［ブロックチェーン技術の最新動向］

③ ブロックチェーンの安全性 ―攻撃や脆弱性とその対策―

松尾真一郎 ジョージタウン大学

ブロックチェーンのセキュリティを再考する

2008 年の Satoshi Nakamoto が公開した Bitcoin の登場は，電子的な送金を信頼できる第三者によらずに実現するプロトコルを提示した．そして，Bitcoin のコア技術である，不特定多数の利用者による台帳の安全な更新と管理を実現する技術を取り出して，ブロックチェーン技術と名付けて扱われるようになった．ブロックチェーン技術が，それまでの技術に比べて新しいのは，台帳の更新が（参加や脱退がいつでも認められる）不特定多数の参加者によってのみ行われる点と，台帳の更新に際して，プログラムによる多様なロジックを組み込むことが可能になっているという点である．

一方で，ブロックチェーンが「これまでにないセキュリティ」を提供するような議論を目にすることも少なくないが，一般論としてセキュリティの向上は，性能や使い勝手などの何かの犠牲によって成り立つものである．また，すべての面においてセキュリティを担保したり，ゼロリスクにするということは，現実的にはほぼ不可能である．本稿では，この視点に基づきブロックチェーン技術がもたらす安全性の範囲（セキュリティ目標），ブロックチェーンのセキュリティに関する理論的な議論の現状，現在指摘されている脅威と脆弱性，そしてセキュリティ向上に向けた研究開発の方向性について述べる．

ブロックチェーンにかかわるセキュリティの全体像

ブロックチェーンのセキュリティ目標（Security Objectives）

ブロックチェーン技術に関する議論は，かなり幅広い応用を見据えたものになりがちであるが，最も本質的に提供する機能は，「不特定多数の参加者が管理する共通の帳簿が存在し，その帳簿を一定のロジック（たとえば Bitcoin のような支払いでは，支払い者の残高を減少させ，受領者の残高を同額だけ増額させるという足し算と引き算）に基づいて，事象の発生順序を保証しながら更新していく．攻撃者が一度合意した更新を覆す可能性は無視できるほど小さい」という点にある．これがブロックチェーンの必須のセキュリティ目標であり，それ以外のセキュリティ目標は，すべてオプションであることに注意が必要である．たとえば，トランザクションにおけるプライバシ保護や，アプリケーションレベルでの利用者認証や処理の整合性は，ブロックチェーン技術を利用したアプリケーション固有の追加的なセキュリティ目標である．

ブロックチェーンのセキュリティ確保のためのレイヤ

一般に，あるセキュリティ目標を達成するには，基盤的な暗号技術，その組合せ，実装，そして運用にいたる異なるレイヤにおいて，適切な検討がなされることが必須である．あるレイヤで正しく構築された技術は，ほかのレイヤの技術が正しく使ってく

れることを暗黙のうちに仮定しているが，その仮定に反した使われ方をされることがある．たとえば，仮に安全な暗号技術を使っていても，暗号鍵の運用が杜撰であればその効果は無になる．2018 年から 2019 年にかけて発生した，取引所のセキュリティインシデントは，杜撰な暗号鍵の運用に起因している．この例にもあるように，安全なブロックチェーンの設計，実装，そして，運用のために，すべてのレイヤで正しい技術の利用や運用を行う必要がある．

ブロックチェーン技術と，それを利用したアプリケーションにおいては，おおむね図 -1 のような 6 つのセキュリティに関係するレイヤが存在する．下から順番に説明する．1 番下にあるのが，基盤的な暗号アルゴリズムと呼ばれる技術で，ブロックチェーンにおいては SHA-2 などのハッシュ関数や ECDSA[☆1] などの電子署名技術がそれに当たる．これらの技術は，日本においては電子政府推奨暗号リストを作成する CRYPTREC[☆2] において評価され，ISO/IEC JTC 1 SC 27 などで標準化が行われている．続くバックボーンプロトコルは，ブロックチェーン技術の根幹プロトコルの部分である．P2P ネットワークや，合意プロトコルがセキュアであるかどうかを確かめる必要がある．3 番目のレイヤは，よりアプリケーションに近いセキュリティ目標を実現するためのレイヤで，プライバシ保護やトランザクション自体が安全に処理されることを確認する必要がある．4 番目のレイヤは支払いや契約などの応用的なロジックを安全に実行するためのレイヤで，Bitcoin や Ethereum などに実装されているスクリプト言語の安全性に関係する．5 番目のレイヤは，安全な実装に関するもので，ブロックチェーン技術とそのアプリケーションを実装するソフトウェアコードや，暗号鍵を守りながら暗号処理を行うハードウェアなどの安全性を確認するレイヤである．そして最後のレイヤは，鍵管理，監査などを行う運用のレイヤである．それぞれ，ISO/IEC などで，標準的な技術や運用手法が定められており，ブロックチェーンにおいてもこれらの標準への適合を確認する必要がある．

