フィンテックと分散システム
— ブロックチェーンとは結局何なのか —

斉藤 賢爾
ks91@sfc.wide.ad.jp

2016 年 1 月 6 日

概 要

「フィンテック (FinTech)」は金融 (finance) と (情報通信) テクノロジー (technology) を合わせた造語であり、過去から存在するが、インターネットが通信/放送・卸売/小売・運輸/郵便・宿泊/飲食・医療/福祉等の各分野にもたらしてきたものと同種のインパクトを金融業にもたらす新技術を表す言葉として、2015 年にバズワードとなった。

本稿では、2015 年末の時点におけるフィンテックの技術的側面の記録となることを意図して、特にブロックチェーン (blockchain) 技術に注目し、ビットコイン・ブロックチェーン (Bitcoin blockchain) の仕組みを振り返り、その応用と課題についてまとめる。また、その他のブロックチェーン技術を紹介し、その課題を述べるとともに、ブロックチェーン技術の本質的な特性と、社会における応用可能性に対する精緻な理解を試みる。さらに、その他の分散レッジャー (distributed ledger) 技術についても紹介した上で、フィンテックに関わる技術的・政策的話題をまとめる。

1 はじめに

1.1 フィンテックと 2015 年

「フィンテック (FinTech)」は金融 (finance) と (情報通信) テクノロジー (technology) を合わせた造語であり、用語としては過去から存在する。しかし、デジタル通貨「ビットコイン (Bitcoin)」[9] (https://bitcoin.org/) が国際送金に応用されるなど、金融におけるディスラプティブ (disruptive; 従来の秩序に対して破壊的) な技術が登場したことを受け、インターネットが通信/放送・卸売/小売・運輸/郵便・宿泊/飲食・医療/福祉等の各分野にもたらしてきたものと同種のインパクトを金融業にもたらす新技術を表す言葉として、2015 年にバズワードとなった。

ビットコインの要素技術であり分散レッジャー (distributed ledger; 分散元帳) を実現するとされる「ブロックチェーン (blockchain)」は特に注目を呼び、各金融機関におけるブロックチェーン技術の応用可能性の検討が本格化している。

本稿では、2015 年末の時点におけるフィンテックの技術的側面の記録となることを意図して、ビットコイン・ブロックチェーンの仕組みを振り返り、その応用と課題についてまとめる。また、その他のブロックチェーン技術を紹介し、その課題を述べるとともに、ブロックチェーン技術の本質的な特性と、社会における応用可能性に対する精緻な理解を試みる。さらに、その他の分散レッジャー技術についても紹介した上で、フィンテックに関わる技術的・政策的話題をまとめる。

1.2 貢献

本稿は、フィンテックの技術的側面をまとめたものであるが、そのことに加え、次のように貢献する。

1. 第 1 の貢献は、ブロックチェーンには一定の応用可能性があるが、「未知の構成要素から成り、不確実性が許容できるシステム」に向いており、金融の根幹を成すシステムへの適用には向かないということを明らかにしたことである。すなわち、
   (a) 金融機関がその勘定系システムにブロックチェーンを採用するとすれば、失敗すると予想できる。
   (b) 勘定系システムに新技術を採用するならば、むしろ、既知の構成要素を前提として従来から耐障害分散システム研究の文脈で培われてきた、言わばビザンチン・パクソス系の技術 [4][5] が向いている。
2. しかし、「従来の文脈においては要件を満たせないが、社会が新たな文脈においてそれを選んでいく」ということこそがディスラプティブな技術がそう呼ばれる所以である。ブロックチェーン技術そのものには課題があるとしても、金融や IoT 等の分野に応用が可能な、新たな文脈における新たな技術の可能性を示したことが、本稿の第 2 の貢献である。

なお、本稿での整理・議論に至る筆者による萌芽的な貢献に関しては、次を参照されたい。

- ビットコインやブロックチェーンの技術や課題の解説: [13] [15] [16]
- 関連技術による社会変容の可能性の検討: [11] [12] [14] [17]

1.3 用語

本稿では以下の用語を改めて定義して用いる。

取引: システムの状態を遷移させる事象。

トランザクション (TX): 取引のうち、確定後は後戻りできないもの。

コンセンサス: システムを構成する (正常な) 参加者による合意。

ビザンチン障害 (含 利己的な振る舞い): 参加者が利己的に振る舞うことでプロトコルを逸脱することを含めた、正常でない任意の現象。該当する参加者の数を f で表す。

2 ビットコイン・ブロックチェーン

2.1 ビットコインというシステム

サトシ・ナカモトを名乗る匿名の開発者が 2008 年に発表した論文 [9] を読み解くことを通して見えてくるのは、ビットコインの技術には「資産のユーザによる直接管理」と「取引の公知化」の 2 本の柱があるということである。前者はデジタル署名で実現される。ブロックチェーンは後者を担う技術である (しかるに、2015 年現在の金融業界におけるブロックチェーンをめぐる喧噪では、この両者が区別されていないように見える。銀行等の従前

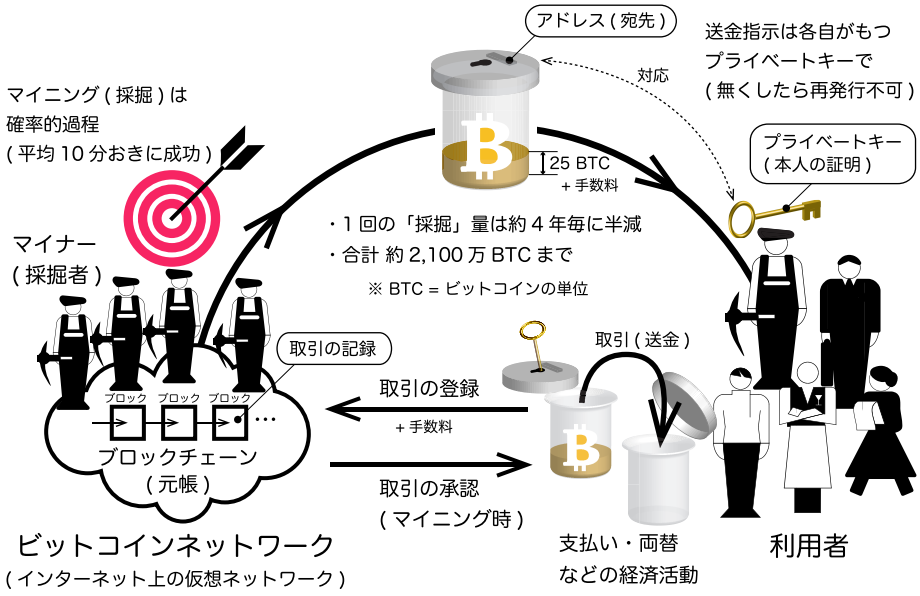

図 1: ビットコインというシステムの概要

の金融業が本質的に欲しているのは、前者であり、後者に関しては公知化でなく関係組織間での共有ができることを潜在的には望んでいる可能性が高いと筆者は考えている)。

図 1に、ビットコインのシステムの全体像の概要を示した。ブロックチェーンはグローバルに単一なデータ構造であり、すべての取引記録を格納し、参加者全員でこれを維持する。

ブロックチェーンは、その名が示す通りブロックのチェーン (連鎖) である。ブロックは「取引」の集合である。取引は、参加者間におけるビットコインの「量」(単位：BTC) の受け渡しを記述する。

図 2に、ビットコインにおけるブロックチェーンの概要を示した。各ブロックには、その手前のブロックのデータ全体を代表する値である「ダイジェスト (digest)」(暗号学的ハッシュ関数により得られるが、ここでは SHA-256 アルゴリズムを二重に適用する) が格納される。そのことによりブロックの順序関係を表現すると同時に、データの改ざんを困難にしている。

取引は任意の参加者により作成され、構造を持たない仮想ネットワークであるビットコインネットワークにブロードキャストされる。それらの取引を収集し、ブロックを作成するのは「マイナー (miner)」と呼ばれる種類の参加者である。このとき、作成するブロックのダイジェストが、システム全体の計算パワーに合わせて調整されている「ターゲット (target)」以下になるように、ブロック内に格納される「ノンス (nonce; その場かぎり)」の値を決めなければならない。どのようにデータを構成すればどのようなダイジェストが得られるかは予め分からないため、このことはノンスの値を総当たりで試す以外の方法では為し得ない。この作業を「マイニング (mining)」と呼ぶ。マイニングは、ターゲットが小さくなるにつれ、確率的に非常に困難な作業となる。

