第７部

特集7 ブロックチェーン技術

鈴木 茂哉

第１章　ブロックチェーン技術の最初の10年

Bitcoinをナカモトサトシが論文として発表し[58]、そのコードが世に出てから10年が経った。その間、インターネット技術のような段階的・実践的な試練を経ずに、即座に実践的に使おうと、多くの投資家やスタートアップ企業によってブロックチェーン関連のビジネスが立ち上げられた。この間、多くの報道にあるように、様々なセキュリティインシデントによる資産流出事故が起きている。これらの事件は、ブロックチェーン自身の問題というよりはブロックチェーンを活用するための周辺技術が十分成熟していないことに起因するように見受けられる。

ブロックチェーンが有用な可能性のある技術であるかどうかについては、まだ議論の余地がある。様々なアプリケーションが開発されつつあるが、既存のデータベースを用いることと比してメリットを感じられないものが多い。一方、分散技術の視点で、ブロックチェーンは、後に述べるようにとてもユニークな特性をもつ技術であると考えられ、特に、分散技術を中心に研究しているWIDEプロジェクトにおいては取り組む価値が十分ある。

本節では、ブロックチェーン自身というよりは、それを取り巻くシステムという見視点を中心にして、ブロックチェーンの現在について整理する。なお、DLT（Distributed Ledger Technology - 分散台帳技術）という語が、より一般的であるという意見も昨今聞くようになってきているが、ブロックチェーン技術は、分散台帳を作るためにだけ使える技術だとは考えにくく、分散台帳に限らず広く用いることができる方式であると考え、本章ではブロックチェーンという語を用いることにする。

第２章　ブロックチェーンの課題

現在のブロックチェーンの課題は、技術的もの、システム設計及び運用に関したもの、エコシステムのガバナンスに関するものと整理できる。以下、それぞれについて議論する。

2.1　技術的な課題

技術的には、スケーラビリティ、プライバシ、セキュリティ、ファイナリティといった領域に課題がある。また、ネットワークに関連した部分でも議論を合わせて紹介する。

2.2　スケラービリティ

ブロックチェーンには、主に、トランザクション速度とブロックチェーンを保持するストレージの点で、スケーラビリティに課題がある。

広く知られているように、Bitcoinブロックチェーンは Proof of Workと呼ばれる手法により、最後に接続するブロックの決定を行っている。Proof of Workによる接続が10分程度になるように必要計算量が定期的に調整される。また、ブロックのサイズは1メガバイトに制限されている。ブロックに納めらられるトランザクションは可変長であるが、過去1年の統計値を見ると平均400バイト前後、ブロック当たりのトランザクション数は2000～3000程度、すなわち、1秒あたり10トランザクション程度の性能となる。クレジットカードのトラザクションが秒間5万と言われているほか、中国で最もオンライン購買活動が盛んだと言われる11月11日「独身の日」のトランザクションが、2019年の場合、秒間54.4万[59]となっている。ユースケースの違いもあるとはいえ、この隔た

りは大きく、一定レベルの改善が求められるのは道理である。Bitcoinのスケーラビリティを上げるために、トランザクションデータの圧縮によりブロックの利用効率を高めたり、ブロック自体を大きくするという提案がなされているが、単純にブロックを大きくすることは、セキュリティ上望ましくないという考えもあり、現在のBitcoin Core（メインラインのBitcoin実装者によるリファレンスコード）では、トランザクションの大きさを小さくするアプローチがとられてきている。

一方、ストレージについては、現在の典型的なブロックチェーンが、全てのノードが全てのブロックの検証を行うことを前提とし、それぞれのノードが検証に必要な全てのデータを持つことを前提としていることによる、利用ストレージの単調増加への対応の必要性がある。筆者のグループでは、分散ハッシュテーブルを用いたストレージ分散方式を提案している[60]。この領域には、今までの分散コンピューティングにおける智恵が、まだ入っていない印象があり、引き続き研究を進めている。