☆1 楕円曲線暗号に基づく電子署名アルゴリズム．ISO 標準になっている．
☆2 総務省と経済産業省による，電子政府推奨暗号リストなどを作成する委員会．

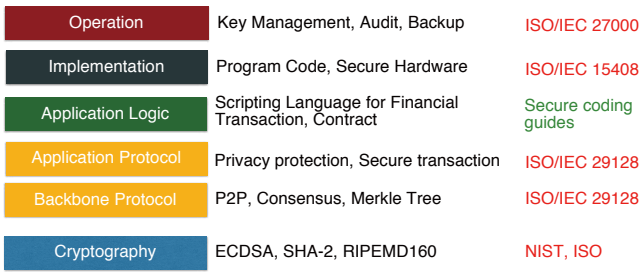

図 -1　ブロックチェーンにおけるセキュリティのレイヤ

ブロックチェーンの基盤技術に関する理論的な議論

本章では，ブロックチェーンの必須のセキュリティ目標の部分（前述の 2 番目のレイヤ）の安全性について，現在のアカデミアの議論を述べる．

2015 年の Eurocrypt[☆3] において，J. Garay らは，Bitcoin で提案された Proof-of-Work を利用した合意アルゴリズム（Nakamoto Consensus）について，セキュリティ目標に繋がる 2 つの性質 Common Prefix と Chain Quality を定式化した[1]．Common Prefix とは，Honest な（プロトコルに従う）参加者の任意の 2 者のペアは，ある一定ラウンド以前の共通のチェーンを共有しているという性質であり，Chain Quality は，Honest な参加者が作成し合意するブロックの比率が，Dishonest な（プロトコルに従わない）参加者のブロックに比べて十分に取れている性質を表している．また同論文では，台帳に必要な性質として Persistence と Liveness を定式化している．Persistence は，あるトランザクションが承認されて以降，ある 1 人の Honest の参加者が所持するブロックの中で，一定ブロック経過した後には，合意が覆ることがない性質である．

Liveness は Honest なアカウントホルダが作成した

☆3 IACR（International Associaltion of Cryptologic Research）主催の暗号学におけるトップカンファレンスの 1 つ

トランザクションは一定のブロックが作成された後にHonestな参加者に承認される性質である．そのため，攻撃者によるDenial of Service攻撃ができないという性質である．この定式化に従い，同論文では，Nakamoto Consensusが，攻撃者のハッシュパワーが全体の1/2以下である場合に，すべての通信の同期が取れているという強い前提のもとに，上記の性質を満たしていることを証明した．この定式化の後，R. Passらは，Eurocrypt 2015の結果を拡張して，台帳に必要な新たな性質としてChain Growthを定義した．これは，Honestな参加者の間では，合意され共有されるブロックが一定数続いていくという性質である．その上で，同期性に関する制約を少し緩め，通信遅延の上限が設定される範囲において，Bitcoinがこの性質を満たすことを示している[2]．現在のブロックチェーンの安全性証明は，基本的にはこの定式化のもとに議論されている．一方で，Bitcoinの合意アルゴリズムについて，同期性に関する仮定を含めた現実を捉えた議論はまだ途中であり，今後の研究の進展も必要である．

上記の議論は，純粋にハッシュパワーやノードの数に依存した安全性の定式化であるが，ブロックチェーンが安全に保たれ続けるためには，Dishonestなノードのハッシュパワーを上回るHonestなノードが常に必要であり，これを維持するためにマイニングによる報酬の付与がシステムに組み込まれている．この報酬に応じてノードを維持するかどうかは，経済学的な合理性の分析が必要であり，ゲーム理論的解析の要素が入ってくる．現在の安全性の定義では，この点を捉えることはできていないため，現在の大きな研究テーマの1つとなっている．