ブロックを作成できたマイナーは、そのデータをネットワークにブロードキャストする。ブロックを受け取ったその他のマイナーたちは、ブロックの内容を検証し、正しければ、それに繋ぐブロックを作成すべくマイニングを続行することになる。

各マイナーは自律的に動作しているため、複数のマイナーたちが、ほぼ同時に異なる内容のブロックをブロードキャストすることも起きうる。その場合、ネットワーク上のポジションによってブロックを受信する順序は前

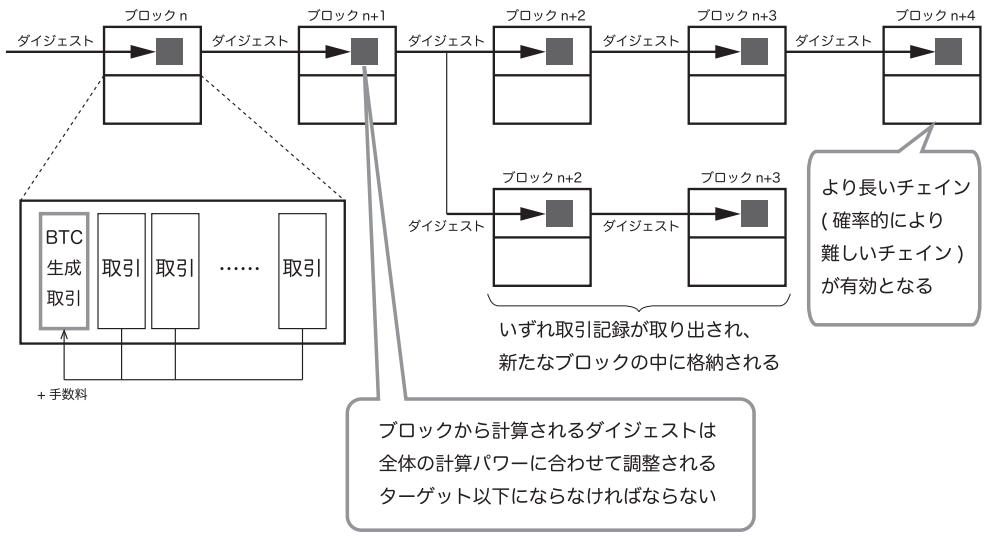

図 2: ビットコイン・ブロックチェーンの概要

後し、異なるブロックを正当と見なすマイナーたちが各々異なるチェーンを伸張させていくことになる。ブロックの列は最終的には一意に決まらなければならないため、ビットコインでは、確率的に最も困難なチェーン (大まかには、最も長いチェーン) が有効であるとするルールを定めている。

無効となったチェーンからは、有効なチェーンに含まれていない取引が取り出され、改めて新たなブロックに格納され、ブロックチェーンに追記されていくことになる。このとき、有効なチェーンと矛盾する取引は捨てられる。このため、希だとは考えられるが、一度ブロックチェーンに格納された取引が、後に無効となる場合がありうることになる。このことに対応すべく、ビットコインのクライアントソフトウェアでは、ブロックチェーンの現在の末尾から遡ること 6 ブロック未満の取引については未確定と扱う慣習になっており、また、ビットコインのプロトコルでは、マイニングの報酬としてマイナーが自身に向けて無から BTC を送る「生成取引」については 100 ブロックがその後に追加されるまで無効としている。

2.2 ビットコインにおける取引

図 3は、ビットコインにおける取引の構造を示している。取引は任意数の入力と任意数の出力から成る組として表現される。入力は、過去の取引の出力への参照であり、入金を表す。出力は出金を表す。図では、出力を液体の容器のような形状で描いているが、ビットコインの取引における出力は、まさに貨幣の量を入れる容器だと見なせる。出力では、貨幣の量の他に、その宛先を (典型的には) 参加者の公開鍵のダイジェストのかたちで与える (ここでのダイジェストは、SHA-256 の次に RIPEMD-160 を適用した 160 ビットの値である)。入力では、参照する出力を取引のダイジェスト (二重 SHA-256 値) と出力の番号で特定し、取引のデータへのデジタル署名を付与する。この署名は、参照する出力の宛先におけるダイジェストとなるような公開鍵で検証できることが求められる。

未参照の出力 (=未使用のコイン) は、ビットコインの用語では UTXO (Unspent TX Output) と呼ばれ、この用語でこのデータ構造を代表させる用法も見られる。

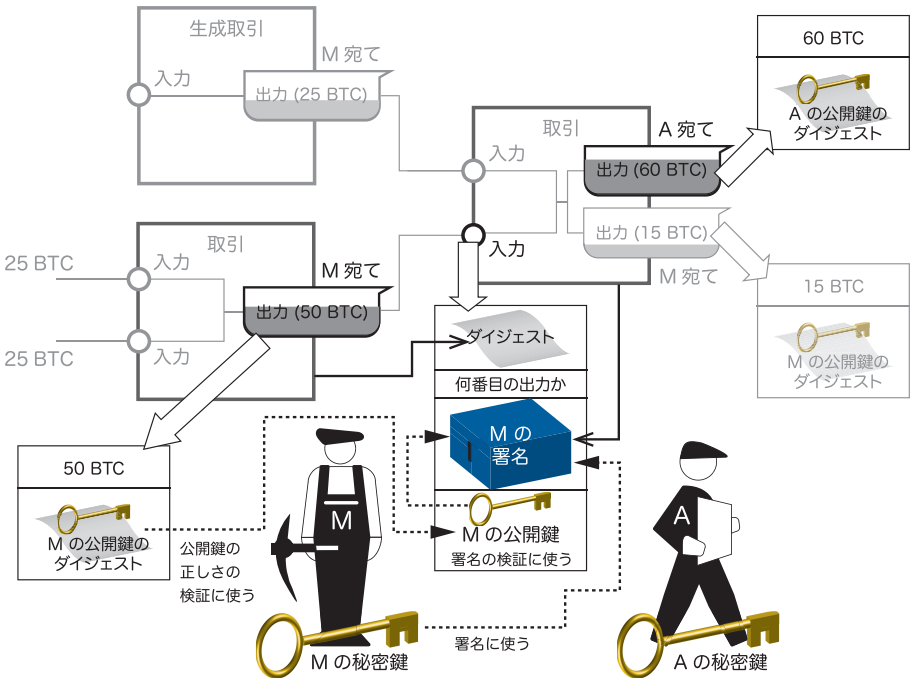

図 3: 取引におけるデジタル署名とその検証

出力における宛先となる公開鍵のダイジェストや、入力でのデジタル署名や公開鍵は、実際にはスクリプトを通して指定される。これにより、送金の宛先やその受領者であることの証明の手段に様々な条件を設定できる。

2.3 公知化と作業証明

サトシ・ナカモトによる論文 [9] からは、ブロックチェーンがパブリッシングのプラットフォーム (取引の公知化の手段) を意図して設計されていることが伺える。論文には「タイムスタンプサーバは、項目を連ねたブロックのハッシュ値を新聞や電子ニュースへの投稿のように広くパブリッシュする働きをする」「分散タイムスタンプサーバをピア・ツー・ピアで実現するためには、新聞や電子ニュースへの投稿の代わりに、アダム・バックによるハッシュキャッシュのような作業証明 (proof of work) システムを用いる必要がある」(筆者訳、下線筆者) とある。ブロックチェーンは、公知化の手段としての「新聞」あるいは「電子ニュースへの投稿」と同等なものを P2P で実現する試みだと考えられる。

ここで、作業証明とは計算コストを投入したことの証明であり、一般に、作業は困難だが、その結果の検証は容易となるような問題を解くことを示す。例えば「あるターゲット以下になるようなダイジェストとなるデータを見つけよ」といった問題である。

作業証明によるコストが課せられていることで、取引の改ざんは困難となる。仮に、誰かが取引記録の改ざんを試みたとする。取引にはデジタル署名が施されているので、取引の記録自体を変更することは非常に困難だが、記録をデジタル署名ごとブロックから削除することは考えやすい。しかし、実際に取引をブロックから削除すると、ブロック全体のデータを代表する値であるダイジェストが変化してしまう。その値は典型的にはターゲットより大きいため、マイニングをやり直す必要がある。首尾よくマイニングに成功しても、そのブロックのダイジェス

トを格納する次のブロックの内容も変えなければならないので、さらにマイニングをしなければならず、次々とマイニングをし直して、進行中の正規のマイニングを追い越していくだけの莫大な計算力が必要となってしまう。

ビットコインにおけるコンセンサスは、作業証明により偽造が困難なデータ構造をネットワーク上にパブリッシュし、その正しさを参加する誰もが検証可能にすることにより得られる。そのことを通して、資金の移動の履歴を一意に保つことに (脆弱性やスケーラビリティの課題を考慮しなければ、ひとまず) 成功している。

