IMES DISCUSSION PAPER SERIES

暗号資産とブロックチェーンの安全性の現状と課題

まつ お しんいちろう
松尾真一郎

Discussion Paper No. 2020-J-8

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2020-J-8
2020 年 6 月

暗号資産とブロックチェーンの安全性の現状と課題

松尾真一郎（まつお しんいちろう）*

要　　旨

2008 年のビットコインの論文の中心的な技術としてブロックチェーン技術が広く注目を集めている。ブロックチェーン技術にはセキュリティの向上の観点で大きな期待が寄せられている一方で、この技術が提供できるセキュリティの範囲については、研究が始まってまだそれほど経過しておらず、十分には解明されていない。本稿では、ブロックチェーンやそれを応用した暗号資産にまつわる安全性の現状と課題を考察する。まず、現時点で指摘されている攻撃とインシデントの実例をサーベイした上で、ブロックチェーン技術が提供するセキュリティの目標を学術的観点から整理する。そして、ブロックチェーンとそれを応用したシステムのセキュリティ設計を考えるためのレイヤーについて述べ、各レイヤーにおける主な研究課題を説明する。

キーワード：暗号資産、セキュリティ、ビットコイン、ブロックチェーン

JEL classification: L86、L96、Z00

*　ジョージタウン大学（E-mail: Shinichiro.Matsuo@georgetown.edu）

本稿は、筆者が日本銀行金融研究所客員研究員の期間に行った研究をまとめたものである。本稿の作成に当たっては、佐藤雅史主任研究員（セコム株式会社 IS 研究所）から有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　　次

１．はじめに

（１）背景

2008 年に Satoshi Nakamoto がビットコインに関するピアレビューを経ていない論文をサイファーパンクのメーリングリストに投稿し、その後 2009 年に実装が公開されビットコインの運用が始まった。ビットコインと、その基盤技術であるブロックチェーン技術は、不特定多数の分散ノードで台帳を管理する技術として広く注目を集めている。ブロックチェーン技術については、情報セキュリティにおける様々な機能の実現が広く期待されている一方で、ブロックチェーン技術が実現しようとしているセキュリティの性質とそのレベル（セキュリティ目標）と、現実のブロックチェーンが達成しているセキュリティ目標について、その知見が十分に共有されているとは言えない。むしろ、それらの情報について誤った理解のもとに、ブロックチェーン技術を用いた情報システムが構築されて、運用されているケースも存在する。暗号資産の交換所や取引所で発生するインシデントは、そのような誤解が原因になっていると言える。

ビットコイン、およびブロックチェーンにおいて、セキュリティ目標を定式化する試み、およびセキュリティの評価を行うためのフレームワークを作る試みについては、2015 年以降、様々な研究成果が発表されるようになっている。一方で、ブロックチェーン技術の安全性は、ベースとなる暗号技術の安全性にのみ基づいているわけではなく、P2P（peer-to-peer）ネットワーク、分散合意アルゴリズム、インセンティブ設計やゲーム理論など、異なる要因が組み合わさって実現されている。ブロックチェーン技術の安全性を理論的に評価するためには、それらの複数の要因を加味したフレームワークが必要である。しかし、このような理論的フレームワークを構築するのは困難であり、本稿の執筆時点（2020 年 3 月末）で合意されたモデルは存在しない。さらに、ブロックチェーン技術のセキュリティ、スケーラビリティ、プライバシなどの性質はトレードオフの関係にあるが、このトレードオフの関係性についても定性的、定量的な分析の結果が存在するわけではない。これらの理論的フレームワークは、個別のブロックチェーン技術や暗号資産を取り扱うシステムのセキュリティが十分であるかを判断するために必要である。

本稿では、暗号資産を取り扱うシステムと、基盤となるブロックチェーン技術について、必要とされるセキュリティの性質について分析を行い、それぞれの性質の安全性評価モデルや安全性評価の研究結果をまとめ、より包括的な安全性評価のための理論的フレームワークの構築に向けた課題を整理する。

