ブロックチェーンの仕組みと課題

鎌田光宣

千葉商科大学人間社会学部

kamata@cuc.ac.jp

要旨　ブロックチェーン技術の仕組みを活用したものの代表がビットコインやイーサリアムといった仮想通貨（暗号資産）である。このお金はどこかの企業が発行したものではなく、管理している明確な組織がないにもかかわらず、しっかりと信用された取引を行うことができるのである。本稿ではブロックチェーンの概要、歴史、課題について説明したあと、ブロックチェーンの今後について考察する。

キーワード　ビットコイン ブロックチェーン 歴史 分散台帳システム

1　ブロックチェーンの概要

ブロックチェーンでは、ある大きさのデータの塊（ブロック）がいくつもチェーン状に繋がっている。物理的なチェーンが存在するわけではなく、ブロックのヘッダー部に、直前のブロックがどれか分かるような情報が記載されている。ここに暗号技術や分散システムの技術を取り入れることで、一度書き込まれたデータは、たとえシステム管理者であってもあとから改竄 (かいざん) することはできないシステムとなる。

ブロックチェーンの特徴を簡単にまとめると、次のようになる。[1]

- 分散型データベースである
- 非中央集権型である
- 書き込み専用・改ざん困難である

ブロックチェーンは、多数のノードが同じデータを共有している。つまりデータを冗長化して保存して稼働しているため、どこかのノードやネットワークに障害が発生しても動き続けることができるシステムである。また、改竄の検出が容易であるという特徴を持つ。

非中央集権型というのは、中央の管理者がいない状態のことを指す。特定役割を持つサーバーが中央にあるわけではなく、大量のユーザーがブロックチェーンを共有する状態である。中央集権型とは違い、管理者が独裁的に管理するということができないため、利用者は信頼できない管理者の存在を気にしなくて良い。お互いに信用できない者どうしであっても、不正があることを心配することなく安心して取引を行える仕組みとなっている。

ブロックチェーンの中を見ると、１つのブロックには多数のトランザクションが含まれており、その中には、どの口座からどの口座にいくら送るか、という情報が書かれている。

ブロックチェーン自体は残高を管理しておらず、利用者が誰なのか、残高はいくらなのか記載されていない。利用者が自分の残高を知りたいときは、自分のウォレットアドレスに関係する取引データを集めて、未使用分の残高である UTXO(Unspent Transaction Output) を求める必要がある。ある金額を相手に送りたいときは、送金するのに十分な残高のある UTXO を入力側に置き、送金したい相手のウォレットアドレスと金額を出力側に置く。入力側、出力側ともに複数の宛先を指定することができ、UTXO と送金額の差額は自分のウォレットアドレス宛に送るよう出力側に配置する。ブロックチェーンには、この取引の記録が延々と綴られているのである。

2　マイニング

ブロックチェーンでは、マイナー（採掘者）と呼ばれるノードがトランザクションを集めてブロックに詰め、それをブロックチェーンに追加する、マイニングと呼ばれる作業を行っている。マイナーは、ブロック追加の成功報酬と送金の手数料を手に入れることができる。

ビットコインのトランザクションの中身を見ると、必ずしも送る側からの入力と受ける側への出力が一致しておらず、その差額は手数料としてマイナーに支払われる報酬になる。この手数料の金額はトランザクションを作る人、すなわち送金する人が自由に決めて良いことになっている。手数料を 0 にしたり、安く設定したりすることもできるが、手数料が安いと、トランザクションをブロッ

クチェーンに取り込んでもらえない（いつまでたっても取引が承認されない）可能性が高くなる。

ブロックチェーンでは、保存されているデータの耐改竄性を担保する仕組みとしてハッシュ値が用いられている。ブロックの中には多数のトランザクションが格納され、トランザクションの中身には、送信者の電子署名と公開鍵、送金する金額、送金先のウォレットアドレスなどが含まれる。これらのトランザクションに加え、前のブロックのハッシュ値と、さらにノンス（Nonce）と呼ばれる値を加えてハッシュ値を求める。これらはすべてブロックの中に取り込まれ、永久に保管されることになる。途中のデータの改竄を行おうとしても、1 ビットでもデータが変わるとそのブロック以降に含まれるハッシュ値がすべて不整合を起こすことになるため、不正を行うことは事実上不可能である。