3　ビットコイン・ブロックチェーンの応用と課題

3.1　ビットコイン・ブロックチェーンの応用

ビットコインは、それ自体が通貨であること以上に、プラットフォームとしての応用価値が認められ始めている。

ひとつの大きな動きは、ビットコイン・ブロックチェーンをそのまま活用しようというものである。例えば 2015 年、リクルートホールディングスは、ブロックチェーンを利用した国際送金サービス「アラインコマース (Align Commerce) (https://aligncommerce.com) の運営会社に出資したが、このサービスでは背後でビットコインを用いている。送金元の通貨をいったん BTC に交換し、BTC を送金した後、送金先で現地の通貨に交換するわけである。

同様のサービスでは、「アブラ (Abra)」(https://www.goabra.com) というスタートアップも注目されている。これは、本質的には、法貨と BTC を両替する交換所の役割を、一般の個人や商店が果たすというものである。そのような交換所は「テラー (teller)」と呼ばれ、アブラのサービスに登録して、居場所を公開する。ユーザは、近所のテラーを見つけて現金をアブラのシステムに入金すると、その後の送金はどこに向けても無料で行える (背後ではビットコインを用いているが、その存在は隠されている)。送金を受けた側は、現金化が必要であれば、自分の近所のテラーを見つけて行う。テラーは手数料を取れるが、その一部がアブラの収入となる。

背後でビットコインを用いていることで、アブラでの送金は BTC の価格変動の影響を受けることになるが、アブラでは 3 日間の価格固定を行い、その間の変動リスクを運営会社が吸収するという方式を採っている。

テラーを「人間 ATM」と称する人もいるが、ATM は元々「自動テラーマシン (Automated Teller Machine)」という意味である。アブラにおけるテラーは自動でもマシンでもなく、単に「テラー」と呼ばれることが相応しい。ウーバー (Uber) によって、誰もが人を運ぶ運転手になれる道が開けたように、アブラによって、誰もがテラー (銀行窓口) になれる時代が到来するというわけである。

アブラは送金業だが、ユーザから一切お金を預からない。ウーバーやエアビーアンドビー (Airbnb) が、自身は自動車や不動産といった資産を持たずに、低コストでかつ価値の高いサービスを提供することで旧来のタクシー業やホテル業を圧迫し、軋轢を生んでいるように、アブラのようなサービスによる既存の金融業へのインパクトが無視できなくなってきた。ビットコインの存在は、他の業種へインターネットがもたらしたものと同じ性質のインパクトを金融業の世界にもたらしつつある。そのことへの危機感が、2015 年に急激に加熱した、金融機関におけるブロックチェーンおよびその他の分散レッジャー技術に関する知識への渇望の要因であると考えられる。

3.2　ビットコイン・ブロックチェーンの課題

筆者は、ビットコイン・ブロックチェーンに関して、プライベートキーの紛失・漏洩への対策の欠如や、マイナーのネットワークが継続的に分断 (エクリプス攻撃) されたときにブロックチェーンの正当性が失われる、といった課題を指摘している [13]。後者はビットコインの規模を考えると難しいようにも見えるが、可能なことはいずれ現実になると考えた方がよい。

また、技術のガバナンスにおいても、グローバルなブロックチェーンは「ワンネス (oneness)」を強要するため、「部分的にそのときの標準とは違うことを試して技術を変化させていく」といったことができず、しなやかさに欠けるという大きな問題がある [13]。

さらに、技術的な問題やガバナンス以外にも、ビットコイン・ブロックチェーンを今後も基盤として使っていくことには大きな懸念がある。

ビットコインでは、1 回のマイニングで得られる報酬は 21 万ブロック毎に半減することになっている。2009 年 1 月にシステムが動き出した当初は 50BTC だった報酬は、2012 年 11 月に 25BTC になった。現在は、平均して約 8 分毎にひとつのブロックが生成されており、このペースで進むと 2016 年 6 月に累計で 42 万ブロックに達し、以降、次の約 4 年間、報酬は 12.5BTC になる。

これまでにマイニングの競争が激化してきた結果、現在は、投入する電力のコストとマイニングによる報酬が釣り合う状況になっているが、報酬が半減するなら (BTC の価格が 2 倍になれば別だが)、多くのマイナーたちは経営が立ち行かなくなり、撤退せざるを得なくなる。マイナーが撤退すると競争が緩くなり、攻撃のための敷居が相対的に低くなる。それは、電力投入のコストにより守られているビットコインのセキュリティが低くなることを意味するのである。

4　その他のブロックチェーン技術

4.1　サイドチェーン

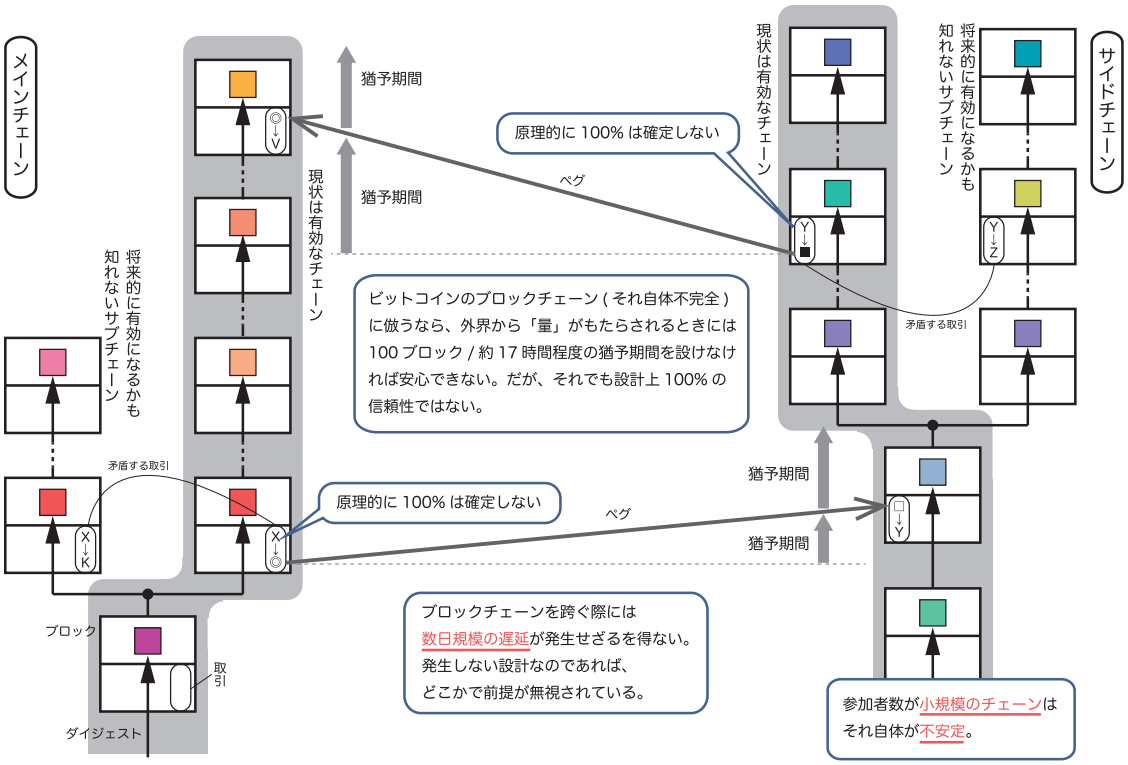

図 4: サイドチェーンとその問題点

これまでに、ビットコイン以外のデジタル通貨基盤や作業証明以外のコンセンサス形成の手法は様々に提案されてきたが、そのポピュラリティ (およびその帰結としての規模の大きさ) と、作業証明というアイデアの強固さから、未だにビットコインを超える基盤は生まれていないと考える向きもある。

そうした中で、ビットコイン・ブロックチェーンを言わば「アンカー」として利用しながら、ポリシーの異なる独自のチェーンを運用するという、「サイドチェーン (sidechain)」ないし「ペグドサイドチェーン (pegged sidechain)」としうアイデアが登場した [2]。その仕組みと問題点を示したのが図 4である。

サイドチェーンは、典型的にはビットコイン・ブロックチェーンをメインのチェーンとして用いる。その BTC における量を、独立したチェーンであるサブチェーンに移転させるべく、再びメインチェーンに戻る必要が無ければ、誰も満たせない条件を出力のスクリプトに記述することにより BTC を消失 (あるいは焼失; burn) させ、もしくは再びメインチェーンに戻る必要があるならば、サブチェーンによってしか満たせない条件をスクリプトに記述することにより BTC を凍結させる (このような凍結を可能にするためには、ビットコイン・プロトコルに修正が必要である)。

