管理者が考え、そこに競争力が生じる。結果、「競争しながらも、みんなで仲良く、正しく」この台帳システムを管理していくという環境が成立する[12]。

---

10 「計算力」を導入する場合に、くじ的な要素を持たせる、かつ、計算結果の正しさを他の管理者たちが検証するために、この計算は「計算自体は単純でも、総当たり的にしか導出できないため時間がかかり、かつ、正しいかどうかの検証はすぐに行える」ものでなければならない。これはチェイニングで望まれるものと同様のものである。ビットコインにおいては、チェイニングとマイニングという２つの異なる処理を、後述する「一方向性ハッシュ関数による計算」によって統合的に行っていることが面白い点である。

11 現実的にそうとは言い切れないが、これはコンピュータでの話において「人を集める」とはコンピュータの台数を増やすことではなく、起動するプログラム（もしくは接続する IP アドレス）を増やすことに対応しているためである。これらが容易であることから、本文のような表現となっている。

12 この状況であってもブロックが唯一に合意できない状況は発生する。この場合、ブロックを分岐させてしまい、その後、何かしらの基準によってどちらかの分岐のみを採用するという方法が採られることが多い。この説明については「人力システム」で例えると不自然な例えとなるので、本章では省略する。

３－４　ブロックチェーンとの対応関係

ここまでに説明した方法により、台帳の管理を平等で複数の管理者によって協力して行い、その中に信頼できない者が存在したとしても、不正な記録（二重取引）や、記録された情報の改ざんが起きにくい形で行える。これにより「記録した情報に通貨のような価値を持たせて、直接譲渡できるシステム」を実現できる。

各項で述べた方法について、コンピュータシステムとの対応関係を示す。３－１の方法は、前述したように、旧来のサーバークライアント方式によるデータ管理方法に対応する。３－２の方法は、「コンソーシアム型」のブロックチェーンに対応する。そして３－３の方法が、ビットコインなどの暗号資産で利用されている「パブリック型」のブロックチェーンに対応するのである。この分類については、第３部「３．２ ブロックチェーンの活用事例から見るその技術的側面」[8] にて説明する。

最後に、従来の情報管理方法との違いを改めて確認するため、ブロックチェーンの新規性について [2] より引用する。

ブロックチェーンの新規性は、不特定多数が仮想通貨による報酬をインセンティブとして時系列順にハッシュ値で繋がれたデータを保持し合うことにより、過去時点におけるデータの存在性および真正性の証明を特定の企業／組織体の信用に依拠せず実現した点にある。

４．要素技術

本節では話をコンピュータシステムに戻し、ブロックチェーンで利用される要素技術について簡単に説明する。

４－１　一方向性ハッシュ関数

ハッシュ関数とは、任意のデータを入力することで、より短い数値データを得ることができる関数（操作）のことである。元のデータの特徴をよりサイズの小さいデータで表現できることから、データ同士の同一性の検証や検索の高速化などに利用される。ハッシュ関数に入力して得られた数値をハッシュ値と呼ぶ。

一方向性ハッシュ関数とは、ハッシュ関数により得られた数値データから、元となるデータを導出することが非常に困難であるハッシュ関数を指す。暗号技術で利用されることが

多く、この場合、次のような性質を持つように設計される。

・入力データと出力値の間に規則性がなく、入力が少しでも異なればまったく異なるハッシュ値となる
・特定のハッシュ値が得られるような入力データを効率よく求めることはできない
・同じハッシュ値となる別の入力データを効率よく求めることはできない

ブロックチェーンのチェイニングとマイニングには、256 ビットの数値（最大値は 10 進法で 78 桁）を出力する SHA-256 などが利用される。また、プルーフオブワークを基準としたマイニングでは

・ブロックに記録するデータに、何かしらの意味のないデータ（ナンス）を加えたものを、一方向性ハッシュ関数の入力とし、得られたハッシュ値が定められた数値より小さい出力が得られたのであれば、そのナンスを答えとする

という計算を行う。上記の性質より、どのようなナンスが答えになるかに規則性ないため、答えを求めるためには条件を満たすナンスを総当たり的に見つけていく必要がある。

４－２　公開鍵暗号方式を利用した電子署名

古くから使われている暗号（共通鍵暗号方式）において、２者間で暗号化した文章を送りあうとき、暗号化（データから暗号文を作り出す）と復号（暗号文を元のデータに戻す）の手順には、お互いが知っているパスワードのような文字列が必要であった。この文字列は「鍵」と呼ばれる。

公開鍵暗号方式とは、暗号化に必要な鍵と、復号に使われる鍵が異なる暗号方式である。前者を秘密鍵、後者を公開鍵と呼ぶ。これらはペアとして利用者に割り当てられる。その名の通り、秘密鍵は本人が秘密にしなければならないもので、公開鍵は広く公開するものである。ある相手に暗号文を送りたいときは、その相手の公開鍵で暗号化を行い、その相手は秘密鍵で復号を行うことができる。

公開鍵暗号方式の暗号方法のうち、公開鍵と秘密鍵を入れ替えても同様の手順が実行できるものが存在する。これを次のように用いることで電子署名が実現できる。

1. 署名したい文章をハッシュ関数に入力し[13]、得られたハッシュ値を自身の秘密鍵を利用して暗号化の手順を行う
2. 得られたデータを署名とし、元の文章に添付して公開する
3. 署名を検証したい場合、相手の公開鍵を利用して、署名に復号手順を行う
4. 得られた数値が、元の文章のハッシュ値と等しければ、「その署名をしたものは、その本人の秘密鍵を持つ者である」ことが証明できる