ブロックチェーンの脅威や脆弱性の現状

ブロックチェーンプロトコルに関する一般的な脅威と脆弱性

ブロックチェーンの根幹である合意アルゴリズムにおいて，最も一般的に知られているのは51% Attackである．これは攻撃者が全体のハッシュパワーの50%を超えるハッシュパワーを有するとき，新たに作られるブロックの内容を自由にコントロールできるようになるため，過去のトランザクションデータを用いてDouble Spending（二重支払い）を成功させることができる．もしくは，新たなブロックに何もトランザクションを入れないというDenial of Service攻撃を行い，暗号資産自体を無効化することもできる．一方で，前述の通り，マイニング報酬を与えることにより，結託しない数多くの参加者がネットワークに参加するインセンティブがある．現状では，少数のマイニングプールのハッシュパワーを足すと51%攻撃は可能となるが，Bitcoinにおいては現時点では発生していない．一方で，十分なハッシュパワーを得られていない暗号資産では，この攻撃が発生している例がある．

そのほかに二重支払いを引き起こす可能性がある攻撃の例として以下のようなものがある

— Finney Attack：まず，支払い者が自分でマイニングしたコインを自分へ支払い，そのトランザクションが入ったブロックを作成し，ほかのネットワーク参加者に送信せずおいておく．次に，そのコインを商店への支払いに使う．商店がトランザクションの承認前に商品を発送したのを確認した後に，元の自己支払いのトランザクションデータをブロックチェーン上で承認する．トランザクションの承認までの期間が短い場合には，この攻撃の成功の確率が高まる．

— Brute Force Attack：十分なハッシュパワーを持つ攻撃者があらかじめ2つのチェーンを事前にマイニングして用意しておく．長いチェーンには自分がコントロールするノードへの送金，短いチェーンには同じ資金の商店への支払いを記録しておく．短いチェーンで商店への支払いを終わり，確定されるまで十分な時間が経過した後に，長い方のチェーンを送信し，商店への支払いを上書きする．

そのほかに，ブロックチェーンのプロトコル実行における攻撃の例として以下のようなものがある．

— Selfish Mining Attack：あらかじめ長いブロックのチェーンをマイニングしておき，そのブロックを隠し持っておいて，のちに公開することで，一度合意したチェーンを覆す攻撃．この攻撃が存在することで，正しいと思っていたマイニングをするユーザのマイニングパワーが無駄になり，正しいマイニングを個別に行うインセンティブが低下する．

— Sybil Attacks：攻撃者がたくさんの利用者のコピーを作り出し，合意において有利な立場を得ようとする攻撃．Proof-of-Work や Proof-of-Stake は，この攻撃の可能性を減らすための仕組みであるが，確率が完全に 0 になるわけではない．

暗号技術の危殆化と量子計算機

安全性と処理性能を同時に追求する現代暗号において，ある暗号アルゴリズムが永久に安全であるという仮定を置くことはできない．多くの場合，計算機の処理能力の向上に従い，暗号技術を破るために必要な時間が減少して攻撃の成功が現実的になったり，そもそものアルゴリズムの設計自体にミスがあり，期待していた安全性が担保できないケースがある．過去にも，米国連邦政府標準暗号であった DES：Data Encryption Standard や，やはり米国連邦政府標準ハッシュ関数である SHA-1 にはアルゴリズム上の脆弱性が発見され，それぞれ AES：Advanced Encryption Standard，SHA-2[☆4] と新しいアルゴリズムへの切り替えがなされている．同様に，暗号技術の安全性のパラメータである鍵データのサイズ（鍵長）は，攻撃者の計算能力に応じて設定する必要がある．現在，RSA[☆5] などの電子署名アルゴリズムでは 2048 ビット（楕円曲線を利用した ECDSA のような電子署名アルゴリズムでは 224 ビット相当）の鍵を使うことが推奨されているが，計算機能力がこれからも向上することを想定すると，いずれ鍵長を伸ばす必要がある．

上記のように，暗号技術が期待していた安全性を保てなくなることを危殆化（きたいか）と呼ぶ．暗号技術の危殆化が発生した場合，取る方法は 2 つある．計算機の能力が向上してその時点での鍵長が不足した場合には，公開鍵暗号や電子署名アルゴリズムであれば，より大きなサイズの鍵に変更して，同じアルゴリズムを使うことが可能だ．しかし，アルゴリズムそのものに脆弱性が発見された場合，さらに共通鍵暗号やハッシュ関数で鍵長やハッシュ値のサイズが不足する場合，アルゴリズムそのものを変更しなくてはいけない．