（２）本稿のスコープ

「ブロックチェーン」という言葉は技術用語であるとともに、ビジネス用語や

マーケティング用語としても使われることがあり、ブロックチェーンについての統一的な定義や、その言葉が指し示す範囲についての合意は、本稿の執筆時点では存在しない。例えば、ビットコインのように、不特定多数のノードがいつでもネットワークに参加したり、ネットワークから脱退したりすることができるようなタイプのブロックチェーンを、パブリック・ブロックチェーンと呼んだり、パーミッションレス・ブロックチェーンと呼んだりすることがある。これに対して、単一の事業者であったり、決められた事業者が運営するノードのみでネットワークを構成したりする場合をプライベート・ブロックチェーンと呼び、複数の合意された事業者の間でネットワークを維持する場合をコンソーシアム・ブロックチェーンと呼ぶこともある。また、パーミッションレス・ブロックチェーンの反対語として、ブロックチェーンのネットワークに参画するために許可が必要な場合を、パーミッションド・ブロックチェーンと呼ぶこともある。

これらの分類は、技術的な側面がある一方で、ビジネスモデルによる分類にもなっており、ここに挙げたタイプのブロックチェーンは、技術的なセキュリティの要件について学術的な分析を行うためのモデルが構築されているわけではない。

上記の異なる呼び方のブロックチェーンには、共通部分として、そのデータ構造（一定時間のトランザクションをブロックの形でまとめて、ハッシュ関数の連鎖で順序性に対する検証可能性を与えるもの）が存在する。ただし、このデータ構造は、1990 年の Haber と Stornetta による暗号学的タイムスタンプ・プロトコルにより提案されたものである（Haber and Stornetta [1991]）。このプロトコルでは、タイムスタンプの作成と付与は、信頼できるタイムスタンプ局によって行われるモデルになっている。

一方で、2008 年のビットコインの論文の革新的な発明のうちの 1 つは、ブロックチェーン・ネットワークを構成するノードのうち、決定能力（ビットコインの場合はハッシュパワー）の過半数が正直にプロトコルを実行している限りにおいて、個別のノードを信頼しなくても良く、タイムスタンプ局の運営への信頼のモデルを緩和したことにある。つまり、個別のノードは、信頼できる第三者機関である必要はない。先に述べたブロックチェーンの分類のうち、プライベート・ブロックチェーンやコンソーシアム・ブロックチェーンでは、ネットワーク内のノードが信頼できるノードであることが仮定されており、信頼モデルの観点ではタイムスタンプ局を冗長化したものに近い。このような信頼モデルでは、セキュリティ上の問題の多くはノードの信頼に帰着させることができ、その問題は既知のものがほとんどである。一方で、（パブリック）ブロックチェーンでは、新しい信頼モデルのもとでトランザクション処理が行われるため、新たなセキュリティ上の研究課題が生じている。そのため、本稿のような研究が必要とさ

れ、世界中で盛んに研究が行われている。

本稿では、ビットコインやイーサリアム（Ethereum） のような、いわゆるパブリック・ブロックチェーンを対象として、これまでにないセキュリティ上の課題がどこに存在し、今後のセキュリティのアーキテクチャ設計と実装のための研究がどこにおいて必要かという領域にフォーカスする。パブリック・ブロックチェーンを応用するシステムとしては、支払い（payment）、暗号資産、そしてスマートコントラクトの 3 つを対象にする。

２．ブロックチェーン技術の概要

ブロックチェーン技術は、2008 年のビットコインの論文（Nakamoto [2008]）で用いられた、分散環境で台帳を管理するためのプロトコルである。Nakamoto [2008]では、ビットコインを実現する技術について以下のように記述している。

・同意している二者が、信頼できる第三者を必要とせずに直接取引が可能な、信頼（トラスト）の代わりに暗号的証明に依拠する電子支払システム
・分散された P2P のタイムスタンプ・サーバを使って、トランザクションの時間的順序の計算機的証明

ビットコインでは、全ての利用者の残高に矛盾なく電子的な支払いを実行するために、全てのトランザクションを記録する共通の台帳を用意する。台帳が不整合のないトランザクションの履歴として維持されるためには、全てのトランザクションが前後関係を失うことなく正しく記録され、記録された後に改ざんされていないことが必要である。これが「トランザクションの時間的順序の計算機的証明」に相当する。

