応
専

❺ ブロックチェーンの分散台帳を利用した電子投票による集合知の構成

―対称的な非集中型監査と絶対中立的な非可逆的記録―

山崎重一郎（近畿大学）

仮想通貨以外の用途へのブロックチェーンの適用

「ブロックチェーン」という用語は甚だしく拡大解釈されている．また，「ブロックチェーン」に対して，仮想通貨以外の用途にも広範に利用可能な有望な技術だ，という期待が広まっている．その期待に呼応して「ブロックチェーン」と称するシステムが次々に登場している．「ブロックチェーン」はまだ未熟な技術であり，多様なデザインが試行錯誤されること自体は望ましい．しかし「ブロックチェーン」と自称している技術が本当に期待されているようなものであるか，それとも幻想かという判断は難しい．

本稿の目的は，仮想通貨以外の用途への「ブロックチェーン」技術の利用可能性について，要件の整理を試みることである．

我々の立脚点は，「ブロックチェーン」という用語の唯一の実像であるビットコインのブロックチェーンである．我々は，これが（1）「対称的な非集中型の監査」を継続的に実施しているシステムであって，かつ（2）「絶対中立的な記録」を実現しているシステムである，という 2 つの特性を持つことに注目する．そしてこの 2 つの性質を備えた「ブロックチェーン」が従来のデータベース技術で実現されている電子投票システムよりも優れていることを明らかにする．

これは同時に，データベース技術と実質的に同等な技術を「ブロックチェーン」と呼称していることへの違和感を際立たせることにもなるだろう．

そして我々が開発した，集合知の構成を目的とする電子投票システム CongreChain（コングレチェイン）を題材に実現技術や課題について説明する．また，関連して「ブロックチェーン」の技術的チャレンジの方向性についても言及する．

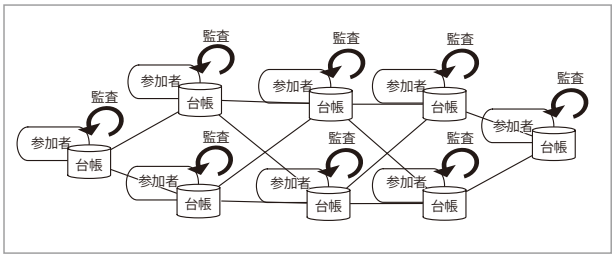

図 -1　対称的な非集中型の台帳監査システム

● ザ・ブロックチェーン

ビットコインの発明者のサトシ・ナカモト（偽名）の論文[1]によると，ビットコインの開発目的は「信頼できる第三者」を必要としない通貨システムの提案である．そしてブロックチェーンは仮想通貨ビットコインの中核となる台帳システムとして発明された．

電子通貨の最大の課題は，電子通貨の二重使用の問題である．従来はこの問題の解決には，IC カードなどの特殊なハードウェアや信頼できるサーバが必要だと考えられていた．ビットコインは，世界中のおびただしい数の仮想通貨利用者によって構成される P2P 型ネットワークのすべてのノードが，ブロックチェーンによる取引台帳の整合性監査を定常的に繰り返すことによって，電子通貨の二重使用の問題をソフトウェアだけで鮮やかに解決した．

ビットコインの P2P 型ネットワークのノードはすべて対等で特別なものは 1 つも存在しない．つまり，ビットコインのブロックチェーンは完全に対称的な非集中型 (decentralized) の台帳監査システムである（**図 -1**）．

またビットコインでは，通貨発行益をめぐるゴー

ルドラッシュに似た人々の欲望に基づく計算競争（マイニング）が常態となるよう巧妙に設計されている．この競争に勝利するためには消費電力が問題となるほどの莫大な計算が必要である．

この競争状態は，仮想通貨システムにおいて3つの重要な機能を担っている．その1つ目は，仮想通貨経済圏における通貨発行手段となっていることである．2つ目は，地球全体に広がる大規模な分散台帳システムにおいて，世界各地で非同期に発生する台帳記録を時系列的に一貫したものになるよう，マイニング競争によって生じる一種の確率的な選択の繰り返しによって最終的に記録内容を一意に合意するための手段になっている．3つ目は，この計算競争が結果として，ビットコインのブロックチェーンの台帳記録をいかなる人や組織にも書き戻すことができない非可逆的記録にしているということである．なぜなら，いったん書き込まれた台帳記録を後で書き換えるためには，マイニング競争の計算結果を再計算し，さらに一定期間マイニング競争に連続して勝利する必要があるが，現実的にそれが不可能だからである．