2.3　プライバシと真正性の確保

ブロックチェーンで真正性を確保できるのは、ブロックが作成された時点から変更されていないことに対する確証が得られるにすぎない。ブロック内のデータの真正性を保証するメカニズムが必要であり、Bitcoinの場合は、トランザクション単位での公開鍵暗号による署名とその検証、および、トランザクション自体が改変されていないことをマークル木を用いて確認できることにより、検証可能としている。ここで、公開鍵暗号の利用は、特定の公開鍵に紐付いたコインを払い出すために用いているにすぎず、その鍵を誰が保持しているのかについては、検証不能である。つまり、Bitcoinに置いて特定の鍵を誰がもつのかという点について、トランザクションレベルでは、匿名性が成立している。一方、ブロックチェーン全体の支払いの流れや、外部情報に頼ることにより、匿名性が成立しない場合もある。

マネーロンダリング対策ということで、グローバル・ボーダレスな暗号資産は脅威となる。この視点で、匿名性をどのような形で排除するのか、あるいは、確保するのかについては様々な議論があり、ZCashのように特に匿名性を重視したブロックチェーンも検討されている。

一方、ブロックチェーンをアプリケーションプラットフォームとし、データの真正性を確認できるようなアプリケーション開発が試みられており、政府により実証実験なども行われてきている。データの真正性をデータの出自から確認したい場合は、どのような形で公開鍵暗号が用いられているのが鍵である。ここで重要なのは、「真正性の確保のため」に作成されたアプリケーションの場合、ブロックチェーンに納めるために署名に用いられる公開鍵を用いて、誰が署名したのかを確認することになるため、情報の出元で署名をしないと、意味が無くなる点である。筆者が観測している限りでは、たとえば、エンドユーザが署名するのではなく、エンドユーザが用いるアプリケーションサーバが保持する公開鍵暗号鍵ペアを用いて署名する実装が多々ある。この使い方の場合は、データの真正性は確認できるが、署名したのはサーバとなってしまうので、ブロックチェーンの本質的な利用となっていない。すなわち、ブロックチェーンの活用のためには、どのような鍵が用いられるかのデザインが極めて重要であり、この視点での研究が求められる。

2.4　ファイナリティ

ブロックチェーンにおいて、ある時点におけるブロックチェーンデータが将来にわたって変更が必要無くなることをファイナリティがある、という言い方をする。ファイナリティがあるブロックチェーンデザインが成立すると主張している実装や研究があるが、現時点で、本質的な意味でスケーラブルでブロックチェーンの特性を全て満たすものではないと考えられる。ファイナリティを満たすために特性の一部を犠牲にするような利用方法も十分考えられるが、既存のデータベースとの差がより少なくなると考えられる、ブロックチェーンを活かしているとは言えなくなる可能性がある。

2.5　各種パラメータとネットワーク特性との関係

ブロックチェーンシステムには、10分で一つのブロックが生成されるといった、いくつか注目に値するパラメータがあるほか、遅延などネットワークの特性に影響を受ける実装もある。これらについての研究は、WIDEプロジェクトで貢献できる領域であると考えられる。以下に、

ルーティングと遅延についての議論を紹介する。

Bitcoinは、10分に一つのブロックが生成される。一見、適当に思える選択であるが、単純に計算時間の設定を小さく減らし、短時間でブロック生成できるようにすると、安全性が下がるだけでなく、たとえば、下支えをしているインターネットにおけるルーティング変更にセンシティブになりうる点でもリスクがあると考えられる。筆者のグループでは、この点での検証を進めている。

また、一部のブロックチェーン実装はスケーラビリティを高めるための手法として、PBFT[66]のような、ビザンチン障害耐性(BFT)をもった合意形成プロトコルを用いているものがある。合意形成のためのメンバを絞ることによって、投票者を少なくし、現実的な実装としている。たとえば、コミッティー型のブロックチェーンは参加者を絞れるので、PBFTが十分適用可能である。また、ALGORAND[61]では、非常の多くの参加者がある状態であっても、過去のブロックチェーンの内容から、決定論的にコミッティメンバを選ぶことによって、BFTプロトコルを適用可能としている。

