卒業研究レポート

～ビットコインとブロックチェーンの数理～

2019 年 2 月 26 日

明治大学　総合数理学部　現象数理学科

学籍番号　2610140006

山口瞳

目次

1.イントロダクション

1.2.概要

2.準備

2.1.ハッシュ

2.2.公開鍵暗号

2.3.電子署名

3.ビットコインの取引の流れ

3.1.取引情報（トランザクション）

3.2.トランザクションの送付

3.3.トランザクション内での電子署名

3.4.確認依頼

4.ブロックの連結

4.1.マイナーの役割と **NONCE** について

5.まとめ

【参考文献】

1.イントロダンクション

近年話題になっている仮想通貨。2018 年の年始頃、私はその流行りにのっかり仮想通貨を投機買いしようと考えていた。しかし、世界で初めての電子決済システムとなれば、管理上の不安からどのような仕組みで動いているのか、興味をもった。そこで色々と調べるうちにどうやら仮想通貨はブロックチェーンという技術を基盤に成り立っているらしい、ということが分かった。そしてそのブロックチェーンは仮想通貨の基盤とされる以外にも、最近では知的財産の管理、遊休施設のシェアリング、そのほか各種届出や登記など、さまざまなアプリケーションにブロックチェーン技術を使えることが分かってきている。経済産業省の試算によると、日本国内におけるブロックチェーン関連の市場規模は 67 兆円に達すると予測されていた。私は、近い未来、自分たちの生活に身近になるとされるブロックチェーンをより深く理解したいと考え今回このテーマの元、ブロックチェーンについて調査を行った。そして、開発元であるナカモトサトシの論文[4]を元に、仮想通貨がどのような流れで成り立っているのかやブロクチェーンの仕組みについて説明していきたいと思う。仮想通貨といっても、ナカモトサトシの論文ではビットコインという仮想通貨を元にブロックチェーン技術について説いている。そのため、今回私はビットコインがどのような仕組みで成り立っているのかを説明しようと思う。

1.2.概要説明

まず、ブロックチェーンとは。
日本ブロックチェーン協会が定めている定義が次の通りである。
１）「ビザンチン障害（１）を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が 0 へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ。」
２）「電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。」

以下、レポートにて説明をしない用語について解説しておく。
（1）ビザンチン障害
相互に通信しあう何らかのオブジェクト群において、通信および個々のオブジェクトが故障または故意によって偽の情報を伝達する可能性がある場合に、全体として正しい合意を形成できるかを問う問題のこと[9]
（2）プロトコル
複数の者が対象となる事項を確実に実行するための手順について定めたもの[10]

上記の定義以外にも、ブロックチェーンでよく表現される言い方は「みんなが見れる『台帳』」である。台帳とはブロックと呼ばれる取引情報記録の塊のことを示している。そして、そのブロックがいくつも鎖のように繋がっているためにブロックチェーンと呼ばれている。
特徴としては以下があげられる。
1、　複数のコンピューター上に分散してデータを保持している
2、　暗号学的技術を駆使することで改竄がほぼ不可能である
3、　同じ機能を複数用意することで1つが壊れたり、止まってもシステム自体は壊れず、止まらない。
4、　全員が同じデータをバケツリレーのようにコピーしあい、それぞれが個人的にシステムを動かしている

ナカモトサトシさんの論文ではこの技術を「ビットコイン」という仮想通貨にて活用する方法とともに説いている。そこでビットコインについても簡単に概要を説明する。

ビットコインとは。
ブロックチェーン技術を利用し実現した、世界で最初の「電子決済システム」である。銀行などの第三者を仲介することなく個人間でお金のやりとり出来ることや少額の手数料で海外送金を可能にしたことから、その利便性に需要が高まり、爆発的に話題になった。ビットコインは円やドルとは違い発行数に上限がある。コインの発行可能総数は2100万コインであり、2018年4月26日まで

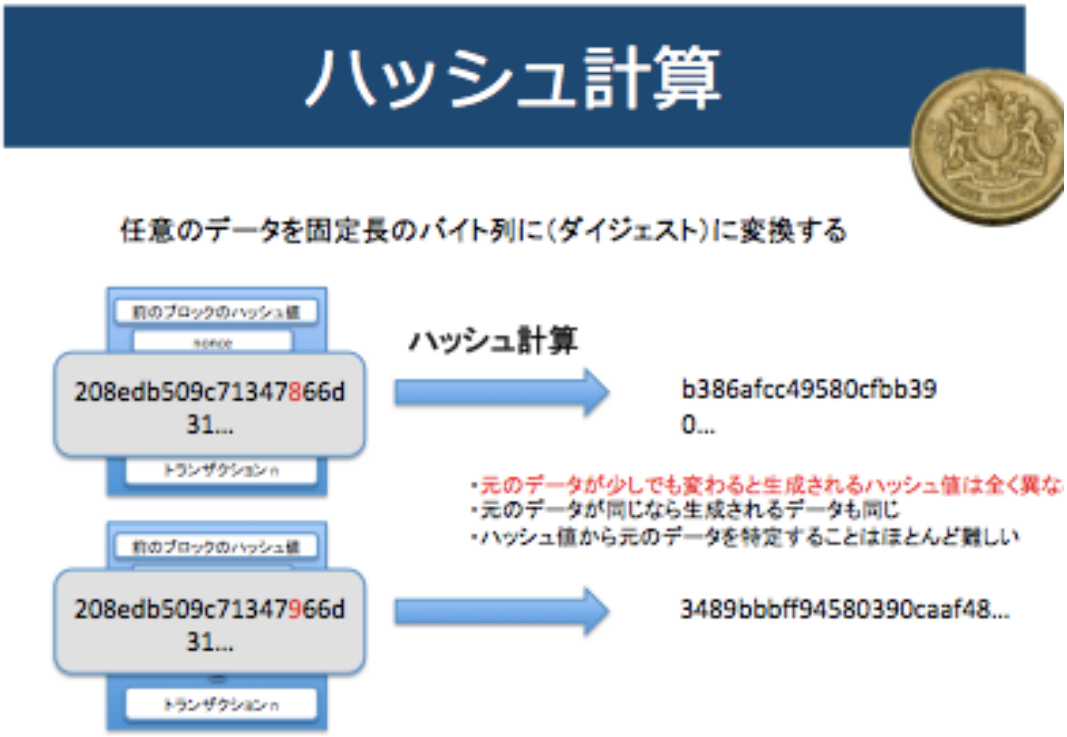
に 1700 万ビットコイン発行済みだ。発行枚数に上限があるのは、コインが既定以上流通されないことでインフレを防ぐのが目的と言われている。