これらの中で，特に3つ目の機能が重要だが，これは技術的な仕組みだけで実現されているわけではない．ビットコインが仮想通貨として現実に価値を持ち，それを求めて膨大な計算を行い続けているマイナーの存在が不可欠である．

ビットコインのブロックチェーンがほかと本質的に異なるのは，それがすでに1兆円規模の資産総額を持つ仮想通貨のインフラとして存在していることである．技術としての分散合意システムや分散データベースなどを指しているのではない．

これは，「インターネット」という用語が単にTCP/IP技術による自律分散型ネットワーク一般を意味するのではなく，現在，全世界の人々が日常的に利用している「その」ネットワークそのものを指し示しているのと同じである．本稿では，これ以降ではビットコインのブロックチェーンを「ザ・ブロックチェーン」と呼ぶことにする．

ザ・ブロックチェーンは，(1) すべてのノードが対称的な非集中型の台帳監査システムであり (2) いかなる人や組織にも支配できない絶対中立的な非可逆的記録である，という2つの性質を備える．

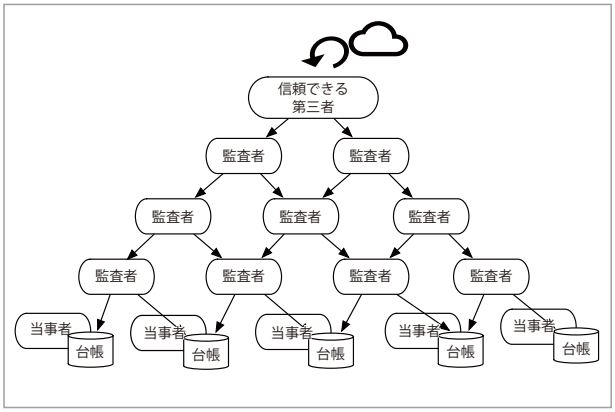

図 -2 「信頼できる第三者」による階層的統治

●「信頼できる第三者」による統治

現代の，通貨，行政，政治，金融などに対する統治システムは「信頼できる第三者」の存在を前提としている．中央銀行，行政機関，政府，金融機関や監査法人などがその例である．「信頼できる第三者」は，我々の社会活動や経済活動などに必要な信用の起点だが，決して永遠不滅なものではない．したがってこれらの重要な「信頼できる第三者」は，社会の安定のためにその信用が虚構でないことを常に示し続けなければならない（**図 -2**）．

また，信用を保つためには，統治が法に基いて適正に運用されていることを検証するための検証者が必要である．またその検証者を検証するためにはさらに上位の検証者が必要である．「信頼できる第三者」とは，このような検証の連鎖による階層的な統治構造の頂点に位置する検証者でもある．

●「信頼できる第三者」による統治の利点と問題点

階層化された統治システムは効率的であり，それによって現代社会の健全性，安定性が保たれていると言ってよいだろう．通貨価値の安定性や社会の平等性や経済活動の健全性などは，まさに人類の英知の集積をもとに信任を受けた人々のたゆまぬ努力に

よって実現されている．

しかし，階層化された統治システムは，その頂点に近づくほど「信頼できる第三者」に対する検証が難しいという問題がある．現在の日本の通貨，行政，政治，金融などの統治は，世界の中では比較的健全に保たれていると言ってよいが，それでも統治の失敗の例は枚挙にいとまがない．

2016 年 6 月の舛添要一東京都知事の辞職問題で明らかになったように，自治体の決裁権限の頂点に位置する東京都知事という「信頼できる第三者」が行った決裁は，制度としては誰の検証も受けない．事実，弁護士による第三者委員会も常識的には不適切と思われる支出についても，知事が決裁した結果を法的な不正として立件することはできなかった．

また，投票における「信頼できる第三者」の代表は選挙管理委員会であるが，その開票作業や集計の正しさも，民主的な選挙制度が定着しているとされる現在の日本でさえ自明なものではない．

2013 年 7 月 21 日に施行された第 23 回参議院議員通常選挙において，香川県高松市選挙管理委員会が比例代表の開票の際，高松市選挙管理委員会事務局長が集計済みの白票約 300 票を再度入力させ白票を増やしたという事件があった．