ブロックチェーンにおいて，暗号技術の危殆化が発生した場合，どういう問題が起きるのだろうか．たとえば電子署名の偽造が簡単にできるようになれば，過去のトランザクションを人が作成したかどうかの見分けがつかなくなる．ハッシュ値のコリジョン（複数の別の値のハッシュ値が同一になること）が見つかれば，一度合意したブロックからほかのブロックへの合意を覆すことができる可能性が増す．それでは，ブロックチェーンにおいて，暗号技術に危殆化が見つかった場合，新しい暗号技術に移行することはできるのだろうか．答えは，そんなに簡単ではない．それはブロックチェーンに格納する新しいデータに適用する暗号アルゴリズムを変更するだけでなく，ブロックチェーンの検証に必要な過去のデータの有効性を延長しなくてはならないからだ．筆者らは，電子署名と証明書の有効期間を延長する技術である長期署名の技術を用いて，ブロックチェーンの有効性を延長する技術を提案している[3]．過去の例では，標準的な暗号アルゴリズムでも，その発明から 20 年から 30 年で危殆化が発生している．ブロックチェーン上の帳簿のデータは長期間，あるいは永久に安全性を保つ必要があり，一方で暗号技術には危殆化のリスクが常に存在することから，危殆化が発生した際のより安全な暗号への移行スキームと運用についての研究が，さらに求められる．

☆4 2001 年に制定された米国標準ハッシュ関数．
☆5 RIvest Shamir，Adleman によって提案された公開鍵暗号方式．

暗号技術の危殆化に関する，もう1つ大きな懸念は量子計算機の発展だ．汎用的な量子計算機の上で1994年に発表されたShorのアルゴリズムを用いると標準的な公開鍵暗号の基盤となっている素因数分解問題や離散対数問題がより効率的に解けることが知られている．また，1996年に発表されたGroverのアルゴリズム，1997年に発表されたSimonのアルゴリズムによって共通鍵暗号の解読における探索を効率化することで知られている．一方で，現在のところ，ハッシュ関数の衝突困難性，第二原像困難性，一方向性をより効率的に破るアルゴリズムは知られていない．本稿では，汎用的な量子計算機の実現性や，暗号技術の解読に至るまでの期間についての議論は行わないが，中長期的には，汎用的な量子計算機の存在がブロックチェーンのセキュリティに影響する可能性が存在する．現在，汎用的な量子計算機が存在したとしても安全性が保たれる暗号技術（耐量子計算機暗号）の研究が進んでいるが，耐量子計算機暗号は暗号鍵のサイズや，電子署名のサイズが非常に大きくなることが知られており，現状ではブロックチェーンに応用することはできない．将来的には，耐量子計算機暗号とブロックチェーンへの適用の理論的研究が必要と考えられる．

ネットワークレイヤに起因する脆弱性

言うまでもなく，ブロックチェーン技術は，足回りのグローバルなインターネットが正しく機能していることが大前提である．そのため，ブロックチェーンのプロトコルは，インターネットに対する攻撃が行われたときにでも正しく動作するかは保証の限りではない．その例として2017年のIEEE Security and Privacyで，Maria Apostolakiらが，BGPプロトコル（インターネットのルーティングに用いられる基本プロトコル）に対する攻撃を利用することで，ブロックチェーンのブロックデータの伝達を妨害する攻撃を発表している[4]．このような研究は，本稿で示した，参加者間の同期に関する前提に対する攻撃の一種と見なすこともできる．

実装攻撃

冒頭に述べたセキュリティのレイヤの中で，プロトコル以外に注目する必要があるのが，実装面での脆弱性である．ここでの実装は，ソフトウェア実装，ハードウェア実装の両方である．すでに，Bitcoin，その他のブロックチェーンにおいて，脆弱性情報がCVE[☆6]レコードとして脆弱性データベースにも数多く登録されている．また，一般のユーザの署名鍵を安全に管理するために，ハードウェアウォレットが開発され，一部利用されている．ただし，安全であることを謳っているハードウェアウォレットであっても，実際にサイドチャネル攻撃などの実装攻撃で，署名鍵が取り出せるケースが報告されている．

セキュリティ向上に向けて

取引所セキュリティの強化について

ブロックチェーンに関するセキュリティに関して，一般に大きく懸念されているのは，暗号資産を取り扱う取引所（交換所）が攻撃されて，暗号資産が流出する事件が多発していることだろう．元々のBitcoinの論文には，取引所自体の存在が仮定されておらず，すべての参加者が自身の署名鍵を自らの責任で漏洩しないように管理することが暗黙の要求事項になっている．しかし，一般の利用者が，正しく署名鍵を管理することが簡単ではなく，また円やドルなどの一般的な通貨との交換も簡単ではないことから，署名鍵を預かりつつ，暗号資産と一般的な通貨の交換を行う取引所が利用されるようになった．本来のブロックチェーンは，51%のマイニングパワーを持つ攻撃者がいない限り安全であることを目指して設計されており，何らかのプロトコル参加者が故障したとしても問題なく動作することが特徴だ．しかし，取引所はいわゆる単一障害点になり得る．2018年以降多発している取引所からの暗号資産の流出は，これらの単一障害点を