このことにより、原理的には、ビットコインの信頼性 (それがそもそも心許ないが) に依拠しつつ、ポリシーの異なるチェーンを実験できることになる。

ただし、量がチェーンを跨ぐ際には、ブロックチェーンから量が消滅したり生成されたりするのであるから、ビットコイン・プロトコルに則るならば、100 ブロック、あるいは 17 時間程度の猶予期間を設けなければ安心して利用できないことになる。メインチェーンとサブチェーンの双方でそうした猶予期間を設けるならば、17 時間 ×2 となり、チェーン間で量を移転させるために 1~2 日を要することになる。もし、サイドチェーンでメインチェーンよりも高速なマイニングを謳うとするならば、ナンセンスということにも成りかねない。

また、サイドチェーンは一般にメインチェーンよりも規模が小さく、競争条件が緩いことからセキュリティ上の懸念があることも、量の移転の際に慎重になる必要がある理由となる。

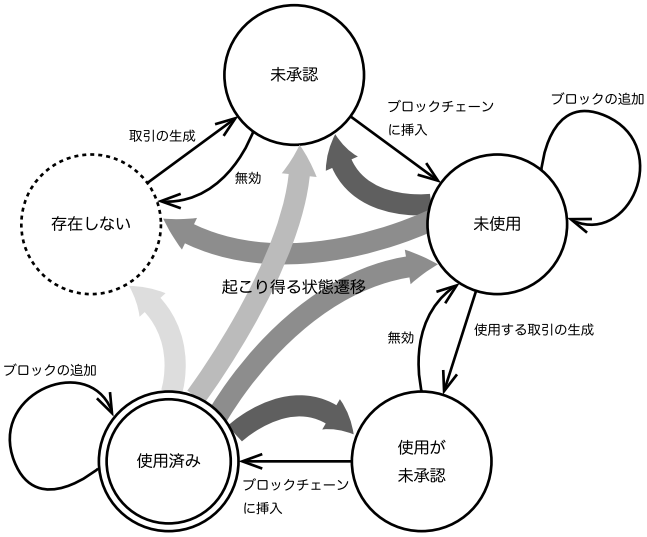

図 5: ブロックチェーンにおけるトークンの状態遷移

図 5は、ビットコインにおけるコイン (=取引の出力) 等、ブロックチェーンで扱われるトークンの状態遷移を示したものである。希ではあるが、どの遷移も後戻りの可能性をもち、特にサイドチェーン技術では、後戻りがチェーンを跨ぐ危険性があるため、設計も複雑にならざるを得ない。

仮に、確固としたセキュリティをもち、かつ各取引をファイナルにし、後戻りさせない技術を以てサイドチェーンを運用できるとし、それによりチェーン間の量の移転を高速かつシンプルにできるとする主張があったとする。その主張はナンセンスと言わざるを得ない。もしそのような技術があったとすれば、それは単独で用いることができ、サイドチェーンの形式を採る必要はないからである。

本稿では、ブロックチェーンを金融の根幹を成すシステムに適用することについて疑いの目を向けるが、サイドチェーン技術に至っては、金融の根幹を成すシステムへの適用はまったく無意味と言って過言ではない。

4.2 カラードコイン

取引は、一般化すると状態の変化の記述であると考えることができる。しかし、ビットコインでは BTC の移転しか記述できない。そこで、あたかも取引の一部の出力に色 (カラー) を付けるかのようにして他から区別し、BTC の量にビットコイン以外の通貨や資産などを紐づけることを可能にしたのが、「カラードコイン (colored coins)」[1] と呼ばれるアイデアである。カラードコインでは、ビットコイン・ブロックチェーンに他の通貨を含む独自のデジタル資産の移転の情報を埋め込むことにより、ビットコインネットワークの規模と信用を流用しつつ、新たな資金・資産の移転のための仕組みを実現できるとされる。

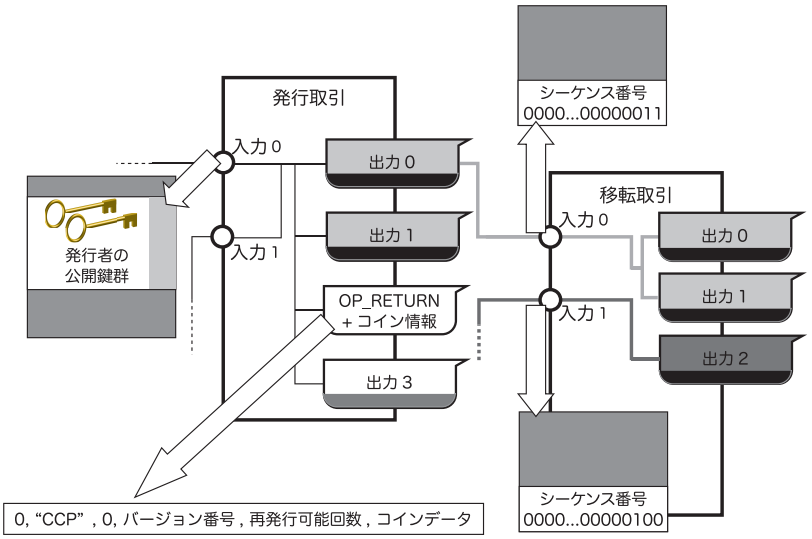

図 6: カラードコインの仕組み

図 6は、統一されつつあるカラードコインの (2015 年 1 月時点での) 仕組みを示したものである。「色つきの」量の流れをブロックチェーンに載せたい場合、参加者はまずそのカラーのための「創世取引 (genesis transaction)」を作成する。創世取引の出力では、スクリプトの先頭に演算子「OP_RETURN (スクリプトの実行を即終了/その出力の参照を許さない)」を置き、後に続く領域にそのカラーの情報を載せる。「OP_RETURN」を先頭に持つ出力に至るまでの (複数の) 出力 (図では 0 番と 1 番) が、そのカラーの出力と見なされる。

同じカラーのついた量を後に再度発行する場合は、創世取引の最初の入力 (0 番) が参照する出力と同じ宛先の出力を入力として参照する必要がある。セキュリティ上、この宛先は単一の公開鍵に対応するアドレスではなく、マルチシグ (multi-sig; 複数の公開鍵に対応するデジタル署名を必要とする方式で、3 個のうち 2 個など m 個中 n 個の数の署名が揃わなければ使用の条件を満たせない) を用いることが奨励される。

創世取引により生み出された色つきの出力は、「移転取引 (transfer transaction)」により参照され使用される。移転取引では、取引の入力データのうち、普段は用いることの少ない「シーケンス番号」を、最大 32 個 (実用上は 31 個) の出力に対応するビットフィールドとして利用する。これにより、特定のカラーを表す入力を特定の出力の集合と結びつけ、複数のカラーを扱う場合でも色が混じらないように取引を構成することが可能になる。例えば、図では入力 0 のシーケンス番号の末尾を 011 とすることにより、3 つある出力 (上から 0 番、1 番、2 番) のうちシーケンス番号の 2^i ビットが 1 であるような i、すなわち 0 番と 1 番に色つきの量が移転することを表現している。

こうした手法により、カラードコインでは、ビットコイン・ブロックチェーンの上で新たに意味づけられた量を取り扱える。しかし、これはハック (場当たりな解法) であり、BTC の価格の変動や、ビットコインの規制を巡る状況などの影響を受けるため、根本的な解法ではない。

4.3 イーサリアム

信用のための十分な数の参加者を得るのは課題ではあるが、ビットコインの弱点を克服したり機能を拡張させた、独自のブロックチェーンを作ることは今後の選択肢のひとつである。

マイクロソフト社が「イーサリアム・ブロックチェーン・アズ・ア・サービス (Ethereum Blockchain as a Service)」を発表したことでも広く知られるようになった「イーサリアム (Ethereum)」[3] (https://www.ethereum.org) は、ブロックチェーンを新たに作り、そこにチューリング完全な言語を装備する試みである。これはカラードコインと同様に、多様なデジタル資産の移転のためのルールを記述する「スマートコントラクト (smart contract)」のための基盤となるべく、最初から設計されている。