世界の国々を見ていくと，「信頼できる第三者」の腐敗や不正がもっと深刻な国はたくさん存在する．ほとんどの国で，通貨，行政，政治，金融などの統治には構造的な問題が潜在していると言ってよいだろう．そして「ブロックチェーン」への期待もそこにある．

対称的な非集中型システムによる監査と絶対平等的な記録による統治

● 対称的な非集中型システムによる互恵的なコストの分散負担

「信頼できる第三者」であり続けるためには，きわめて重いコストを負担しなければならない．たとえば銀行などの金融機関は「信頼できる台帳」を維持するために莫大なコストを費やしている．銀行の「信頼できる台帳」を維持するためには，銀行が扱う膨大な数の取引に関して，その内容の正確性と整合性の確保や改ざん防止が必要である．そして，システムは数秒の停止も許されず，いついかなるときでも利用できる状態を永続的に保つ必要がある．またそのコストには，モラルを保つための人件費や大規模な災害に耐える拠点の立地や建築設備，組織犯罪やテロへの対策なども含まれる．

ザ・ブロックチェーンの維持管理コストは，世界中のおびただしい数の参加者全員により均等に互恵的に負担されるために，1 つのノードあたりの負担は小さく見える．また，ザ・ブロックチェーンは「野生」のブロックチェーンである．このため新たに「ブロックチェーン」を構築するコストが不要なことも，非常に重要である．もし人工的に同等の「ブロックチェーン」を構築しようとすると，現行の銀行のシステムの構築と変わらないほどのコストが必要だろう．

ザ・ブロックチェーンはきわめて頑強なシステムであり，2009 年 1 月 3 日の運用開始以来，現在に至るまで実質的には一度も停止状態には至っていないと言われている．このザ・ブロックチェーンの頑強性は，ノード数の規模が重要な役割を果たしている．

ザ・ブロックチェーンをターゲットにした大規模なスパムや実装の脆弱性をついた攻撃などは幾度も発生している．数秒の停止も許されない銀行の台帳システムと確率的に決済の完了が確定するビットコインを直接比較するのはフェアではないが，誰でも攻撃可能なパブリックなネットワークシステムでありながら，仮想通貨（現金）取引の台帳記録の整合性が深刻なレベルで毀損されたことがないことは驚くべきことである．また，過去の攻撃への対応として繰り返された改良によって，より頑強なものに進化してきたとも言える．

もし銀行が自社で運営している「信頼できる台帳」をザ・ブロックチェーンに置き換えることができれば，企業コンプライアンスや法制度に準拠するためのコストなど，新たに発生するコストも存在するが，それらを考慮してもメリットは大きいだろう．残念なことに現在のザ・ブロックチェーンでは性能

やスケーラビリティや台帳記録の表現力や認証／認可などのセキュリティ基盤や法制度の未整備などで，すぐにそれを実現することは不可能である．しかし，技術革新による進化は進んでいる．すでに有望な技術はいくつか存在し，ザ・ブロックチェーンへの適用も始まっている．

一方で，「ブロックチェーン」と呼ばれているシステムの中には，対称性を放棄し，限定された少数のノードに特別な役割を担わせているものがある．そういうものの中には，性能要件を満たすには 20 ノード未満のスケーラビリティしか許容できない「ブロックチェーン」技術も存在している．こういう非対称的な「ブロックチェーン」の中には，現行のデータベース技術に近い性能を示すものもあるが，管理，運用のコストや頑強性などを含めて，総合的に従来のデータベース技術の代替技術の観点で評価するべきだろう．

● 'Code' が支配する絶対中立的記録

ザ・ブロックチェーンは，人が創りだしたものでありながら，人には支配できないシステムである．ザ・ブロックチェーンの記録は，国家や大企業などを含めて，特定の人や組織には絶対に支配できない中立的な非可逆的記録である．ザ・ブロックチェーンは，人ではなく 'Code'（プログラムと法の 2 つの意味を持つ）が支配している．すべてのノードが 'Code' の仕様にそって台帳記録の検証を行うからである（**図 -3**）．

絶対中立的なシステムの運用方法の知見は少ない．たとえば，'Code' そのもののガバナンスの方法もその 1 つである．現時点では BIP-9[2] などの提案が存在し，すでに実施されている．手探りながら確実に前進していると言ってよいだろう．