2.準備　Preliminaries

ブロックチェーンの仕組みを説明する上で使用する単語の意味などをまず始めに解説しておこうと思う。

2.1.ハッシュ

ブロックチェーンではハッシュ関数を利用しており、「ハッシュ関数をかける」というのは、元のデータから特定の別のデータを計算によってつくることである。
計算に使う関数をハッシュ関数、計算によって求められた別のデータをハッシュ値という。どんなハッシュ関数を使うかによって得られるハッシュ値が異なり、ビットコインで使用されるハッシュ関数は SHA256 と RIPEMD160 である。これらのハッシュは GPU や計算専用のハードウェアである ASIC で計算するのに向いている。これに対し、他の（ビットコイン以外で利用されている）ブロックチェーンでは普通の PC でも使いやすいように、GPU や ASIC では計算しづらいハッシュアルゴリズムを使っているものも多く存在しているようだ。



（図１）

特徴として、同じデータを入力値としてハッシュ計算すれば、そのデータが１バイトでも１メガバイトでも１ギガバイトでも出力値は常に16進数表記として64桁と固定されている。そして、異なるデータからハッシュ計算され、同じ値になることは２の256乗分の１という天文学的な確率でしか起きないとされている。

（ちなみに、2017年２月にグーグルが最初の衝突例を発見するまで２２年間かかった。このとき要した計算回数は900京回以上に及び、一般的なCPUで言えば6500年である。）

そして、ハッシュ値は一方向性関数である。一度ハッシュ関数を適用してハッシュ値をだしてしまったら、どうやっても元のデータに戻すことは出来ない。

例えば、ある人が暗号化された機密文書を復合する際に「abc」というパスワードを使用したとする。このとき「abc」というパスワードをPCに打ち込む行為によって機密文書は、第３者に見られてしまう可能性がある。悪意のある攻撃者によってサーバコンピュータなどに不正アクセスが行われ、パスワードが漏れてしまうリスクがあるからだ。ここでハッシュが大いに役に立つのである。

それは「abc」をハッシュ値にしてしまい、これを PC 上に保存しておくのだ。仮に悪意のある人が PC の不正侵入に成功したとしても､ハッシュ関数は一方向性関数の特性があるのでハッシュ値から得られるのはハッシュ値であり、本来のパスワードは盗み取られない。
ハッシュ関数はもとのデータが同じである場合、必ず同じハッシュ値を作り出すので正規の利用者が機密文書を復号化するため「abc」と入力すれば、それが本人か否か確かめる認証システムは「abc」をハッシュ関数にかけ、正しいハッシュ値をだし、機密文書を復号化できるのである。
ブロクチェーンではこの特性を最大限に利用している。

2.2.公開鍵暗号

次に「公開鍵暗号」というものを説明する。ブロックチェーンではこの公開鍵暗号を用いて「データ暗号化」（このレポートの 3.2.にて説明）と「電子署名」（2.3.にて説明）を行なっている。その２つの仕組みを説明する前に公開鍵暗号について述べる。

公開鍵暗号は対になる「公開鍵」と「秘密鍵」という 2 種類の鍵を利用してデータを暗号化し、復号できるようにする暗号方式のことを指す。
公開鍵は公開されている誰でも取得できる鍵だが、秘密鍵は公開鍵の作成者だけが保持している鍵である。そして公開鍵によって文書やデータは暗号化され、そのペアである秘密鍵だけがその暗号化されたものを解くことができる。（逆も然り。ただし公開鍵は公開するものなので、逆の使い方は暗号としての意味を持たなくなる。）
ブロックチェーンでは公開鍵暗号方式を取引する際のシステムにおいて採用している。

2.3.電子署名

公開鍵暗号を用いて行われる「データ暗号化」と「電子署名」のうち電子署名（デジタル署名とも呼ばれる）について先に説明する。
電子署名とは、サインのように自分が合意した証をつけたいデータや文書のハ

ッシュ値を得て、そのハッシュ値を公開鍵暗号を用いて暗号化した暗号文のことである。
例えば、文書の送信者が鍵ペアを作るとする。手元に秘密鍵を残し、公開鍵は公開してしまう。そして、秘密鍵で文書の暗号化を行う。これが電子署名になるのだ。署名した文書をメールなどで送ると、受け取った受信者は公開鍵でそれを復号する。
この話だけを聞くと電子署名は何の意味も持たないように聞こえるだろう。暗号の仕組みを応用してはいるけれど、暗号とは似て非なるものである。ではどのようにしてこの技術がブロックチェーンの一部として使われているのか、後に説明する。（レポート内の 3.3.にて）