2.6 システム設計上及び運用上の問題

ブロックチェーンの運用において、暗号資産交換所で起きている問題を見ると、その殆どが、ブロックチェーン技術に固有な問題でない。唯一の例外は、鍵の管理と運用に纏わる複雑さと考えられる。

問題の一つの面は、署名をオンライン状態で行うためには、どうしても秘密鍵が何らかの形でオンラインになっている必要があるという点(いわゆるホットウォレット)である。この問題は暗号資産固有の問題ではなく、署名をオンライン状態で行う必要があるあらゆるオンラインシステムで共通な問題と言える。強固なサーバを作るために、インターネットのサービスでは、ハードウェアセキュリティモジュール(HSM)の活用などが行われてきており、アプリケーションによってはHSMの適切な運用で十分な強度を得ることも可能であるが、暗号資産の場合は、払い出しの署名が一度されてしまえば、その資産は失われてしまい、秘密鍵自体が盗まれるかどうかは重要でないという特性の違いがある。これらの視点から、一部有志によって、暗号資産におけるセキュリティ分析が行われており、更新が行われている[62]。

2.7 エコシステムのガバナンス

ブロックチェーン、あるいは、暗号資産のエコシステムをガバナンスという視点で捉えたとき、我々が着目すべき点が二点ある。

一つ目は、コードの安定性である。ブロックチェーンが今までの情報システムと決定的に異なる点は、コードとデータがセットで運用され活用されている点である。コードを活かすためにはデータがなければならないし、データを活かすためには、コンパチビリティのあるコードが必要である。ブロックチェーン以前のソフトウエアシステムの場合、バックワードコンパチビリティが概ね保たれるのが普通であり、特にWindowsエコシステムについては、過去のデータの活用性については注意深くデザインされている。従って、既存のデータと新しいオペレーティングシステムやアプリケーションを組み合わせることに大きな問題は生じないし、新しいアプリケーションがあればアップグレードパスがあり、ユーザの意思をもって、アップグレードのタイミングを選ぶことが出来る。一方、ブロックチェーンの場合、ブロックチェーンのデータ自身とコードのコンパチビリティが常時保証されている必要があり、必要に応じて、ソフトウェアコンパチビリティのある形、あるいは、ソフトウェアコンパチビリティのない形でのデータないしコードのアップグレードが行われ、それがソフトフォーク、ハードフォークという呼ばれ方をする。オペレータは、随時、自分のポリシーに見合ったアップグレードであるかどうかを見極めた上で、新しいソフトウエアを導入する必要があり、アップグレードしなかった場合によっては、当該ブロックチェーンの運用から取り残されて行くリスクがある。また、アプリケーションデベロッパの立ち場で言うと、コードのスタビリティが無いと開発がままならない。二つのメジャーなブロックチェーン実装、Bitcoin Core(現在の主流のリファレンス実装)とEthereumを見ると、Bitcoin Coreが非常に堅実な更新ポリシーを維持しているのに対し、Ethereumコミュニティは非常にアグレッシブにコードを修正していく。このため、Ethereumを用いるデベロッパは注意深く最新動向を追いつつ開発を進め

る必要がある。いずれにせよ、それぞれのデバロッパコミュニティがどのようにガバナンスされているかに依存しているわけで、ガバナンスの問題と言える。

二つ目は、健全な暗号資産エコシステム形成をどのように進めて行くかという視点である。Internetは、規制をはねのけ、グローバルなエコシステムを成立させた。暗号資産も、同様に、グローバルなエコシステムを成立させうる。ここ数年で、規制当局は、インターネットによるグローバル化で何が起きたかについて考え、暗号資産のエコシステムには、インターネットと同様のマルチステークホルダー型の協調が必要であると認識した([63]の13段落目)。議論は、金融庁の高梨氏の論文[takanashi]にまとめられている。これに従い、日本の金融庁が、過去3年弱の間、各方面に働きかけつつある状況にあり、2020年３月　に、"Blockchain Global Governance Conference (BG2C)"という会合を実施することになっている。