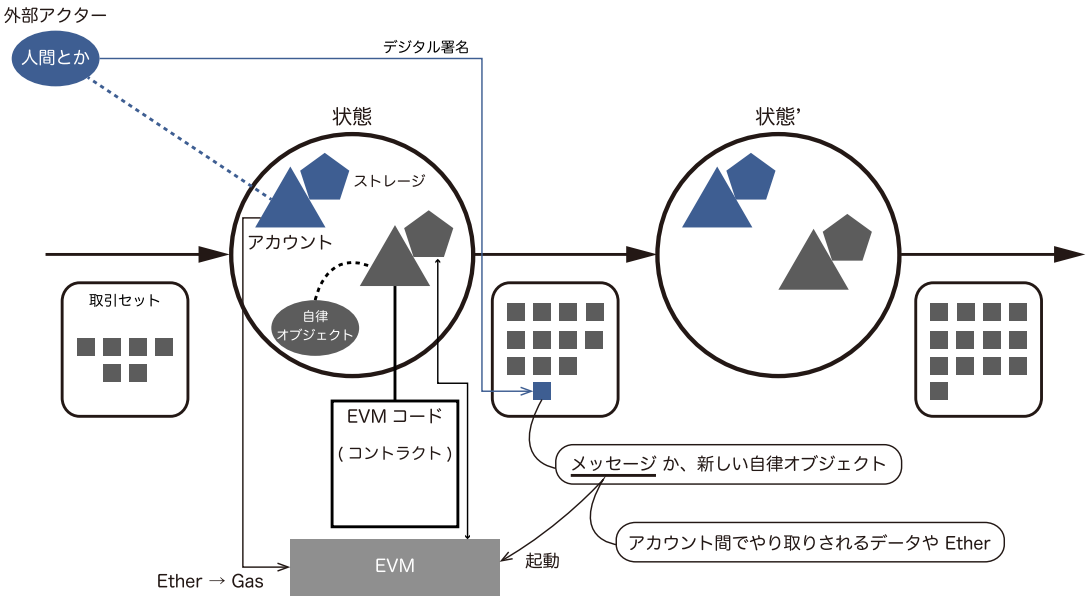

図 7: イーサリアムと EVM

図 7は、イーサリアムの動作の概要を示したものである。詳細な解説や議論は別の機会に譲りたいが、イーサリアムではブロックチェーンを状態マシンの run (実行履歴) として捉える。状態は各ノードにより維持される。ブ

ロックは状態を遷移させるためのコマンドである取引の集合である。人間などの外部アクターや、システム内の自律オブジェクトはアカウントを持ち、アカウントはシステム内通貨である Ether の残高やストレージや EVM (Ethereum Virtual Machine) コードを持てる。マイナーに当たるノードは EVM を持ち、手数料とも解釈できる Ether の供給を受けて、指定されたコードを実行する。

このように、取引が一般の状態遷移を記述可能だとすれば、究極的には分散コンセンサスを実現する基盤は「分散コンピュータ」を抽象化するものだと見なすこともできる。したがって、コンピュータが社会において果たしてきた役割のすべてを担える可能性を秘めているが、そもそも論として、そうした広い応用のためにブロックチェーンを用いることには、実行の意味論 (状態を遷移させるコマンドが後に無効となる可能性がある)、脆弱性、スケーラビリティ、および技術のガバナンスの面で懸念がある (5節にて詳細に議論する)。

4.4 NEM とミジン

「NEM (New Economy Movement)」(http://nem.io/) は、ビットコインやイーサリアムと同様に、オープンソースコミュニティにより開発が進められているブロックチェーン環境である。ビットコインと比較して多くの改善が試みられているが、実行の意味論、脆弱性、スケーラビリティ、および技術のガバナンス等の面で同じ問題を抱えると見られる。

「ミジン (mijin)」(http://mijin.io/ja/) は、テックビューロ株式会社が提供し、NEM に基づき NEM の開発チームにより開発されているプライベートなブロックチェーン環境である。プライベートなブロックチェーンは応用毎に作られるため、スケーラビリティと技術のガバナンスの面では一定の改善になると考えることができる。ただし、プライベートなブロックチェーンが実行される環境の条件下では、同じことを実現するために、より安価で高速な技術が適用可能だとも考えられる。

4.5 オーブ 1

「オーブ (Orb) 1」(https://imagine-orb.com/jp/) は、株式会社 Orb が提供する Orb SmartCoin の背後で動作するブロックチェーン環境である。オーブ 1 のブロックチェーンは応用毎に作られ、実行主体が存在することを利用してブロックチェーンの実行の意味論を変更し、確定的な動作 (すなわち取引をトランザクションとしてファイナライズできる) とエクリプス攻撃への耐性を備えている。ただし、ブロックチェーンが抱える諸課題に対する長期的な解とは考えられておらず、あくまで従来のブロックチェーン技術に対するハックという位置づけになる。

筆者は Orb 社のチーフサイエンティストとしてオーブ 1 の設計と実装に携わった。

5 ブロックチェーン技術とは結局何なのか

5.1 分散システムの指向パターン

ブロックチェーン技術とは結局何なのかを考えるにあたり、まず、2000 年に Brewer により予想され、後に Gilbert らにより定式化・証明された「CAP 定理 (CAP theorem)」[6] を振り返っておきたい。

図 8に示したこの定理では、分散システムにおいて、表 1に示した 3 つの性質を同時には満たせないことが示されている。ただし、この内任意の 2 つの組み合わせは満たすことが可能なため、具体的な分散システムは、C-P (一貫性-分断耐性), A-P (可用性-分断耐性) ないし C-A (一貫性-可用性) を指向することになる。

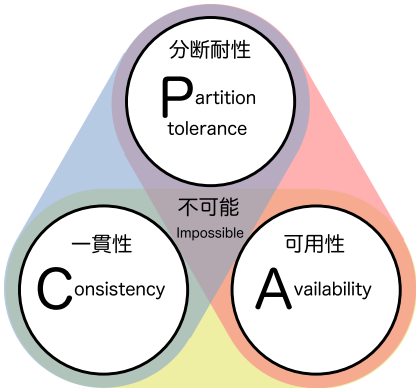

図 8: CAP 定理

表 1: CAP 定理上の 3 性質

性質	意味
Consistency (一貫性)	読み出しは直前の書き込みの内容を返す
Availability (可用性)	必ず有限時間内に応答する
Partition tolerance (分断耐性)	ネットワークが分断されても動作する

また、P2P の実用が進んだことで、分散システムの指向性を議論する上では、表 2に示した「ガバナンス指標」も重要となってきている。この指標は、ブロックチェーンの文脈では「Permissioned」「Permissionless」の区別として表現されることが多い。

5.2 分散レッジャー技術史

分散レッジャーは、中央による制御を持たないかたちで記録を保持していくものである。分散レッジャーを設計する上では、CAP 定理の 3 性質はいずれも重要であるが、地理的に分散した環境下で動作するためには、ネットワークを分断する障害の発生を前提と考えれば P (分断耐性) は必須となる。あとは、C (一貫性) をより重要な性質として採用すれば、A (可用性) は一時的に失われてもいずれ回復されるという設計になるし、A (可用性) をより重要な性質として採用すれば、C (一貫性) は一時的に失われてもいずれ回復されるという設計になる。

従来のデータベース研究における分散トランザクションの研究系列では、参加ノードのメンバシップが管理されている (permissioned) 前提のもとで、C-P (一貫性-分断耐性) が指向されていると考えられる。一方、ビットコイン・ブロックチェーンをはじめとするいわゆる permissionless なブロックチェーンでは、A-P (可用性-分断耐性) が指向されていると考えられる。この考え方に基づき、分散レッジャーの技術史を年表にまとめたのが図 9である。