3. ビットコインの取引の流れ

では、実際にどのような流れでビットコインの取引が行われているか例をあげて説明する。

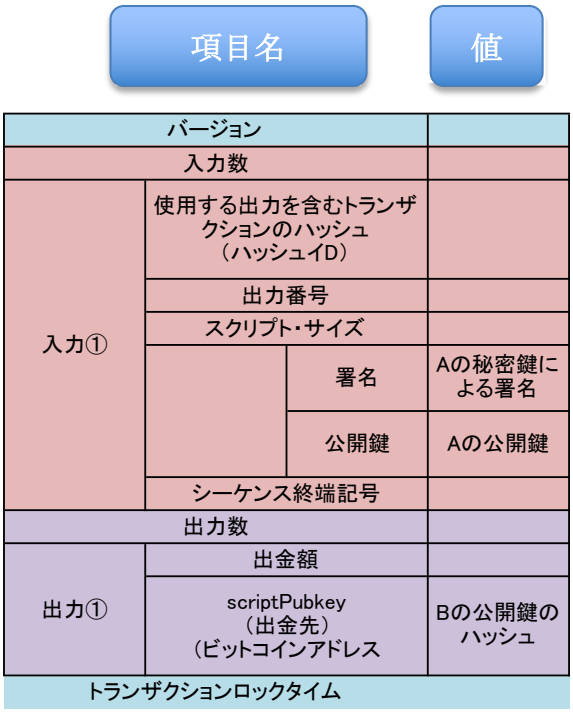
（図２）

上の図は A（アヒル）が B（ねこ）へ 10BTC の送金をする場合を例にあげている。その流れとしては、
① 取引情報を A が作成

② 取引情報を A が B へ送付
③ 取引情報を A が維持管理ネットワークへ送付→取引が正当であることの承認依頼
④ 維持ネットワークにて確認者たちの承認（複数の取引情報をまとめたブロック単位で承認）
⑤ 取引の確定
ここまできてやっと、B が 10BTC を使用可能となる。

3.1 取引情報（トランザクション）

まずは図２の「①作成」と「②送付」で、取引情報（決済データ）の作成をし、B と取引をする流れから説明する。
ビットコインでは取引内容（トランザクションと呼ばれるもの）は下のような構成になっている。



（図３）

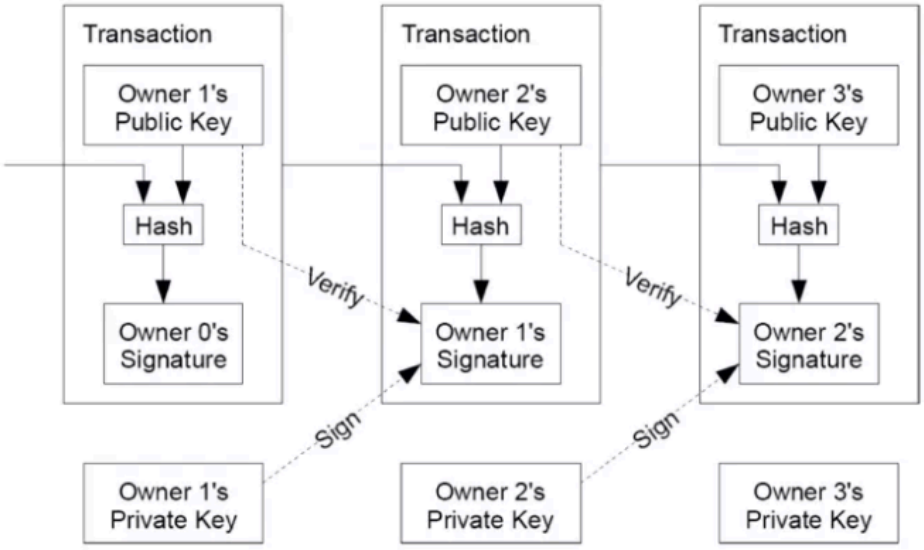
◆左の列から
バージョン（４バイト）：どのルールに従うか指定
入力数（１～９バイト）：トランザクション入力の数
入力（複数）：トランザクションの入力
出力数（１～９バイト）：トランザクションの出力の数
出力（複数）：トランザクション出力
トランザクションロックタイム（４バイト）：ブロクチェーンに追加されうる最も早い時間
を定義（通常０：即時追加）

◆中央の列
トランザクション・ハッシュ（トランザクション ID）（４２バイト）：入金に使用する未使用出力（出金）を含むトランザクションへのポインタ
出力番号（４バイト）：入金に使用する未使用出力（出金）のインデックス番号（何番目の出力か）
スクリプトサイズ（１～９バイト）：スクリプトの長さ（バイト単位）
ScriptSig(署名スクリプト)（可変長）：入金に使用する未使用出力（出金）の使用条件を満たすスクリプト
シーケンス終端記号：FFFFFFFF に設定される

※未使用出力…UTXO（Unspent Transaction Output）
※ポインタ…あるオブジェクトがなんらかの論理的位置情報でアクセスできるとき、それを指し示すもの
※署名スクリプト…デジタル署名ブロックがコメントとしてスクリプトに書き込まれる

