ブロックチェーンの安全性とその課題

松尾真一郎（まつお・しんいちろう）

MIT メディアラボ研究員 / 所長リエゾン（金融暗号）

1. はじめに

ブロックチェーン技術は，2008 年のサトシ・ナカモト（Satoshi Nakamoto）の論文で提案された暗号通貨ビットコイン（Bitcoin）で利用されている，暗号技術，P2P（Peer to Peer），分散コンピューティングにおける合意アルゴリズムなどを巧妙に組み合わせた技術である．その登場が暗号通貨という形であったために，フィンテック（Fintech）という文脈で語られることも多いが，様々な記録やトランザクションを中央集権的なサーバや運営者なしに処理することができる基盤として，2014 年以降大きな注目を集めている．

ビットコインが 8 年以上にわたり，基本的な部分における技術的欠陥から大きな事故を起こすことなく運営されていることから，実証的に確かめられた技術であり，その技術がビットコイン以外の様々な応用に適用できるようなイメージが持たれている．しかし，現実には，ビットコインで実証的に確認されている利用方法や利用環境と，ブロックチェーンの文脈で考えられている利用方法や利用環境には，当然ながら差異が存在する．本稿では，ブロックチェーンが担保すると期待されるセキュリティの面に焦点を絞り，その安全性についての 2017 年 3 月現在での現状と課題について述べる．なお，本稿においては，特に断りのない限りビットコインで提案されたようなパブリックブロックチェーンを議論の対象とする．

松尾真一郎
1972 年東京生まれ．シリコンバレー在住．博士（工学）．暗号技術の研究開発に従事．ブロックチェーンの国際学術研究ネットワーク BSafe.netowrk 共同設立者．学術専門誌 "LEDGER" エディタ，IEEE，ACM，W3C におけるブロックチェーン国際会議のプログラム委員を務める．ISO TC307（Blockchain）の日本 National Body 委員． 東京大学リサーチフェロー，慶應義塾大学特任教授を兼務．

2. ブロックチェーンに必要な安全性

ブロックチェーン技術では，不特定多数のネットワークノードに，同じ台帳のデータを分散管理をすることが基本である．その台帳のデータの更新方法は，個別のビジネスロジックで異なるが，ビットコインの場合は残高の管理と価値の移動などを取り扱うロジックが埋め込まれている．よく「分散台帳」という日本語がブロックチェーンの説明として使われるのは，このようなデータの管理方法に由来している．

ブロックチェーンは「分散」,「台帳」という二つの側面から，セキュリティに関する要件を紐解くことができる．まず基本的に「台帳」である必要がある．信頼できる台帳であるためには，台帳に載せられているデータは一貫していて，前後性が保証でき，誰でも検証ができて，後から改ざんできないように管理されている必要がある．この性質を実現するために，ビットコインをはじめとする現状のブロックチェーン技術では，電子署名技術とハッシュ関数によるチェーンの仕組みを利用している．

もう一つの「分散」という側面は，主にビットコインが目的としている非中央集権性と関係する．あるサーバが安定して運用され，サーバの中で改ざんや，システムの利用者の意図に反した処理のコントロールが発生しないのであれば，従来から実現されているデータセンターのバックアップなどを除けば，あえて分散させる必要はない．しかし，個人情報やクレジットカード番号の漏洩が頻繁に発生し，時にはそのようなサーバの運営者や事業者が故意に不正を行うこともあり，上述のような理想的な運用環境を実現することは難しい．そのため，(少数の)悪意を持った人がいたとしても全体として台帳が保たれるようにするために，台

帳のデータをあえて（多数の）複数のマシンに保管し，（同じ）ビジネスロジックの処理をなるべく多くの人で実行している．この性質を実現するために，ブロックチェーン技術ではデータを分散させるための P2P ネットワーク技術と，分散されたデータが同一であることを保証するための「分散合意アルゴリズム」が使われている．もし台帳のデータが分散していないのであれば，理論的には単一に保持されている台帳データに，ISO/IEC 18014-3（Time-stamping services - Part 3: Mechanisms producing linked tokens）で規定されている暗号学的タイムスタンプや，ヒステリシス署名と呼ばれる前後性を保証可能な電子署名技術を適用したものと変わらない．台帳データをわざわざ分散させることでシステムの処理性能は確実に落ちるため，分散させることで得られるメリットがない場合には，上記の既存の技術を使うべきである．つまり，ブロックチェーンを使うモチベーションとして，いかに分散にして非中央集権にするのか，というのは大きなポイントである．そのうえで，本来は中央のサーバが保っていたトラスト（信頼）を分散した状態でも保つことが，ブロックチェーンに課せられた安全性要件の一つになる．