ビットコインでは、ハッシュ値の先頭が所定数の「0」の並びになるノンスを求める作業を各ノードで行っている。ノンスを変えて、何度も何度もハッシュ値を求め、ハッシュ値の先頭が所定数の「0」の並びになるノンスを発見すると、ブロックを追加し、コインを新規発行することができる仕組みになっている。この作業はマイニング（採掘）と呼ばれ、時間と電力をかけて行っている処理の正体である。

3　ブロックチェーンの歴史

ブロックチェーンの元となったアイデアは、1991 年の Stuart Haber と W. Scott Stornetta の研究 [3] に遡る。デジタル文書にタイムスタンプを付けることによって、日付が遡ったり、改竄されたりを防ぐというものである。このシステムでは、暗号化され、鎖のように繋がったブロックを使用してタイムスタンプの付いた文書を保存し、複数の文書を 1 つのブロックにまとめることが行われた。

1999 年の Markus Jakobsson と Ari Juels の論文に PoW(Proof of Work) という言葉が登場した [4]。サービスを受ける側に、コンピューターによる処理時間を要求することで、DoS 攻撃や迷惑メールの送信を抑えようとする仕組みである。2004 年には Hal Finney がリユーザブル Proof of Work(RPoW) と呼ばれるシステムを発表した。Web サイトのユーザーが使用した PoW トークンを、新しい未使用の RPoW トークンと交換でき、その後同様に RPoW トークンの受け入れ態勢が整っている第三者のウェブサイトで使用できるというものである。

ビットコインの始まりは 2008 年に Satoshi Nakamoto と名乗る人物が発表した論文 [5] である。最大の特徴は、中心となる運営者が存在しないということである。

その後、ブロックチェーンにさまざまな機能を持たせて仮想通貨以外の分野にも応用しようとする動きが起こる。イーサリアムは、ループ処理などを含む複雑なアプリケーションを開発し、実行できる機能を実現した。さらに、イーサリアムの機能を利用することで、イーサリアムのブロックチェーン上でオリジナルの仮想通貨を簡単に作成・発行できるようになった。これにより、新たな仮想通貨が爆発的に増えることになった。

4　ブロックチェーンの課題

4.1　安全性

暗号資産はウォレットの秘密鍵がなければ勝手に使われることはない。しかしながら、秘密鍵が盗難されると全て犯罪者の手に渡ってしまう。ウェブウォレットや取引所のウォレットを利用している場合、秘密鍵がサービス事業者側に知られていることになるため、自分がいくら気を付けていても事業者側で盗難される可能性がゼロではない。実際に、2014 年に起こったマウントゴックス事件では、利用者に落ち度がなく、事業者の内部でビットコインが盗まれた。

巨大なマイニングプールの存在も安全性に影を落としている。ビットコインをはじめメジャーなブロックチェーンにおいて、個人がマイニング競争に勝つことは事実上不可能である。どこかのマイニングプールに参加して、チームの一員として報酬を得るしかない。マイニングプールとは、マイナーを集めた巨大なマイナー集団で、マイニングが成功して報酬が得られると、その貢献度に応じて各マイナーに報酬が分配される仕組みになっている。このマイニングプールが巨大になったため、現在のビットコインではいくつかのマイニングプールが談合すれば、不正なブロックを故意に追加することも不可能ではない状態になっている。

4.2　スケーラビリティ

多数のユーザーが一度にブロックチェーンを利用すると、ブロックチェーンの処理能力が追い付かなくなることがある。トランザクションの遅延が発生すると、ユーザーはより早くトランザクションを処理してもらうために手数料を高く設定するという状況が起こり、手数料が高騰してゆく。ブロックチェーンでは、システムの処理量が増加したときにノードを増やしても、1 つのノードが処理するタスク量は減らないため、システム全体の処