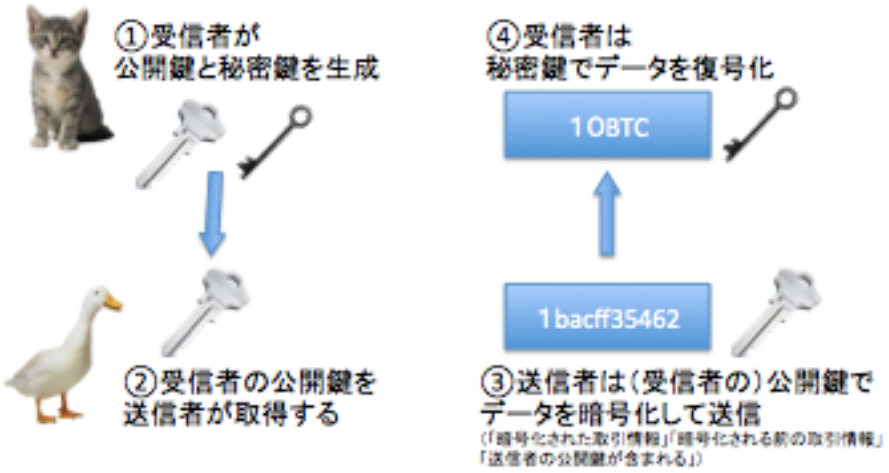
3.2.トランザクションの送付

以下、（ナカモトサトシの論文より拝借）トランザクション送付の流れを示した図である。



（図 4）

「Public Key」と「Private Key」と呼ばれる鍵が、先に説明した公開鍵暗号技術の「公開鍵」と「秘密鍵」である。
この公開鍵暗号を用いてブロックチェーンのシステム内で行われるトランザクションの送付の流れを分かりやすく以下の図に置き換えてみた。



（図５）

① コインの受信者が公開鍵暗号の秘密鍵と公開鍵のペアを生成する。
（ちなみに、ビットコインでは秘密鍵から公開鍵を生成する際に secp256k1 という楕円曲線を利用している。）
②受信者のもつ秘密鍵と対になる公開鍵をコインの送信者が取得する。
③送信者はその公開鍵を使ってトランザクションを暗号化して受信者に送信する。
③受信者は自身の秘密鍵でデータを復号化し、トランザクションを取得する。

3.3 トランザクション内での電子署名

図５の④で復号化されたデータが「本当に送信者から送られてきたものなのか」を検証するために、2.3.で説明した「電子署名」によって、確認される。

（図６）

送信者は（以後 A とする）受信者（以後 B とする）の公開鍵によって暗号化されたデータ（図５の③）に「トランザクションのハッシュ値を A の秘密鍵で暗号化したデータ」を追加し、これを B に送る。B は自らの秘密鍵を使って「公開鍵で暗号化されたデータ」を復号すると同時に、A の公開鍵（図３.トランザクション内にある）を使って「A の秘密鍵によって暗号化されたデータ」を復号化する。この復号化されたデータ両方に含まれるハッシュ値同じであれば A が送った情報だと確認でき、検証が完了する。

ちなみに公開鍵暗号で使われる、秘密鍵と公開鍵のペアの公開鍵データから変換して作られるのが、ビットコインアドレスというものだ。これはビットコインを受けとる際に必要になり、トランザクション内で受信者の宛先として使用される。