この性質を満たすために、1990 年に Haber と Stornetta によって提案された暗号学的タイムスタンプ・プロトコルのテクニックを使っている。具体的には、ビットコインの場合はおおよそ 10 分ごとに支払いのトランザクションをひとまとめにする（これを「ブロック」と呼ぶ）。このブロックのデータ全体に対して、暗号学的ハッシュ関数を用いてハッシュ値を計算する。このハッシュ値を次のブロックの中に埋め込む。このようにして、前後のブロックの間でハッシュ値を入れ子構造の形で繋げる（チェーン）ことで、事後のブロックやトランザクションの入替えへの対策となり、前後関係を証明することができる。ここまでは、暗号学的タイムスタンプを用いて台帳を作るための技術である。

また、ビットコインでは、支払元や支払先を識別する必要があり、個々の支払いのトランザクションに ECDSA を利用した電子署名が付与される。

そして、ビットコインにおいて重要なのは、「信頼できる第三者を必要とせず」

の部分である。このために最初に用いられるのが、「分散された P2P のタイムスタンプ・サーバ」である。つまり、（前述の暗号学的タイムスタンプで仮定している）信頼できるタイムスタンプ・サーバの存在なしに実現することが、ビットコインの新しいところである。これを実現するために、ビットコインでは、台帳の全ての情報（全てのブロックの情報）を、不特定多数のサーバで同期しながら複製を保持する。この場合、個別のサーバが正直（honest）なサーバなのか、悪意を持ったサーバなのかをあらかじめ判別することができないため、正直にプロトコルに従ったサーバに対して報酬を与えることにして、サーバに正しく行動するインセンティブを与える。このような報酬を与える仕組みのことを「マイニング」と呼んでいる。

本稿の執筆時点では、ビットコインにおいては、Proof-of-Work というプロトコル（ゲーム）に最初に勝ったマイニングを実行するノードの運営者に対して、12.5 BTC（約 1,000 万円）が付与される。そして、マイニングを実行する正直なノードが作ったブロックデータが、全てのノードに伝搬され、ノード間で同じ台帳のデータが共有され続ける仕組みとなっている。技術的には、暗号技術、タイムスタンプ技術、P2P ネットワークの技術が底流にあり、その上で、正直な計算をするノードのハッシュパワーが過半数に達することを保証するために、分散合意アルゴリズムとマイニングの仕組みが動作している。

３．ブロックチェーンと暗号資産を巡る攻撃とインシデント

（１）既存の攻撃や脆弱性の実例

イ．暗号資産取引所におけるインシデント

本稿執筆時点の、過去に発生した暗号資産に関する主なインシデントの一覧を図表 1 に示す。これらのインシデントの多くでは、暗号資産取引所が攻撃を受け、そのシステムの内部にあるウォレット（暗号資産のアドレスに対応する署名鍵を保管しているデバイスやストレージ）に保管された電子署名用の署名鍵が漏洩し、その署名鍵によって、攻撃者（あるいは攻撃者が結託している第三者）のアドレスへの支払いの取引が行われている。ここでのアドレスとは、鍵データから導出される識別子を指す。

ビットコインのオリジナルの考え方では、ビットコイン・アドレスに対応した ECDSA の署名鍵は、ビットコインの利用者が責任をもって管理することが前提になっている。しかし、一般的な利用者が署名鍵の管理を適切に行うことは容易ではない。そのため、暗号資産取引所は利用者の署名鍵を預かり、利用者によるビットコインの取引を代行することがある。この結果、暗号資産取引所には多数の署名鍵が保管されることになる。署名鍵の情報が、暗号資産取引所に対する攻撃で盗まれると、大量の暗号資産の流出につながる。また、一度、

図表１　暗号資産取引所における主なインシデント

取引所名	発生時期	損失額（発生時）	インシデントの概要
Mybitcoins	July 29, 2011	27,000 BTC ($ 370,000)	消失
Linode	March 2012	46,703 BTC ($ 200,000)	サーバへの侵入
Bitcoinica	March and May 2012	61,000 BTC	サーバへの侵入
Bitfloor	September 2012	24,000 BTC ($ 250,000)	サーバへの侵入
Mt.Gox	February 2014	850,000 BTC ($ 473,000)	トランザクション展性 サーバへの侵入
Bitstamp	January 2015	19,000 BTC	サーバへの侵入
Cryptsy Exchange	July 2016	11,325 BTC	サーバへの侵入
Bitfinex	August 2016	119,756 BTC	サーバへの侵入
Gatecoin	2016	250 BTC 185,000 ETC	サーバへの侵入
NiceHash	December 2017	4,700 BTC	サーバへの侵入
CoinCheck	January 2018	$ 580,000,000	標的型攻撃
BitHumb	June 2018	$ 30,000,000	サーバへの侵入
Monappy	September 2018	$140,000	サーバへの侵入
Zaif	September 2018	$ 50,000,000	サーバへの侵入
Binance	May 2019	$ 40,000,000	サーバへの侵入
Bitpoint	July 2019	$ 32,000,000	サーバへの侵入