5.3 確率的状態マシンとしてのブロックチェーン

確定的状態マシン

表 2: 分散システムのガバナンス指標

種別	特徴
Permissioned (許可要)	実名・制御・許可制
Permissionless (許可不要)	匿名・自由・無許可

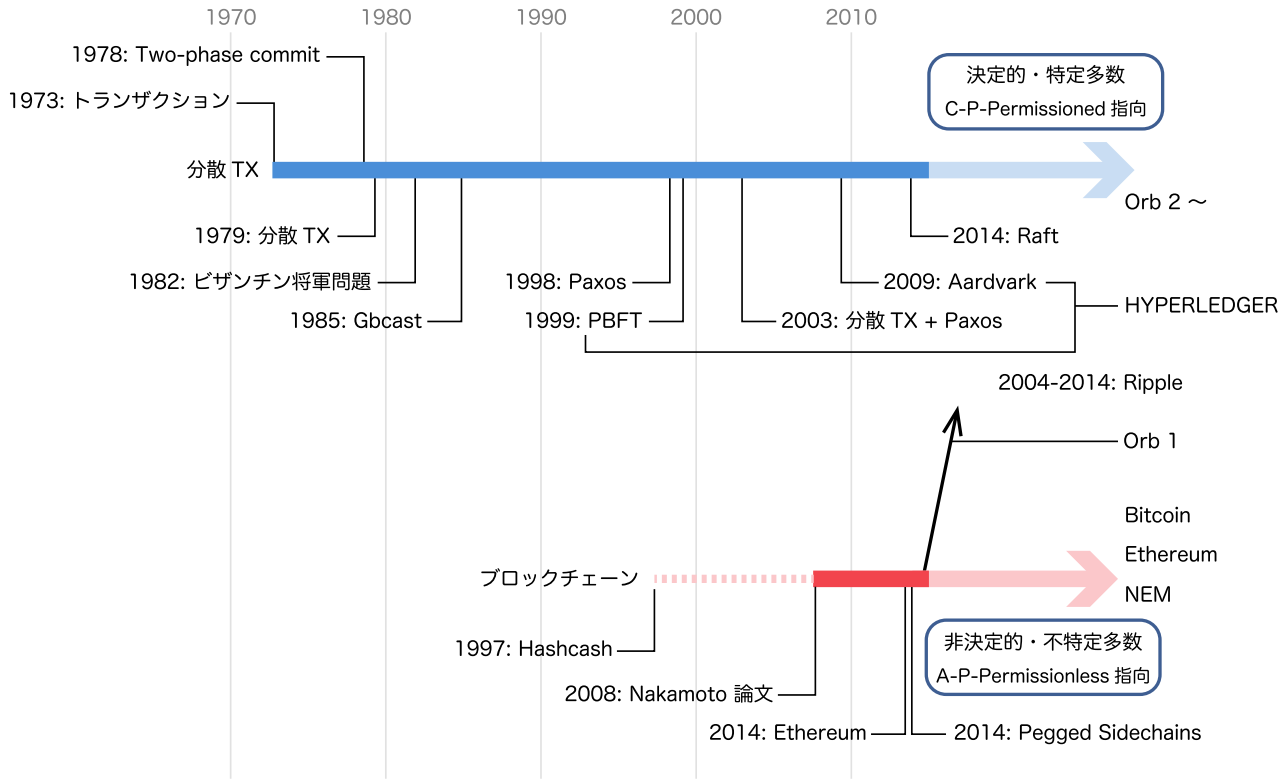

図 9: 分散レッジャー技術の歴史

分散トランザクションが実現するのは、トランザクションを状態を遷移させるコマンドと見なせば、「確定的な状態遷移を行う状態マシン (Deterministic State Machine)」(図 10) である。この状態マシンでは、状態の遷移が後戻りしない。分散化にあたっては、この状態マシンを複製することにより応答性や耐障害性を向上させることになる。

この確定的状態マシンの実現は、送金等の資産の移転が各々ファイナル (取り消せない) だと考えれば、金融機関の勘定系システムにおいては必須要件だと考えられる。

確率的状態マシン

一方、ブロックチェーンが実現するのは、常に分岐しながら進行していくチェーンの伸張に対し、その時点において最もスコアの高いチェーンを採用しながら、個々の参加者の視点からは状態を修正しながら進行していく「確率的な状態遷移を行う状態マシン (Probabilistic State Machine)」(図 11) である。全体としては、収束した取引の履歴を採用していくことになるが、その収束も、原理的にはチェーン全体が停止しない限り確定しない。

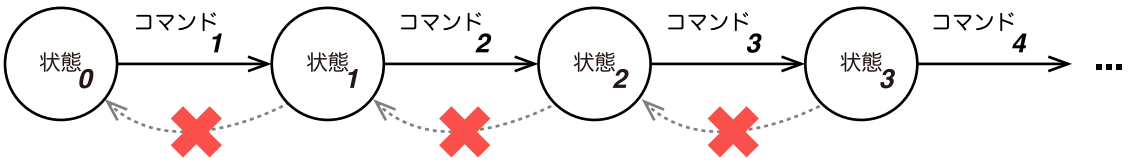

図 10: 分散トランザクションの確定的状態マシン

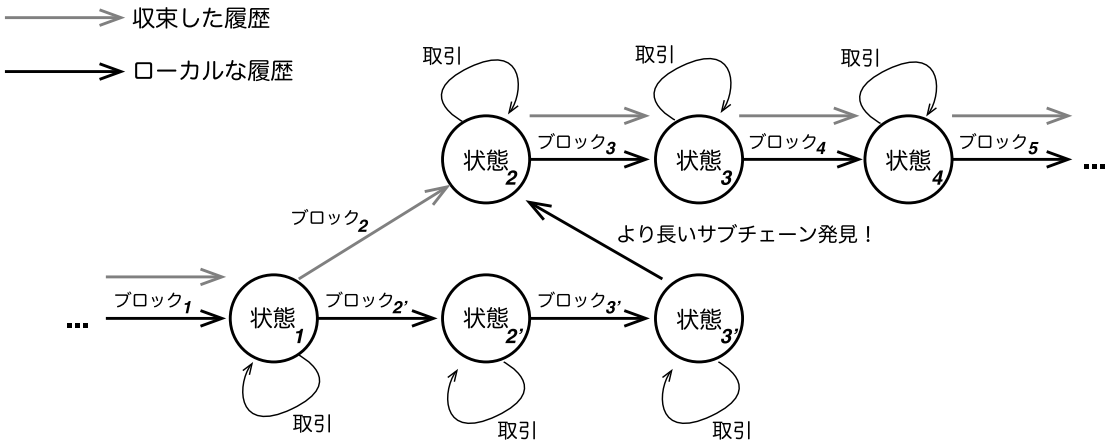

図 11: ブロックチェーンの確率的状態マシン

また、収束は各々の参加ノード上で非同期に進行するため、応答性は高いが、応答内容の一貫性には欠けることになる。

これは不確実性が許容できるアプリケーションに適合する考え方であり、金融業における応用では、保険を掛けられる範囲での利用が向いていると言える。

5.4 拡張されたビザンチン将軍問題

Lamport らによって 1982 年に定式化されたビザンチン将軍問題 [8] は、以下のものである。

- 前提
  - n 人の将軍がそれぞれの軍隊を率いており、攻めるか、撤退するか、合意しなければならない。
  - 将軍らは地理的に隔離されていて、伝令者を通してしか通信できない。
  - 高々 f 人の裏切り者/届かない伝令者がいる。
- ゴール
  - 忠実な将軍は全員、同じ計画に合意する。
  - 合意された計画は、忠実な将軍の誰かの発案と等しい (裏切り者にだまされない)。

このように、伝令の未達や書き換えを含む任意の事象による障害を、歴史的にビザンチン障害と呼ぶ。

Lamport らは、[8] において、この問題の最適解の条件が $n > 3f$ であることを示した。一方、ビットコイン・ブロックチェーン等、permissionless なブロックチェーンでは、n は未知である (対して、分散トランザクションシステムでは、n は動的に変化し得るが、既知である)。

表 3: ブロックチェーンとビザンチンパクソス

項目	**ブロックチェーン**	**ビザンチンパクソス**
特徴	資源の総和を利用する	参加者の総数を利用する
動作条件	$P > 2F$ ただし資源の総和 P は未知	$n > 3f$ ただし参加者の総数 n は既知
採用条件	• n が大きい • f は未知 • 確率的な状態遷移を許容	• f の上限を決められる
備考	エクリプス攻撃への対策が必要	メンバシップ管理が必要

そこで、n が未知の場合も想定して、新たに以下のように変数を定義し、ブロックチェーンとビザンチンパクソス (Lamport によるコンセンサスアルゴリズムであるパクソス (Paxos) をビザンチン障害耐性を持つように拡張したと見なせる一連のプロトコル [4] [5]) を比較したのが表 3である。

- n : 参加者の数
- f : ビザンチン障害下の参加者の数
- P : 投入される資源量

  (ビットコイン・ブロックチェーンにおいては計算パワー (電力) であるが、他にも、ブロックチェーンで扱われる通貨量等を競争に用いる方式があり、それらを「参加者が投入する資源量」として一般化したもの。)
- F : ビザンチン障害下の参加者により投入される資源量

ブロックチェーンにおいては、停止している参加者は (それによりネットワークが分断されなければ) F を増加させず、P と F を同量、減少させるため、動作条件の成立に影響しない。ただし、n が小さければ、一般には個々の参加者の投入する資源量の影響力が大きくなり、動作条件を成立させないことが容易になるため、採用条件としては n が大きいことが重要となる。