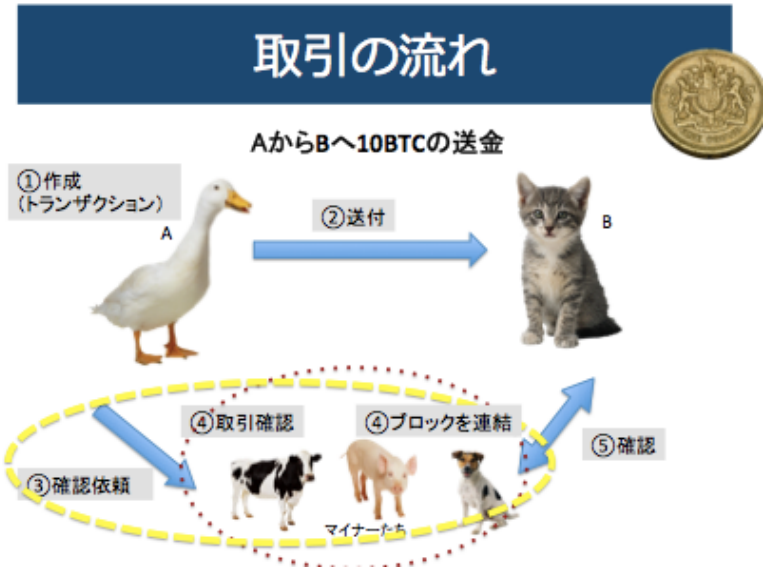
（図７）

特徴として、秘密鍵から公開鍵を、そのペアからビットコインアドレスを生成

することは出来るが、ビットコインアドレスから公開鍵を生成したり、公開鍵から秘密鍵を作成することは出来ないため、この検証は成立する。

3.4.確認依頼

次に A は取引が正常に行われているか、マイナー（維持管理ネットワーク）と呼ばれる取引の確認者たちに確認依頼をする。（黄色枠の遷移）



（図８）

マイナーが行う確認事項が以下の２点である。

①　トランザクションが二重支払いされていないかどうかの確認

②　検証が済んだ個々の取引情報を集めブロックにまとめる

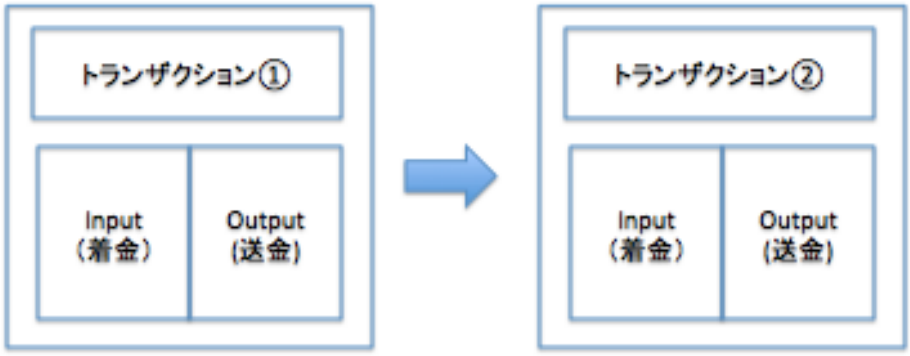
二重支払いとは、同じビットコインを別々の決済や送金に使用することである。同じ硬貨や紙幣（100 円や 1000 円）を別々の支払いに使用することはできないが、ビットコインは電子データであるため、そのデータをコピーして複数の人に送信することが可能だ。

この二重支払いが起きては仮想通貨が成り立たないため、ブロックチェーンで管理している UTXO（未使用 output）を確認して、実行されたトランザクションが二重支払いではないということを確認しなくてはならない。

マイナーは過去から現在まで、すべてのブロックチェーンと取引データをダウ

ンロードしており、ブロックチェーン上で UTXO を確認することができる。そのため、マイナーは自身が持つ全てのデータを参照して「二重支払いがないかどうか」の確認を単体で行う。
ここで UTXO とは何かを説明する。
トランザクションデータ構造にあったように、トランザクションには input と output の 2 つが記録されている。ビットコインの着金が input に記録され、送金が output に記録される。

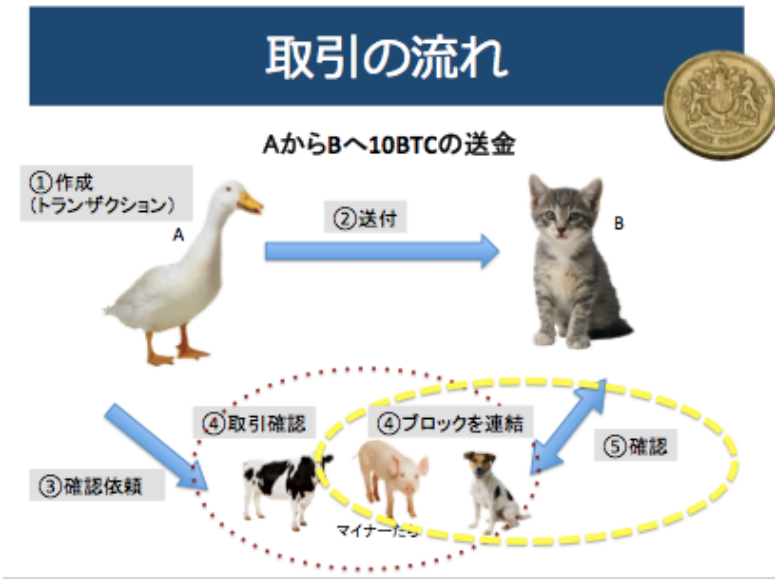
例えば、A が B のビットコインアドレスに 10BTC 送金し、トランザクション①が記録されるとする（以下の図をご覧いただきたい）。10BTC の input（入金）情報と共に output（送金）情報も記録される。その時の UTXO とは、B のまだ誰にも送金していないトランザクション①の output のことである。そしてこれは B のアドレスの残高も示している。



（図 9）
そして次に B は C のアドレスに 10BTC 送金するとしよう。
取引はトランザクション②の input と output に記録される。この時トランザクション①の output のみ、未使用から使用済みになるため、UTXO ではなくなる。そしてトランザクション②の output が UTXO（未使用残高）とされ、C のアドレスの残高を示すことになる。
つまり、「ビットコインを所有している」というのは、「自分で動かすことができる UTXO がブロックチェーン上に存在している」ということと同じである。言い換えると、UTXO はコインの存在証明なのだ。

よって、自分の保有するビットコイン残高を知る為に、いちいち過去の全取引を足したり、引いたりする必要はなく、ブロックチェーン上に残っている UTXO を足し合わせるだけで、残高を確認できるようになっている。