WIDEプロジェクト関係各方面においては、議論に参加または協力を仰ぐことになる。

第３章　ブロックチェーンに関連した技術・応用 - Identity技術

本節では、ブロックチェーン技術とIdentity技術の深い関連性について述べる。

先に議論したように、公開鍵がだれの持ち物であるかを知ること、すなわち、identity技術の応用は、ブロックチェーンの応用にとって決定的に重要である。反対に、identity技術の成立のために、ブロックチェーン技術が重要である。

現在、ブロックチェーンを用いたIdentity技術として、DIDがある。DID - Decentralized Identifier[64]は、IDの正しさを、スキームとデータで構成されるDID文字列から、スキームに応じた方法でDIDに含まれるデータを用い、検証するために必要な情報を含むDID Documentを得た上で、DID Documentに記載された情報を用いて、Identityの確からしさの検証を可能とする技術であり、W3Cで標準化が進んでいる。たとえば、Bitcoinブロックチェーンのトランザクションとして DID Documentを納め、そのトランザクションを指し示すDIDを作成し用いることが可能である。

また、統治可能なIDということで、ソブリンID (Sovering ID)、特に、自己統治可能なID (self sovering ID --SSI)も注目されている。現在用いられている認証技術は、Google、Facebookなど、なんらかのIDプロバイダ運用組織に依存しているが、たとえば、Google認証を用いているユーザがGoogleアカウントへのアクセスを停止された場合、Google認証を用いているサービスを受けられなくなるというリスクがある。無論これはGoogle内部のサービスに限らず、サードパーティサービスにおいても使えなくなるリスクがある。すなわち、最終的なコントロールをユーザ自身が持っていないといえる。そこで、自己ソブリンIDシステムでは、ユーザ自身が最終的なコントロールを掌握できるようなシステムとなっている。自己ソブリンIDシステムにおいては、基盤としてブロックチェーンが用いられており、たとえば、Sovrin Foundation[65]のSovrinが例として上げられる。

第４章　終わりに：WIDEとしての取り組みの方向性

最後に、ブロックチェーンの領域で、WIDEプロジェクトでの取り組むべき事項について上げる。

4.1　分散システムの研究者視点での、ブロックチェーンの安定性についての議論

先に、Bitcoinの10分というブロック生成時間とルーティングの安定性について簡単に述べたが、こういった現在または将来のインターネットが持つパラメータが、上位アプリケーション(この場合はブロックチェーン)に影響を与える可能性について、インターネットプロトコルのエキスパートとして、研究を進める必要がある。たとえば、ブロックチェーンを安定して運用するには、どのような下支えが必要であるかといった議論である。

4.2　分散システムへのブロックチェーン応用

Bitcoinにおける最後に接続するブロックを決定するため

のアルゴリズムは、Nakamoto Consensusと呼ばれるようになってきた。これはコンセンサスアルゴリズムでは無いという意見もあるが、この最終ブロックを決定するためのアルゴリズムには、以下に示す、いくつかの重要な特性がある:

・プロトコルの成立に対して、一方向通信で良いため、遅延による影響が限定的である
・参加できるノード数に制限がない

これらの特性は、過去に議論されてきた合意形成プロトコルでは重要な意味を持っている。たとえば、Hyperledger Fabricのように、非Proof-of-Work型のブロックチェーンにPBFT[66]が使われることが多々ある。PBFTは、参加ノード数に強い制限があり、かつ、遅延による影響を受けやすいという特性がある。筆者が耳にしている範囲では、十数台のノードを日本国内で分散した程度であっても、合意形成がうまくいかないことがあるとのことである。Proof-of-Workは、ムダに電力消費される点を含め、デメリットが複数ある。しかし、上記の特性に着目したときに、このプロトコルの可能性が感じられ、十分な研究をする価値があると考える。

4.3 Identity技術

先に繰り返しのべたように、Identity技術は、ブロックチェーンにとて極めて重要である。そして、いうまでもなく、インターネットサービス全般についても重要である。Sovrinなどのコンセプトも参考にしつつ、identity技術について研究を進めるのも重要である。