ブロックチェーンの動作条件 $P > 2F$ は、参加者 i が投入する資源量を P_i と置けば、n や f を用いて

$$\sum_{i=0}^{n-1} P_i > 2 \sum_{j=0}^{f-1} P_j$$

または

$$\sum_{i=f}^{n-1} P_i > \sum_{j=0}^{f-1} P_j$$

と書ける。これを用いることで、ブロックチェーンとビザンチンパクソスの動作条件・採用条件についてより詳細な議論を行うことも可能であるが、別の機会に譲りたい。

5.5 エクリプス攻撃に対する脆弱性

ここで、表 3の備考に示した「エクリプス攻撃」について、特に触れておきたい。

ブロックチェーン方式には、ネットワークに関わる隠れた前提条件があり、その前提が覆されるとコンセンサスの形成に失敗する。その前提条件とは、ネットワークにブロードキャストされた取引、あるいはその帰結としてのブロックが、いずれ参加者全員に届くというものである。

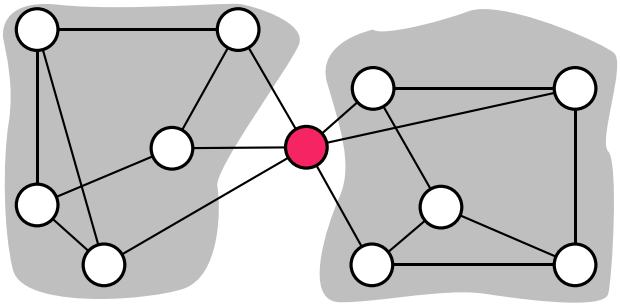

図 12: エクリプス攻撃の概念

無秩序に作られる P2P ネットワークでは、ネットワークを分断し、この条件を満たさなくするような攻撃が一般に可能である。このような攻撃 (図 12) を「エクリプス攻撃 (eclipse attack)」と呼ぶ。

この攻撃では、裏切り者がネットワークを分断し、互いのサブネットワークへの情報の転送をわざと行わないことで、互いを見えなくする。これは、ブロックチェーンの場合は、チェーンの分岐が永続することを意味する。

この攻撃は $f = 1$ で原理的に可能である (それを暴論だと思う場合は、n より十分に小さい数 C を用いて、$f = C$ で可能だと読み替えて欲しい)。資源の総和 P は無関係であり、ブロックチェーンの動作条件は崩れることになる。

一方、ビザンチンパクソスでは、「参加者の各々を互いに結ぶ通信路が存在する」という条件を明示して考えることが多い。この前提が崩れる場合に関しても、分断された反対側のネットワークに存在する参加者の数を f に組み入れて考えることで、動作条件の議論が可能である。

エクリプス攻撃に対するビットコイン・ブロックチェーンの脆弱性については、既存の研究 [7] が存在する。この研究では、改善策を提案し、一部がビットコインの開発コミュニティにより採用されている。また、ブロックチェーン一般に適用できる研究として [18] がある。これは、上記改善策も不十分であることを示唆した包括的な研究である

ブロックチェーンが向いているとされる、不特定多数が参加する状況では、エクリプス攻撃は無視できず、何らかの対策が必要である。

6　その他の分散レッジャー技術

6.1　リップル

「リップル (Ripple)」[10] (https://ripple.com) は、信用できる共通の第三者を含む支払い経路を見つけることに基づく分散型の支払いシステムであり、Ripple Labs により運用される。そのアイデア自体は 2004 年頃にすでに提唱されていたが、初期のアイデアはコンセンサスには言及していなかった。

リップルにおける支払い経路は「リップルパス (Ripple path; リップル経路)」と呼ばれる。例えば、ユーザ A がユーザ C に支払いたいが、直接使える支払い手段を持たないとする。このとき、もし A は B に支払え、B は C に支払えるとするなら、A → B → C がリップルパスとなる。リップルにおける支払いは、任意の通貨建てによる IOU (I Owe You; 非公式な借用書) の清算という形態をとる。支払いの際には、手数料を共通通貨である XRP (リップルクレジット) で支払う。

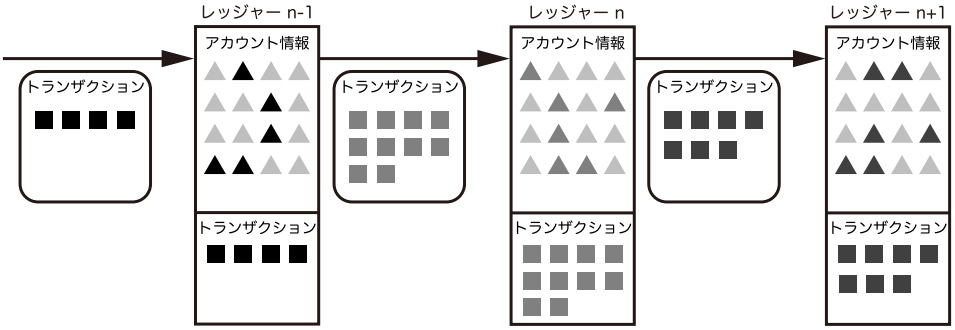

図 13: リップルにおけるレッジャー

リップルにおけるコンセンサス形成は、リップルのネットワーク全体が同一の「レッジャー」に合意する過程である。リップルでのレッジャーは、システムの状態のスナップショットであり、全員の口座残高や与信情報などを含む。レッジャーの内容はトランザクションにより変化することになる (図 13)。この構造はブロックチェーンと類似しており、設計上の影響が見られる。

リップルでは、多数決を用いて、現在のレッジャーに対して適用するトランザクションの集合に合意する。この際、合意はそれぞれの参加者が構成員を選ぶ「UNL (Unique Node List)」と呼ばれるサブネットワーク内で取られる。したがって、コンセンサスが実際に一意となるかどうかの精度は UNL の構成に依存する。

UNL は、共謀しないことが信用できる実名の参加者の集まりであり、ユーザはそれぞれ 1,000 ノード以上を選択し UNL を形成する。「異なる大陸から 200 ずつ選ぶ」「商業・金融・非営利・政党・宗教など異なるカテゴリーから選ぶ」といったことが推奨されるが、実用上はクライアントソフトウェアが選択するデフォルトの UNL を使用することになると考えられる。

UNL 内の多数決で「採用するトランザクション集合」を決めるが、このとき、最大で 80% のノードの合意が必要とされる。互いと共通のノードを持たない UNL を採用すると、全体でのコンセンサスは達成できないが、実用上は UNL のノードは重複すると前提できる。図 14 は、UNL 間でどの程度の重複が必要かを図示したものである。図で、破線で示したノードはノード数 6 のクラスタ (集まり) とノード数 5 のクラスタを繋いでおり、それらに共通である。クラスタが互いと異なる合意に向かうと仮定する場合、a) の状況では互いのクラスタ内の破線ノードをマイノリティと見なせるため、全体の合意が達成できないが、b) の状況ではその数が $\frac{1}{5}$ 以上となるため、クラスタ同士が互いと異なる合意に達することはできない。

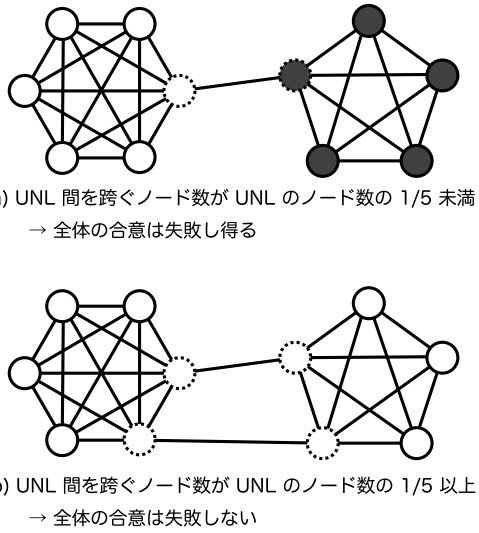

図 14: リップルにおける UNL と合意形成

合意が速やかに形成されるためには、矛盾するふたつのトランザクションのうちどちらを選ぶかについてのルールがなければならない。リップルでは、トランザクションはソートされ、矛盾するふたつのトランザクションのうち先のものが常に採用される。

このように、リップルは作業証明のコストを排し、かつ任意の通貨による取引をホストできる新たな仕組みではあるが、共謀に関する条件や UNL の重複に関する条件等、コンセンサスが成立するための条件が多岐に渡り、ビットコイン・ブロックチェーンのようにほぼメインテナンスフリーで動くようには思えない。

6.2 ハイパーレッジャー

「ハイパーレッジャー (Hyperledger)」(http://digitalasset.com/hyperledger/index.html) は、当初はオープンソースコミュニティにより開発され、現在は Digital Asset Holdings が開発・提供する分散レッジャーである。