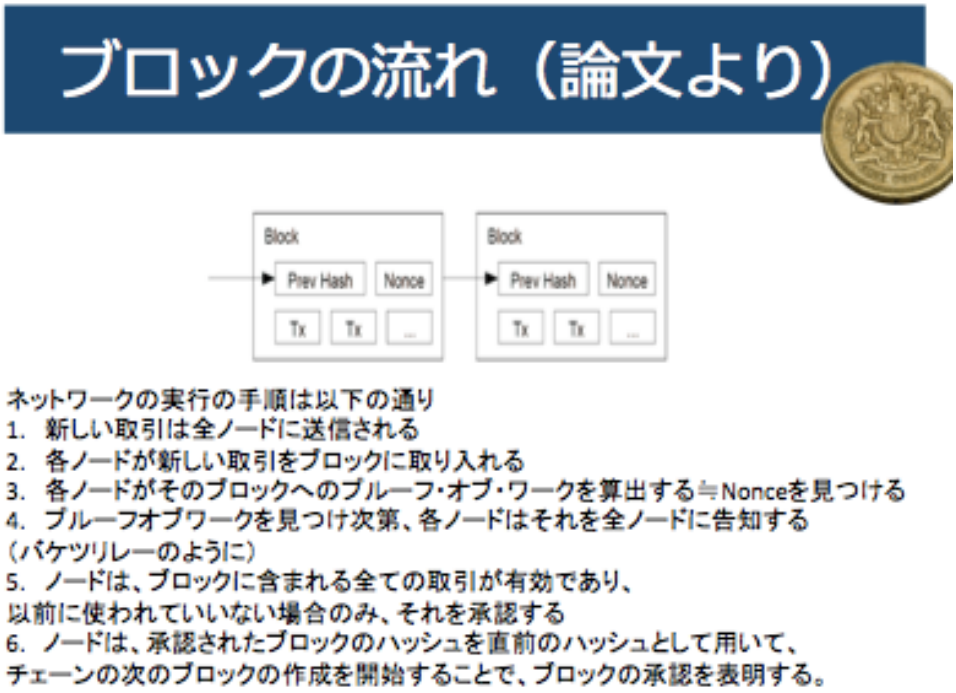
4.ブロックの連結



（図 10）

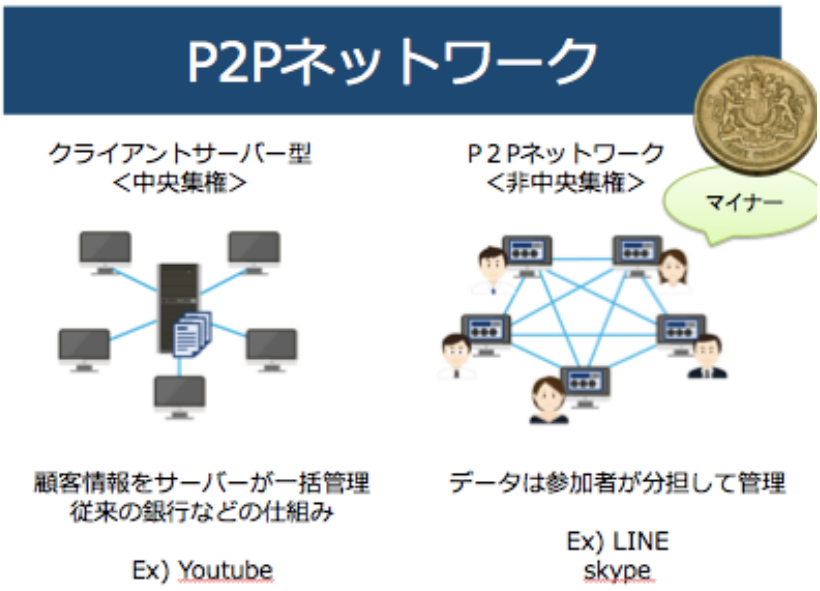
最後に、マイナーが集めた取引情報をまとめブロックにし、そのブロックを前のブロックに繋ぐ遷移ついて。

ブロック連結の手順をナカモトサトシの論文[4]では以下の通りに説明されている。



（図 11）

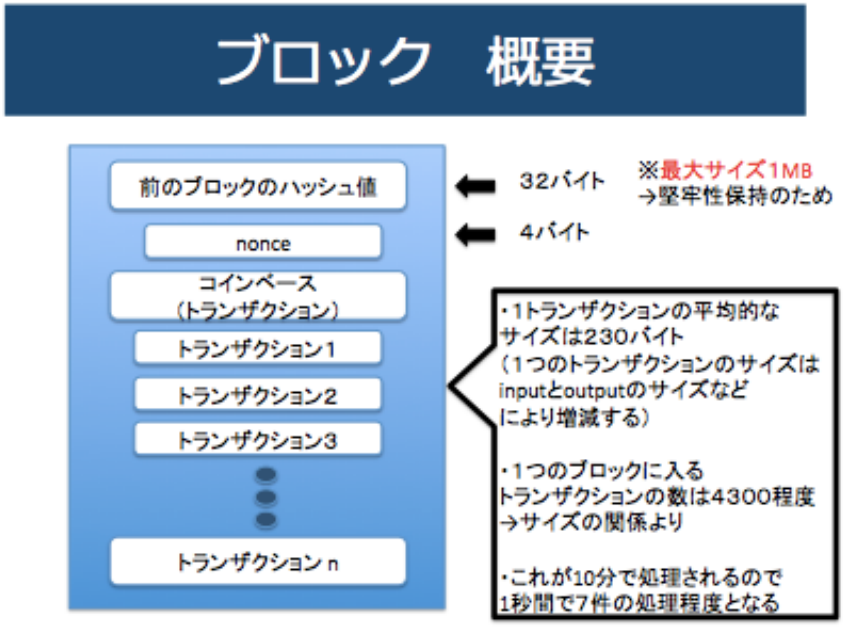
まず図 11 の 1. 2.を構築するシステムについて説明する。
ブロックチェーンでは「Peer to Peer ネットワーク」と呼ばれるシステムを採用している。Peer とは個人や企業の PC などの端末を指しており、サービス利用を行うクライアントと提供を行うサーバーの両方の役割を果たす。



（図 12）
従来使われているクライアントサーバー型とは異なり、それぞれの Peer が同じ内容のデータをバケツリレー式に繋いでいく特徴を持つので参加者全員が同じデータを保有している。また、サーバーに依存しないため、特定の Peer が切断してもサービスの提供は止まることはない。