ビットコインの場合，ネットワークの参加者のすべてに対して，個別のトランザクションのプライバシーを確保することは，その設計思想上重要な点になっている．一方で，より広い応用を考えたときの，ブロックチェーンを考えた場合，プライバシーの確保を行うことは必須の要件ではない．ただし，前述の通り非中央集権的な応用を考えるとき，プライバシーは検討すべき課題の一つであり，多くの場合オプションのセキュリティ要件と考えてよいだろう．

3. ブロックチェーンシステムの安全性に関する現状

ここでは，前節で述べたブロックチェーンの安全性について，どのように実現されているのか，あるいは実現のための課題があるのかを述べる．ブロックチェーンの安全性に関する解説の多くは，暗号技術が利用された部分が中心になることが多い．つまり，暗号学的ハッシュ関数（ISO/IEC JTC1 では 10118 にて標準化）で計算されたハッシュ値を連鎖させることでブロックの前後性を保証する部分，電子署名アルゴリズム（ISO/IEC JTC1 では 14888 にて標準化）で計算された電子署名データにおいて個別のトランザクションの非改ざんとトランザクションの

主体を証明する部分，そしてプルーフ・オブ・ワーク（Proof-of-work）のような暗号学的パズルと呼ばれる不正を防ぐために多くの計算力を必要とする部分である．このような暗号技術と通信を組み合わせて，様々な機能を実現する技術のことを暗号プロトコルと呼ぶが，暗号プロトコルが様々な攻撃に耐えて当初要求している安全性を保つかどうかを保証するのは実は簡単ではない．パブリックブロックチェーンにおいて，たとえばビットコインの暗号プロトコル全体について，安全性に関する数学的証明は存在しない．また，どの程度の攻撃の可能性が残っているかという学術的評価ができているわけではない．このことはビットコインが安全でないことを示すわけでもないが，未知の攻撃の可能性を現時点では否定できないということには注意すべきである．

また，一般的にある暗号技術は未来永劫，設計当時の安全性を保つわけではなく，ある年数を経ると安全性が低下する．これを暗号技術の危殆化と呼ぶ．暗号技術の危殆化が起こる原因としては，①人間が設計するアルゴリズムの中に弱点が発見されて，暗号の解読，電子署名の偽造，ハッシュのコリジョンなどの発見にかかる計算量が当初の見積もりよりも少なくなるという場合と，②ムーアの法則に代表されるように計算機の能力が向上し，解読に必要な計算量が同じであったとしてもその計算量を達成するまでの時間が短くなるという場合がある．過去には，共通鍵暗号 DES（Data Encryption Standard）の解読，ハッシュ関数 SHA（Secure Hash Algorithm）-1 のコリジョン発見，そして素因数分解が可能となる対象の数の拡大などがあり，標準となる暗号を新しいものに交換したり，公開鍵暗号の鍵サイズを増やしたりする対応が取られている．ブロックチェーンにおいても，この問題は当然発生する．ブロックチェーンに使われているハッシュ関数や電子署名アルゴリズムが危殆化した際に，どのように新しいアルゴリズムに更新するのか，その方法についてブロックチェーン技術ではまだ考慮されていない．ブロックチェーン技術が，今後の我々の生活の基盤として長期間使われるものを目指すのであるとすれば，この問題を解決する必要がある．

上記は，パブリックブロックチェーンのプロトコル仕様についての状況である．一方で，ブロックチェーンに限らず暗号技術を利用したシステムの安全性は，暗号プロトコル仕様の部分だけに依存するわけではない．現実の脆弱性や攻撃は，それ以外の部分で起こることも多い．その意味で，ブロックチェーンの「システム」に対する安全性を保つために必要なことを考える．上述した暗号アルゴリズ