この絶対中立的な非可逆的記録という性質は，ほかの「ブロックチェーン」では自明ではない．たとえば，仮想通貨 Ethereum では，2016 年 6 月に The DAO という Ethereum 上のクラウド・ファンディング・プラットフォームからの資金流失事件が発生し，被害者らの圧力によって，Ethereum のブロックチェーンを事件発生以前の時点にまで書き戻した．これを実施したのは，Ethereum の発明者であり主要な開発者でもある Vitalik Buterin 氏である．この事実により，Ethereum のブロックチェーンは，絶対中立的な非可逆的記録ではないことが分かる．

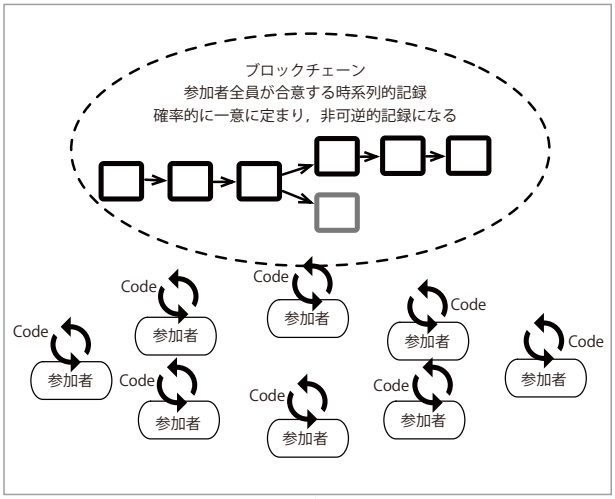

図 -3　絶対中立的記録としてのブロックチェーン

ブロックチェーンの投票への適用

ブロックチェーンの通貨システム以外への適用可能性を検討するための最初の一歩として，投票への利用について検討する．

仮想通貨ビットコインは，「通貨とは何か」という根本的な問に対しても多くの知見を与えるものであった．電子投票について議論しようとするときも，やはり「投票とは何か」という問から始めなければならないだろう．

● 投票とはなにか

投票による多数決は社会的選択における民主的なコンセンサス形成の方法の 1 つとして古代から世界各地で利用されてきた．特にフランス革命期に登場した Rousseau の「社会契約論」で人民主権の理論の中で精密にその意味が検討された．

Rousseau は，主権者である個人は，自分が属する集合体の一員としての自分自身と「社会契約」を結んでいるとしている．個人は，自分の利害に基

づく意志だけでなく，自分が属している社会の一員として利害を超えた意志を持つこともできるとし，それを「一般意志」と呼んでいる．Borda や Condorcet は，この Rousseau の思想の影響の下に投票による多数決を，この一般意志を明らかにするための社会的装置の 1 つであると考え，その問題点の指摘と数学的基礎の精緻化を試みている．

● 国家や組織などから中立な投票システム

投票には，「一般意志」の概念を持ち出すまでもなく，政府や特定の組織を超越した中立性が要求される．ビットコインは，国家や企業などの信用に依存しない通貨を実現したが，電子投票システムは，電子通貨以上に国家や組織に依存するべきでない．したがって，電子投票システムには，きわめて高水準の透明性と中立性が要求されることになる．

紙の投票用紙による投票の場合，投票後に投票箱が開けられ，投票用紙に記載された文字を読む開票作業や集計を行う作業を行うのは選挙管理委員会の担当者であり，その作業に不正が生じる可能性を完全に払拭することはできない．

● 理想の電子投票システムの要件

電子投票の場合は，選挙管理委員会に加えて，システムを作成するベンダや運用管理を担当する企業が存在するため，これらの不正についても対策が必要である．理想的な電子投票の要件は，以下のようなものである [1]．

（1）投票資格の検査と本人確認
（2）投票の一意性（二重投票の防止）
（3）投票内容の正確性
（4）投票内容の改変不能性
（5）投票内容の検証可能性と追跡可能性
（6）システム自体の信頼性
（7）個人の投票内容と方法の秘匿性
（8）柔軟性（複数の投票手段が選択できる）
（9）利便性（情報リテラシーが不要）
（10）試験可能性（仕様を投票者が確認できる）
（11）透明性（投票に関する全工程の可視化）
（12）システムの運用コストが合理的

● ザ・ブロックチェーンによる電子投票システムの優位性

電子投票システムをザ・ブロックチェーンで実現する場合，投票結果は台帳として管理されるのが自然である．また投票は基本的に送金と同様の処理になるだろう．

上記の理想的な電子投票システムの要件のうち，（2）（3）（5）（6）（10）（11）（12）は，ザ・ブロックチェーンの特性である「対象的な非集中型監査」によって実現できる．また，（4）は「絶対中立的な非可逆記録」によって実現できる．（1）（7）（8）（9）などの要件は，それぞれすでに既存技術が存在する．