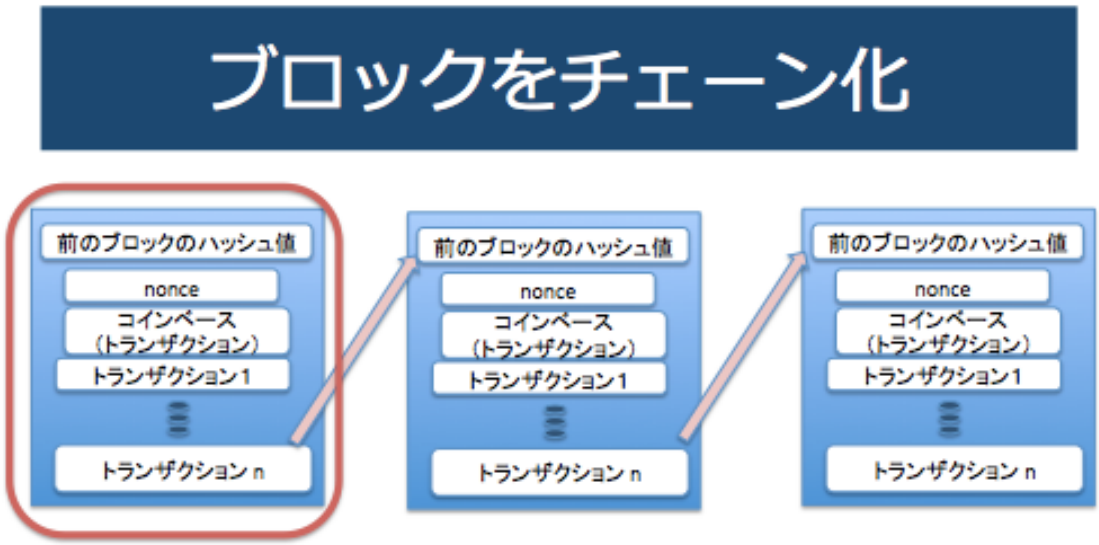
この「P2P ネットワーク」システムにより、ノード（≒マイナー）は全員が同じ取引情報、同じブロック履歴を保持している。そしてこのネットワークによって、次々と新しい情報は共有され更新されていく。

ではどのようなブロックが共有されているのか、ここでブロック構造について説明する。



（図 13）
ブロックは前の「ブロックのハッシュ値」・「Nonce」・「コインベース」・「トランザクション」によって生成されている。「Nonce」・「コインベース」については後ほど説明するとして、「トランザクション」は先ほど述べた通り、取引情報である。そして「ブロックのハッシュ値」とは、そのブロックの一つ前のブロックのデータをハッシュ計算して出たその値である。
前のブロックデータのハッシュ値をブロックに含むことによって前のブロック

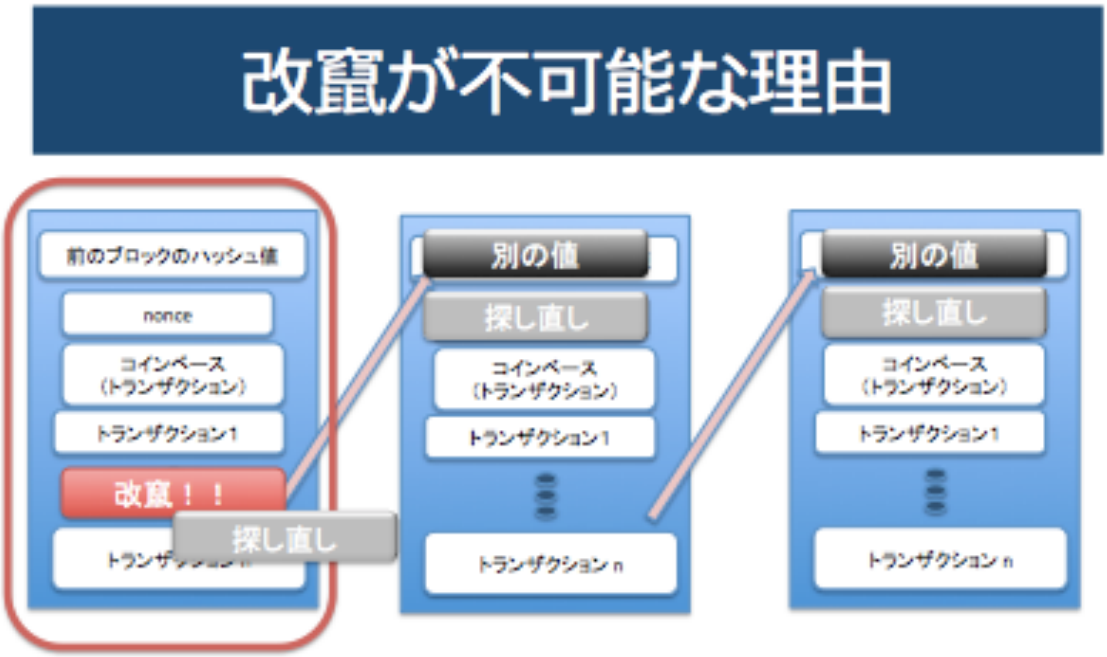
がどれであるか示している。



（図 14）

これにより、隣同士のブロックが関連をもちつつ１つの繋がったデータが作られていく。

また、どこかのブロックの内容を密かに変更しようとしても、そのブロック全体のハッシュ値が変わってしまうので、その次のブロックが持っている前ブロックのハッシュ値との間で不整合が起こり、変更したことが分かってしまう。



（図 15）

それを避けるためには、次のブロックも変更しなければならなくなり、結局変更したいブロック以降のブロック全てを変更しなければならなくなってしまう。これが過去のデータの書き換えを不能にしている仕組みのひとつだ。