ムの安全性は，世界中のアカデミアで長年研究がされていて，各種の技術標準を参照することが必要である．暗号プロトコルの部分については，今後の研究が必要である．

これに加えて，まずシステムの実装について考える必要がある．ブロックチェーンに関わる処理は，ソフトウェアあるいはハードウェアの形で実装される．しかし，この実装にバグがあることによって，暗号処理の安全性が損なわれたり，秘密に管理しなければいけない暗号鍵（ブロックチェーンでは電子署名を計算するための署名鍵）が漏洩することがある．暗号処理の実装の安全性をチェックする方法としては，ISO/IEC 15408 で規定されているコモンクライテリア（Common Criteria）という評価基準があり，Cryptographic Module Validation Program（CMVP：日本においては JCMVP）において認証する枠組みもある．

ブロックチェーンシステムにおける実装で，もう 1 点考えなければいけないのは，暗号以外の部分の実装だ．ブロックチェーンは，単に暗号の処理で非改ざんを保証するだけではなく，そのうえでビジネスロジックに基づく処理（トランザクション）を実行して，その結果をさらに非改ざん性を持って記録できる点が機能面で重要な点である．つまり，システムロジックの部分にバグや脆弱性があると，その問題がブロックチェーン上に残り続け，場合によってはそれが拡散していくことになる．2016 年に発生した The DAO 事件は，イーサリアム（Ethereum）のスマートコントラクトプラットフォームの上で，Distributed Autonomous Organization（DAO）のビジネスロジックを実行する部分の脆弱性から発生した．このように，ブロックチェーンを利用したシステムが持つビジネスロジックの部分の実装に脆弱性がないことは，システム全体の安全性で見た時に重要なポイントとなる．現在のブロックチェーンのシステムで，実装のセキュリティを保つためにどのようなチェックをすればよいかの基準は存在しない．前述のように，暗号実装に関しては既存の標準を参照することである程度安全性を確保できると見込まれるが，その他のレイヤも含めて，実装の安全性を確保するための基準を検討する必要がある．

もう 1 点，安全性について考える必要があるのは運用の部分だ．ブロックチェーンにかかわらず，セキュリティ上の事故や問題は，人間のオペレーションによって発生することが多い．この運用には暗号技術の肝である鍵（ビットコインの場合には署名鍵）の管理も含む．ブロックチェーン技術に用いられている電子署名

の署名鍵は，一般には数年単位の有効期間をもって更新することが通常の運用である．しかし，現状のブロックチェーン技術の実装では，このような鍵のライフサイクルを考慮した運用について十分に検討されているわけではない．

また，ブロックチェーン技術について注意が必要なのは，中央集権的なサーバが不要になるので管理コストが低下するというのは必ずしも成り立つわけではないという点である．ブロックチェーン技術の本質は，中央集権的なサーバが担ってきたシステムの信頼担保のための負担を，ブロックチェーンノード全体に分散して負担させるようにした，トラストモデルの変更である．このことはすなわち，各ノードに，システムを安全に担保させるための責任が薄く広く負わされているということと同義であり，各ノードを運営する人（場合によっては一般の人を含む）が，これまでクラウドサーバがやっていたように暗号鍵を厳重に管理したり，マルウェア，ウイルスなどに対する対策を十分にとったり，場合によってはサイバー攻撃対策をとらないといけない．ブロックチェーンはノードが分散しているから，マルウェアやサイバー攻撃に対しても堅牢である，という主張もあるが，現実にブロックチェーンの運用するソフトウェアは多くの場合単一の実装で，その環境にも多様性がないとすると，あるマルウェアが登場した時に，同時に多数の（51% を超える）ノードが脆弱になるというシナリオは十分に可能性があると言える．P2P ソフトウェアである Winny が普及した時に，「原田ウイルス」や「山田ウイルス」によって，一般のパソコンから秘密情報が漏洩する事件が多数発生したことを思い出せば，その重要性は理解できるだろう．その意味でノードの運用を厳密に行うというのは，ブロックチェーンにおいて，明示的に論じられることが少ない，隠れた責任とコストであることを認識する必要がある．