コードが安定し、再びオープンソース化されるまでの間、詳細は不明だが、資料によれば、ハイパーレッジャーはブロックチェーン技術とは異なり、一連の「実用的ビザンチン障害耐性 (practical Byzantine fault-tolerance)」技術 [4] [5] に基づくものと考えられる。データ構造としては UTXO 形式 (第 2.2節) を採用すると見られる。

7 その他のフィンテック系話題

7.1 分散レッジャー以外の話題

フィンテックの文脈において、分散レッジャー以外に注目されている技術やサービスには以下のようなものがある。

1. 新たな融資・出資方法

(a) クラウドファンディングまたはレンディング (crowdfunding or lending)
インターネットを通して出資・寄付や融資を募るサービスである。

(b) ネットワークにより支援される融資
ネットワークに接続された POS を通して店舗の経営状況を把握すること等を通して、より効果的かつ顧客の負担を軽減したかたちで融資を行うサービスである。

2. 新たな資産運用・管理サービス

(a) ロボ・アドバイザ (robo-advisors)
資産運用のためのエキスパートシステム (簡易な人工知能による診断プログラム) である。

(b) 個人資産管理 (Personal Financial Management)
複数の銀行口座をまとめて管理できるようなサービスである。
いわゆる銀行 API が整備される以前である現在は、オンラインバンキングのパスワードをサービス運用会社に預けて実現する等、セキュリティ上および銀行との約款上の問題がある。

7.2 フィンテックとポリシー

フィンテックの文脈における標準化に関わる動きを列挙する。

1. R3 (http://r3cev.com/)

   R3 CEV (以下 R3) はニューヨーク等を拠点とするベンチャー企業であり、分散レッジャーに関して金融機関を束ねたコンソーシアムを運営する。コンソーシアムには、日本のメガバンク 3 行を含む、世界の多くの金融機関が参加している。

   R3 の目的は、銀行業務上の要求 (セキュリティ、信頼性、性能、スケーラビリティ、監査) を満たす分散レッジャーの共同研究および開発であり、以下を行う。

   - 1 日当たり数千億トランザクション (数百万/秒) の達成。
   - 互いに分析・検証可能な共用データの格納と維持。
   - 研究室環境 (サンドボックス) でのプロトタイプの検証。
   - 「ウォール街における課題」を解決する商用アプリケーションの開発。

2. Financial Innovation Now (https://financialinnovationnow.org)

   Financial Innovation Now は、Amazon, Apple, Google, PayPal 等から成るコンソーシアムであり、主として送金の分野におけるイノベーションを追求する。

3. Linux Foundation の open ledger プロジェクト (https://blockchain.linuxfoundation.org)

   Accenture、ANZ Bank、Cisco、CLS、Credits、Deutsche Börse、Digital Asset Holdings (Hyperledger; 第 6.2節)、DTCC、富士通、IC3、IBM、Intel、J.P.Morgan、ロンドン証券取引所グループ、三菱 UFJ フィナンシャル グループ (MUFG)、R3 (上述)、State Street、SWIFT、VMware、および Wells Fargo が参加し、商取引のためのオープンな分散レッジャーの開発を行う。

4. W3C

   W3C においても、支払いインタフェースの標準化が検討されている。

5. 日本における動き

   経産省が「産業・金融・IT 融合に関する研究会 (FinTech 研究会)」をシリーズ開催している。2015 年末における現状は課題を明確にする問題発見のステージである。

8 おわりに

2015 年現在、金融業界において、ブロックチェーンおよび、より抽象化された概念である分散レッジャーに対する興味が過熱している。

しかし、ブロックチェーンには一定の応用可能性があるが、金融の根幹を成すシステムへの適用には向かない。そのような応用は、ブロックチェーンが意味をもつ以下の条件に合致しないためである。

- n が大きく、f が未知で、確率的な状態遷移を許容する (ただし n は参加者の総数で、f はその中でビザンチン障害下にある参加者の数)。

ただし、金融の根幹に対して適用できないからといって、n が大きく f が未知であることを前提とする分散レッジャー技術に価値がないわけではない。仮にそのような技術が社会の基盤として活用されれば、金融業に対してディスラプティブな効果をもたらし、従来の金融という概念そのものが揺らぎかねないからである。

とはいえ、ブロックチェーンは技術的に幾つもの課題を抱えており、社会の基盤として用いていくには心許ない。その根本的に大きな問題に、適用する取引ないしトランザクションの集合を時系列に一列に並べる「全順序 (total order)」を維持するという考え方がある。

これは、ビットコイン・ブロックチェーンの設計が付けた道筋であるが、グローバルで単一なデータ構造を全員が共有し、そこへのアクセスが無ければシステムの状態を遷移させられない (例えば、送金できない) という仕組みである限り、様々な事故や障害の発生 (によるネットワークの分断) などを考慮すれば、日常生活をこの技術に依存することは危うく、国際送金など限定的な場面でしか十分には使用できないことになる。地域・局所性などに基づいてデータ構造に管轄を設ける分権が実現できなければ、段階的に地域性をもつ社会の構造にマッチできないのである。

仮に、全順序ではなく、因果関係の前後のみを保証する「因果順序 (causal order)」に基づく基盤が作れるとすれば、無関係なトランザクション同士の順序を考える必要はなく、分権が可能になる。社会に実際にフィットするコンセンサス基盤を作るためのヒントは、その辺りにあるのかも知れない。

また、現状では最も信用のおけるブロックチェーン環境は未だにビットコイン・ブロックチェーンであるが、これについては、2016 年 6 月にマイニング報酬が半減するという大きな出来事が待ち構えている。この夏が何らかの大きな変化の起点となることは間違いなく、依然としてフィンテックの動向からは目が離せない状況が続く。

参考文献

[1] Yoni Assia, Vitalik Buterin, m liorhakiLior, Meni Rosenfeld, and Rotem Lev. Colored Coins whitepaper. Available electronically at https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE.

[2] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. Enabling Blockchain Innovations with Pegged Sidechains. Available electronically at https://blockstream.com/sidechains.pdf.

[3] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. Available electronically at https://github.com/ethereum/wiki/wiki/White-Paper.

[4] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems (TOCS)*, Vol. 20, No. 4, November 2002.

[5] Allen Clement, Edmund Wong, Lorenzo Alvisi, Mike Dahlin, and Mirco Marchetti. Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults. In *Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI '09)*. USENIX Association, 2009.

[6] Seth Gilbert and Nancy Lynch. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-tolerant Web Services. *ACM SIGACT News*, Vol. 33, No. 2, June 2002.

[7] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse Attacks on Bitcoin's Peer-to-peer Network. In *Proceedings of the 24th USENIX Conference on Security Symposium*. USENIX Association, 2015.

[8] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Vol. 4, No. 3, July 1982.

[9] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Available electronically at http://bitcoin.org/bitcoin.pdf.

[10] David Schwartz, Noah Youngs, and Arthur Britto. The Ripple Protocol Consensus Algorithm. Available electronically at https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[11] 斉藤賢爾. インターネットで変わる「お金」 ビットコインが教えたこと. 幻冬舎ルネッサンス新書, 2014 年 12 月.

[12] 斉藤賢爾. インターネットと金融 — 弱体化する貨幣経済 (角川インターネット講座 10 第三の産業革命 経済と労働の変化 第 9 章). 角川学芸出版, 2015 年 2 月.

[13] 斉藤賢爾. 未来を変える通貨 ビットコイン改革論. インプレス R&D, 2015 年 5 月.

[14] 斉藤賢爾. お金のギモン！　何で私に聞くんですか？ 金曜日, 2015 年 6 月.

[15] 斉藤賢爾. ネットワーク参加者の「コンセンサス」を確保する仕組み：分散処理でも単一の元帳を維持できるのはなぜか (特集 暗号通貨 2.0). 金融財政事情, Vol. 66, No. 21, pp. 20–27, 2015 年 6 月.

[16] 斉藤賢爾. ビットコインというシステム (特集　情報通信プラットフォームをめぐる法と政策/暗号通貨の諸問題 (ビットコインを題材に)). 法とコンピュータ, Vol. 33, pp. 21–29, 2015 年 7 月.

[17] 斉藤賢爾. ビットコインと来たるべき社会変容 (特集 ビットコインを知る). 月刊金融ジャーナル, Vol. 56, No. 7, pp. 8–11, 2015 年 7 月.

[18] 澁田拓也. 単一グローバル台帳暗号通貨のエクリプス攻撃脆弱性分析. 修士論文, 慶應義塾大学 大学院 政策・メディア研究科, 2015 年 7 月.