では以降のブロックを含めてすべて書き換えれば変更できるのかというと、実はブロックを生成するには、とても時間がかかる計算処理をしなければならないという難題が課されており、それによっても書き換えが難しくなっている。この計算処理のことをプルーフ・オブ・ワークといい、ブロックを構造する１つのデータ「Nonce」をマイナーが見つける作業である。

4.1.マイナーの役割と Nonce について

ブロックチェーンではマイナーが大きな役割を果たしている。先に述べた２点の事項（①トランザクションが二重支払いされていないかどうかの検証②検証が済んだ個々の取引情報を集めブロックにまとめる）を確認するためにマイナーはマイニングと言われる大きく４つの仕事を行なっている。

① トランザクションが不正でないか確認
② 未承認（マイナーが二重支払いされていないかの検証を行っていない）のトランザクションを集約
③ 報酬トランザクションを加える
④ Nonce を加えハッシュを計算

報酬トランザクションというのは、ブロック構造３つ目の「コインベース」である。マイナーは組み立てるブロックに作業の成果報酬としてビットコインを受け取ることができ、コインベースをブロックに加えることによって報酬を得ている。（現在だと 12.5 ビットコインを受けとっている）

そしてその報酬は「③Nonce を加えハッシュを計算」した際、ハッシュ値が正しいブロックとしての条件を満たす Nonce を、一番早く発見したものに与えられる。

では Nonce（number used once）とは

マイニングで新たなブロック生成の際、使用される「一度きり使う数値」のことだ。ランダムな３２ビット（２進数の 32 乗パターンが存在）値で表す。

（図 16）

Nonce は一定の長さであること以外は特にルールのない任意の値で
この Nonce を変化させることにより、ハッシュ値を 0 が一定数連続する値にする。ハッシュの元のデータは復元できないため、ハッシュ値が連続する 0 から始まる値になるような Nonce を総当たり的に探すしかない。
正しいブロックとしての条件は、ハッシュ計算をしたときに出た値が、先頭に 0 が 16 個並ぶハッシュであることである。

ただ、そう簡単に Nonce を見つけられるわけではなく、計算処理には膨大な量の PC やそれを使うための電気が必要である。
そして報酬を得るためのマイナーによる Nonce 発見競争は、１つのブロックに対して約 10 分間行われる。これは、10 分で Nonce が見つかるよう調整されているからだ。ブロックチェーンの仕組み上、最後の 2016 ブロック（２週間毎）が生成されるのにかかった時間を測定し、実際にかかった時間と求められる時間との比が計算され適した調整が行われているのだ

この計算の難しさや 10 分という時間の短さから、トランザクションを改竄した場合、その後に続く全てのブロックの Nonce を探し直す大変さが伺える。１つの Nonce を見つけるだけでも多くの計算量が必要であるにも関わらず、計算し直している間に他のマイナーが新しいブロックを次々にチェーン化しているため、最新のブロックに追いつくには、他のマイナーたちの何倍もの計算速度で計算しなければならないのだ。

以上のことから、過去のデータを改竄することは非常に困難であると言われている。

この Nonce を見つけるマイニング作業によって、ブロックは改竄されることなく連結されトランザクションが正しくブロック内に保存される。

5.まとめ

- いくつかの個人間の取引情報を１つのブロックの中に集約して、そのブロックを鎖のように繋いでいくため、ブロックチェーンと呼ばれいる。
- ブロックチェーンはみんなが共有・確認できる「台帳」のようなものでありながらも、その仕組みから、データを改ざんしたり、そのシステムを壊す・止めるなどの行為は非常に難しいデータ蓄積システムである。

最後に。
今回の論文を通して、「ブロックチェーンとは何か？」
これを説明するのは非常に至難の業だと感じた。ブロックチェーンは非常に奥深く難しい。暗号やデータ構造、P2P システムや分散システムなど、それぞれの要素だけでも本１冊にはとても収まりきらない話が絡み合っている。
ただ、このレポートの作成や卒業研究発表会を通して、ブロックチェーンの理解を少しでも深められていたら、嬉しい限りである。

【参考文献】

[1]いちばんやさしいブロックチェーンの教本　杉井靖典

[2]ブロックチェーンがよ〜く分かる本　石黒尚久　河除光所瑠

[3]ブロックチェーン　相互不信が実現する新しいセキュリティ　岡嶋裕史

[4] Bitcoin: A Peer-to-Peer Electronic Cash System　Satoshi Nakamoto
https://bitcoin.org/bitcoin.pdf

[5]日本語で読むビットコイン原論文
http://www.kk-kernel.co.jp/qgis/HALTAK/FEBupload/nakamotosatoshi-paper.pdf

[6] Mastering Bitcoin　日本語 Ver
https://bitcoinbook.info/wp-content/translations/ja/book.pdf

[7]Bitcoin を技術的に理解する 富士ゼロックス株式会社
https://www.slideshare.net/kenjiurushima/20140602-bitcoin1-201406031222

[8] 日本ブロックチェーン協会(JBA)
https://jba-web.jp/archives/2011003blockchain_definition

[9]ビザンチン障害問題について　Wikipedia
https://ja.wikipedia.org/wiki/%E3%83%93%E3%82%B6%E3%83%B3%E3%83%81%E3%83%B3%E5%B0%86%E8%BB%8D%E5%95%8F%E9%A1%8C

[10]プロトコルについて　Wikipedia
https://ja.wikipedia.org/wiki/%E3%83%97%E3%83%AD%E3%83%88%E3%82%B3%E3%83%AB