4. 今後のアカデミアの役割と研究課題

ビットコインやブロックチェーンは，主にデベロッパコミュニティで開発されてきた．一方で同じようにインフラのための技術であるインターネットは，大学の研究や実証実験を経て，25 年以上かけて技術を成熟させてきた．インターネットが商用化されたのは 1995 年であるが，その前には，全米科学財団（NSF：National Science Foundation）が中心となって構築した NSFNET と呼ばれる実証実験のためのネットワークがあり，そのネットワークが，インターネットの

技術のインフラとしての成熟度向上に大きな役割を果たした．BSD（Berkeley Software Distribution）のような，オープンソースによる「カイゼン的」な開発と，サイエンスによる慎重な検証がうまくマッチして，拙速にならずに必要な時間を掛けることができた成功例と言ってよいだろう．

一方でブロックチェーンは，2008 年のサトシ・ナカモト論文と，その参照実装の登場から，コミュニティを中心とした活動でソフトウェアが開発され，それに多くの投資がなされることで，アカデミアなどが参画することなく，実際のビジネスになりつつある．コミュニティによるオープンソフトウェア開発は前述の BSD 的なプロセスであるが，車の両輪のもう一方であるアカデミアによる検証がなされていない．そのため，コミュニティの中の技術仕様の議論も，科学的な議論よりも経済的な利害に基づいて行われることが多い．また，The DAO 事件のように脆弱性を含むソフトウェアが実働してしまうことで，50 ミリオンドル（約 55 億円）が流出する危険にさらされた．ブロックチェーンのスタートアップは多数登場しており，それぞれのスタートアップは「カイゼン」スタイルで日々ソフトウェアとサービスの開発を行っているが，過剰に投資されており，その投資に応えるために，未熟な技術でも新しいビジネスを始める圧力にさらされることは，ブロックチェーンの技術の建設的な成熟と評価を高めることにマイナスの面を持っている．その意味で，インターネットが過去に行ってきた研究と開発の両輪を回すエコシステムの構築が必要である．

アカデミアに課された，ブロックチェーンにおけるセキュリティ面での研究課題としては，暗号や暗号プロトコルのレイヤで，安全性がどこまで担保されていて，どのようなリスクが残っているのか，ということを明らかにすることと，安全な運用条件を示すことが必要だ．また，暗号以外の部分でも，たとえばスマートコントラクトで脆弱性の発生を減らすような開発の方法を提示するなどは，The DAO のような事件を起こさないためにも必須だ．現状のスマートコントラクトは，かなり自由度の高い言語になっているが，その自由度のために問題が発生する余地を残している．たとえば，個別のビジネスドメインに必要最低限の計算の計算モデルとそれを実現するだけのプログラミング言語（Domain Specific Language）を定義して，形式検証による安全性評価が容易になるような仕組みの研究が必要であると言える．

また，ブロックチェーンは，性能と安全性，非中央集権性など，多くのメリッ

トが，トレードオフの関係になっている．たとえば，性能を上げようとすると，非中央集権性が損なわれる．そのため，個別のアプリケーションに必要なトラストモデルと，そのトラストモデルに適した最適なチューニングを見つけることが，ブロックチェーンの良さを発揮するために重要なポイントとなる．このチューニングに関する知見は，応用研究として求められる点だ．

5. まとめ

本稿では，パブリックブロックチェーンが本来持つメリットを振り返りながら，ブロックチェーンに求められる安全性に焦点を当てて，何が必要とされて，現状のブロックチェーン技術では何ができないのか，その課題までを述べた．本稿にあるように，ブロックチェーン技術は，ビットコインに代表されるように華々しいプレゼンテーションはされているが，社会基盤になるにはまだ未熟で実力不足だ．筆者はパブリックブロックチェーンが，社会や市民の生活の体験に新しいイノベーションをもたらすための重要な基盤だと信じているが，その基盤を構築するために，インターネットが商用化まで 25 年以上かけたように，着実に成熟する必要があるのも事実だ．その点で，この分野の研究と，開発者との協力が進むことを願っている．