従来の従来のデータベース技術を核とする電子投票システムを採用した場合，「信頼できる第三者」を仮定しない電子投票システムで，（2）（3）（4）（5）（6）（10）（11）を実現することは，事実上実現不可能である．もし政府や選挙管理委員会やシステムベンダを「信頼できる第三者」としない場合にも，それらの外側に「信頼できる第三者」を導入することになるだろう．したがって，ザ・ブロックチェーンの「対象的な非集中型監査」と「絶対中立的な非可逆記録」という特性は電子投票システムに有用な特性である．

● 集合知形成のための投票

「対称的な非集中型監査」が実施される透明性の高い電子投票が可能なら，投票された結果のデータを活用して，単に候補者の得票数を集計する以上の高度な計算を行うことも可能になる．なぜならば，誰もがそのデータを利用して自分で計算を再現できるからである．

集団行動が個々のメンバの能力を超えることがあることは，社会性昆虫や動物の群れの行動などにおける「群知能（Swarm Intelligence）」として知られている．

あるいは，都市の公共施設の建設場所を選定するような投票の場合は，投票結果の公開データからの

適切な評価関数を計算することで，候補の中には直接存在しない最適な場所を選ぶことが可能になるかもしれない．

また，正解が存在するような 2 択問題の投票では，投票者の人数が増えるに従って多数決の結果が正解に近づくという「コンドルセの陪審定理」が存在する[3]．この定理には，いくつか仮定があるが，それに従うとすると，個々のメンバ 1 人の正解確率が 60% の場合，101 人で投票すると多数決が正解である確率は 98% に達する．

● CongreChain（コングレチェイン）

我々は，ザ・ブロックチェーンを利用した電子投票システム CongreChain を開発し，北九州市の門司港レトロ地区で開催されたイベント「第 2 回北九州カレーマルシェ選手権」で実験を行った．

CongreChain は，ビットコインのトランザクションデータにメタ情報を付加することによって，少額のビットコインの送金に乗せて，任意のアセットの流通させることを可能にする Open Assets Protocol を利用している．

また，コンドルセ - ヤング法[3]を利用した，コンドルセ表というデータ構造を利用したペア比較型投票を実装し，最尤法による順位判定を行った（**図 -4**）．

●「ブロックチェーン」技術の今後

本稿では，仮想通貨以外の用途への「ブロックチェーン」技術の利用可能性について，要件の整理を行った．

	A	B	C
A	-	4	3
B	7	-	5
C	8	6	-

A は B よりも美味しい：4 票
A は C よりも美味しい：3 票
B は A よりも美味しい：7 票
B は C よりも美味しい：5 票
C は A よりも美味しい：8 票
C は B よりも美味しい：6 票

A>B>C（A>B, B>C, A>C）4+5+3=12
A>C>B（A>C, C>B, A>B）3+6+4=13
B>A>C（B>A, A>C, B>C）7+3+5=15
B>C>A（B>C, C>A, B>A）5+8+7=20
C>A>B（C>A, A>B, C>B）8+4+6=18
C>B>A（C>B, B>A, C>A）6+7+8=21 ←最尤順序

図 -4　コンドルセ表による順位判定の例

現在進められているさまざまな「ブロックチェーン」技術の研究開発は，この技術が実用技術に成長するために必要不可欠である．ただし，それは，ザ・ブロックチェーンと独立なものではないだろう．さまざまなインターネット技術がザ・インターネットを発展させていったように，「ブロックチェーン」技術は，ザ・ブロックチェーンの問題点を補完し拡張する形で発展していくのではないだろうか．

参考文献
1）Gritzalis, D. : Secure Electronic Voting : New Trends, New Threats, New Options, 7th Computer Security Incidents Response Teams Workshop (2002).
2）Wuille, P., et. al. : BIP 9, Version Bits with Timeout and Delay (2015).
3）坂井豊貴 : 社会的選択理論への招待―投票と多数決の科学 , 日本評論社（2013）．

（2016 年 9 月 1 日受付）

山崎重一郎（正会員） yamasaki@fuk.kindai.ac.jp

近畿大学 産業理工学部 情報学科教授．博士（情報科学）九州大学，1983 年富士通入社．富士通研究所を経て，2003 年より現職．