「その秘密鍵を持つ者」と強調したのは、秘密鍵を盗まれたり漏洩したりしてしまえば、署名が無意味になってしまうからである。秘密鍵は数値データであるが、特に暗号資産（仮想通貨）に利用するものは、それこそ金庫の鍵のように厳重に保管する必要がある。

4－3　スマートコントラクト

スマートコントラクトは、正確に定義するのは難しいが、一般的にコンピュータネットワーク上で自動的に契約処理を行う概念や機能を指す。ブロックチェーンの主要な用途であり、ブロックチェーンの活用事例はスマートコントラクトの実現を前提としている。なお、スマートコントラクトという考え方自体はブロックチェーンの登場以前より存在している。

前述したように、ブロックチェーン自体は情報を記録するデータベースでしかないが、そのデータベースに、プログラムの動作手順を記録できるようにし、そのプログラムを任意に実行できるような仕組みを導入することで、スマートコントラクトが実現される。このプログラムが実行されたとき、その結果もブロックチェーンに記録されていく。これにより、従来のサーバークライアント方式のように中央集権的な管理者がいない元で、任意のプログラムを実行し、その手順や出力結果が改ざんされていないことをすべての管理者で保証する環境が実現できるのである。スマートコントラクトの詳細は、第３部「３．２ブロックチェーンの活用事例から見るその技術的側面」［8］にて説明する。

13　この手順は署名データを小さいものにするために行われる。

５．ブロックチェーンを利用する場合の技術的問題点

本節ではブロックチェーンの利用するときの、技術的問題点を、本章で説明した範囲に絞り簡単に述べる。

記録するデータの大きさを制限しなければならない

３－２で述べたように、ブロックチェーンに管理者として参加している全部のコンピュータは、原則としてすべての取引履歴を保持するため、そのサイズは莫大なものとなる。さらに書き込まれたデータを後から削除することはできない。そのことを十分に理解した上で、必要最低限の情報を記録するような形のシステムを設計する必要がある。

情報の伝達後、すぐに記録として反映されるわけではない

３－２で述べたように、利用者が伝達した取引情報は、一定時間、未完了情報として保留された後に、ブロックに記録される。完了処理が行われるのは早くともブロックが作成される時点（ビットコインでは 10 分間隔）である[14]。

プライバシー対策は厳格ではない

３－３にて「この仕組みを利用する場合、誰がどのような取引を行ったかは、誰でも確認できるということが前提となる」と述べた。これについては公開鍵暗号方式を利用した電子署名を利用することで一応の解決は行われている。公開鍵暗号方式において、公開鍵と秘密鍵のペアは誰でも容易に生成することができ、第三者機関に個人情報を伝えたりする必要はない。つまり、公開鍵（署名）と個人情報を結びつけなければ、少なくとも「誰が」取引をしたのかを知られることはない。

ただし、「同一の署名を持つ者が、いつ、誰と、いくらの取引を行った」のかは、すべて公開されているため、その情報を抽出することで、行動履歴の推測や、場合によっては個人の特定を行われてしまう可能性がある。

14　前述したように、ブロックの内容が合意できず、ブロックを分岐が発生することもあり、この場合の完了処理はさらに時間がかかる。

51％攻撃

プルーフオブワークなどの基準を導入することで「数の原理」を解決したかのように説明したが、実際は、その基準において過半数（51%）以上を掌握している管理者が不正を行うことは可能である。ビットコインのような大規模で運営されている暗号資産であれば、そのようなことは起こりにくいが、規模の小さい暗号資産で、そのような攻撃が実際に行われている［7］。

6．まとめ

本章では、ブロックチェーンの技術的側面について、なるべく平易な説明を試みた。ウェブでブロックチェーンについて検索してみても、曖昧な説明で行っているページが多く、正確に理解するには骨が折れる。本章が特に暗号技術に詳しくない方が技術理解のきっかけにして頂ければ幸いである。なお、本章を執筆するにあたり文献［1］-［6］を参考にした。

参考文献

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

［2］岩下直行，“暗号資産への脅威と対策― ビットコインの社会への展開による変質―，”デジタルプラクティス，Vol.10 No.3, 情報処理学会，2019.

［3］近藤真史，“証券業界におけるブロックチェーンの活用に向けた検討とオープンイノベーションの推進，”デジタルプラクティス，Vol.10 No.3, 情報処理学会，2019.

［4］アンドレアス・M・アントノプロス（著），今井崇也（訳），鳩貝淳一郎（訳），“ビットコインとブロックチェーン：暗号通貨を支える技術，”NTT 出版，2016.

［5］松尾真一郎ほか，“ブロックチェーン技術の未解決問題，”日経 BP 社，2018.

［6］樋口匡俊，“ビットコイン論文からさぐる ブロックチェーンのヒント，”https://www.ogis-ri.co.jp/otc/hiroba/technical/bitcoinpaper/（2021 年 1 月 10 日閲覧）

［7］井上輝一，“モナコインへの攻撃、なぜ成功？　小さな「アルトコイン」襲う巨大なハッシュパワー，”https://www.itmedia.co.jp/news/articles/1806/04/news122.html, ITmedia 2018/06/04（2021 年 1 月 10 日閲覧）

［8］小林直人，“ブロックチェーンの活用事例から見るその技術的側面，”国府台経済研究第 31 巻第 2 号，2021.