☆6 Common Vulnerabilities and Exposures：個々の脆弱性情報につけられる識別子．

守ることが難しいことを示している．

現在の取引所のシステムには，安全なモデル実装が用意されておらず，取引所ごとにバラバラに設計と実装がされている．また，安全なシステムの設計ノウハウを持たない事業者がサービスを行っているケースもある．そのため，取引所のセキュリティ強化は，ブロックチェーンシステム全体の安全性を確保し，利用者に広く安心して利用できるようにするために必須である．セキュリティ専門家も加わっている CGTF（Croptoasset Governance Task Force）では，取引所のシステムを情報セキュリティマネジメントシステム：ISMS の手法を用いてリスク分析し，Security Control を検討するためのサポート文書を作成している [5]．

スマートコントラクトと形式検証

2016 年に発生した The DAO 事件では，Ethereum 上に構築したスマートコントラクトを実行するソフトウェアにおいて，再帰呼び出しを行う際のトランザクションのロックの処理に不備があり，暗号資産が自動的に流出する事象が発生した．Bitcoin のような単純な支払いのロジックではなく，より高度なビジネスロジックのためのプログラムを構築する際に，バグの発生がブロックチェーンのレイヤの問題を引き起こす可能性がある．このような事象を防ぐために，スマートコントラクトのバグの可能性を減らす手段として，形式検証を行うための研究が進められている．この研究には，大きく 2 つの方向性があり，スマートコントラクトのコードを形式検証し，セキュリティの問題が発生するトレースが存在しないことを示す方法と，形式検証可能な範囲にスマートコントラクトの言語を制限する方向である．

TEE（Trusted Execution Environment）

CPU 上に，秘密情報を用いる演算を行う独立した領域を用意し，秘密情報を保持する仕組みである TEE（Trusted Execution Environment）の利用は，ブロックチェーンにおける暗号鍵を利用した処理のセキュア化と，Zk-SNARK などのブロックチェーンのプライバシ保護のための暗号処理の実現，そしてスケーラビリティ確保の意味で，広く注目されており，関連論文も多く発表されている．TEE 自体のセキュリティについては，まだ未熟な点もあるが，セキュリティとスケーラビリティの両方を向上する手段として，TEE の活用は有望な方向性の 1 つであり，今後の研究の発展が期待される．

今後の研究課題

本稿では，ブロックチェーンにまつわるセキュリティの全体像を俯瞰し，ブロックチェーン自体とそのアプリケーションを構築する際に留意すべきセキュリティのレイヤ，現時点で明らかになっているセキュリティ上の問題，そしてセキュリティ向上のための検討の方向性を示した．ブロックチェーンにおけるセキュリティの定式化，およびセキュリティに関する依存関係の解析はまだ道半ばであり，引き続き研究が必要な状況である．

参考文献

1) Garay, J., Kiayias, A. and Leonardos, N. : The Bitcoin Backbone Protocol : Analysis and Applications, In : Oswald, E. and Fischlin, M. (eds), Advances in Cryptology - EUROCRYPT 2015, EUROCRYPT 2015. Lecture Notes in Computer Science, Vol.9057, Springer, Berlin, Heidelberg (2015).
2) Pass, R., Seeman, L. and Shelat, A. : Analysis of the Blockchain Protocol in Asynchronous Networks, In : Coron, JS., Nielsen, J. (eds), Advances in Cryptology - EUROCRYPT 2017, EUROCRYPT 2017, Lecture Notes in Computer Science, Vol.10211, Springer, Cham (2017).
3) Sato, M. and Matsuo, S. : Long-Term Public Blockchain : Resilience Against Compromise of Underlying Cryptography, 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, pp.1-8 (2017).
4) Apostolaki, M., Zohar, A. and Vanbever, L. : Hijacking Bitcoin : Routing Attacks on Cryptocurrencies, 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, pp.375-392 (2017).
5) Sato, M., Shimaoka, M. and Nakajima, H. : General Security Considerations for Cryptoassets Custodians, draft-vcgtf-crypto-assets-security-considerations-03 (work in progress) (Jan. 2019).

(2019 年 10 月 22 日受付)

松尾真一郎　shinichiro.matsuo@georgetown.edu
ジョージタウン大学 Department of Computer Science 研究教授．CyberSMART 研究センターでブロックチェーン研究ディレクターを務める．国際学術研究ネットワーク BSafe.network 共同創業者．