理能力は変わらないままである。

4.3 ダブルスペント（二重送金）問題

ビットコインのブロック追加速度はおおよそ 10 分間隔で、さらに確定するには 6 ブロックほど待つ必要がある。しかしながら、そこまで顧客を店舗で待たせるわけにはいかず、トランザクションが承認されていないことを承知で顧客にモノを売ることになる。この運用を「ゼロ・コンファメーション（0-comfirmation）」と呼ぶ。

ビットコインでは、手数料が低く設定されたトランザクションは、いつまでたってもブロックチェーンに取り込まれない、という事態が起こる。そのような事態への救済措置として、「RBF」(Replace by Fee) という仕組みが導入された。後から手数料を高く設定しなおしたトランザクションを送ることで、先に送ったトランザクションを取り消せる、というものである。しかし、この RBF を導入したせいで、ビットコインは意図的なダブルスペント（二重送金）ができてしまう状況になってしまった。

4.4 消費電力

PoW の仕組みを取り入れているブロックチェーンでは、マイナーはチェーンに新しいブロックを追加して報酬を得るため、無意味ともいえる計算で莫大な電力を浪費している。

ビットコインのマイニングに使われる消費電力が、世界の電力消費の 0.25%に達するというデータもある。SDGs の面でも、例えば PoW を PoS に変えて消費電力を減らすなどの対策が求められる。

5 ブロックチェーンの今後

即応が必要なものは、いまのところブロックチェーンに向いていない。ブロックチェーン上で動く分散アプリケーション（DApps）は、いちどブロックチェーンに載せてしまうと変更ができないため、頻繁にシステムに変更を加える用途には向かない。また、秘匿性の高い情報については、たとえそれを暗号化したとしても、パブリックに流すというのは不要なリスクを生むことになる。容量の大きなものの流通にも向いていない。

ブロックチェーンの優れたところは、非中央集権型であり、データの改竄ができず、参加者がみんなで検証できるというものである。信頼していない者同士で構成されたネットワークで、不正があることを心配することなく安心して取引を行えるのである。

法定通貨の信用度が低い地域、例えば偽札が多く出回っていたり、通貨の価値が乱高下したりするようなところでは、ブロックチェーンによる暗号資産の評価が高い。現状では日常の決済に向いているとは言い難く、決済の高速化を図る仕組みの開発が期待される。

電子投票システムには、ブロックチェーンの耐改竄性がぴったりと当てはまる。いつ、誰が、何に投票したのかをブロックチェーンに記録することで、不正の余地をゼロに近づけることができる。ただし、本人確認をバイオメトリクス認証などを用いて厳格に行う必要があり、また、「誰が、何に」の情報は、個人のプライバシーとして保護されるべきものであるため、記録を検証できる人物や団体は限定される可能性がある。

電子データ化された証憑書類の保存の用途にもブロックチェーンは有効である。現在利用されている電子署名や電子証明書は、それを認証する認証局自体の信頼性や安全性が問われるが、例えばハッシュ値や電子署名をブロックチェーンに記録しておけば、書類自体はブロックチェーンの外にあっても改竄の有無を確認することができる。

ブロックチェーンは新しい技術や仕組みが取り入れられ日進月歩で進化を続けているが、万能ではない。ブロックチェーンが得意とする分野とそうでない分野をしっかりと把握した上で、活用方法を模索していく必要がある。

参考文献

[1] 鎌田光宣, “ブロックチェーン技術の歴史と展望”, 国府台経済研究,31 巻 2 号（掲載予定）

[2] 「ブロックチェーンの定義」を公開しました, https://jba-web.jp/news/642, 日本ブロックチェーン協会　(2021 年 1 月 5 日参照)

[3] Stuart Haber & W. Scott Stornetta, “How to timestamp a digital document”, Journal of Cryptology volume 3, pages99–111(1991)

[4] Jakobsson, Markus; Juels, Ari. “Proofs of Work and Bread Pudding Protocols”. Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers: 258–272. (1999)

[5] Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/ bitcoin.pdf (24 May 2009)(2021 年 1 月 10 日閲覧)