（備考）・BTC、ETC は、それぞれ、ビットコイン、イーサリアム・クラシックを意味する。
・本図表は、各インシデントに関する報道情報等を収集し、独自に作成したものである。

署名鍵が不正使用されると、ビットコインの各ノードがその取引を停止したり、取引を元に戻したりすることはできない。

前述のように、第三者が署名鍵を預かり取引を代行するような運用モデルは、ビットコインの設計思想では想定外であるが、現実の利便性を考慮して後付けで発生したものである。この場合、暗号資産取引所は、単一障害点となるため、新たなセキュリティの要件と基準が必要となる。

ロ．プロトコルに対する攻撃の実例

2014 年に発生した Mt. Gox 事件では、ビットコインのプロトコルのトランザクション展性（transaction malleability）が悪用されたとされている。トランザクション展性とは、トランザクションの取引内容を変えずに、異なるトランザクション ID によって支払いが認められてしまう現象である。支払元はトランザクションが承認されたことを確認できなくなり、結果として二重支払い（double spending）が成立してしまう。

また、2018 年には、ビットコインのいわゆるアルトコインの 1 つであるモナコイン（MonaCoin） に対して、Selfish Mining Attack が実際に行われた。Selfish Mining Attack の詳細は本節（2）ロ．で説明するが、十分な数のノードやハッシュパワーを確保できなくなると、プロトコルで想定された安全性を維持できなくなる。これは、十分な数のノードやハッシュパワーが存在することが、ブロックチェーンの安全性の前提になっていることを意味する。同様に

2018 年には、ハッシュパワーが少ないアルトコインにおいて、51%攻撃が成功している例も報告されている。

ハ．実装の脆弱性の実例と対応

ビットコインのプロトコルを実装したソフトウエアやハードウエアに脆弱性が発見され問題となっている例もある。2018 年に、ビットコインのソフトウエアである「bitcoind」に、あらかじめ決められている上限である 2,100 万 BTC 以上のコインを発行できてしまう脆弱性が発見された[1]。

この脆弱性を公開する前に、ビットコインの開発者コミュニティである「Bitcoin Core」のメンバーは、脆弱性があるソフトウエアをインストールしているマイナーノードが全体のハッシュパワーの過半数にならないように、そのソフトウエアをアップデートする必要があった。このとき、Bitcoin Core は、あらかじめ正しく行動するとわかっている、全体のハッシュパワーの 51%以上のハッシュパワーをもつマイナーを選び、それらのマイナーに脆弱性に対応したソフトウエアを配布し、アップデートを行った。

しかし、ビットコインの信頼モデルによると、「正しく行動するとあらかじめわかっている、全体のハッシュパワーの 51%以上のハッシュパワーをもつマイナー」を事前に特定できない。そのため、この脆弱性対応は異例であるとともに、脆弱性が発生したときの対応方法について検討が必要であることを示している。ソフトウエアの入替えに伴う強制的なチェーンの分岐（ハードフォーク）が必要になることがあり、その実施方法とガバナンスもブロックチェーンを用いたシステムの課題である。

（２）ブロックチェーンに対する攻撃手法の例

イ．51%攻撃

ブロックチェーンの根幹である分散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%攻撃である。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場合、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り、過去のトランザクション・データを用いて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。

ブロックチェーン技術においては、51%攻撃は技術仕様上避けられない攻撃である。これに対抗するためには、仮に、攻撃者のハッシュパワーの合計が高々

1 この脆弱性は CVE-2018-17144 として報告・公開されている。

k と想定する場合、全体では $2k$ を超えるハッシュパワーが常に Proof-of-Work などのゲームに参加する状態を実現する必要がある。

マイナーの間でのマイニング競争に負けるリスクを抑えるために（あるいは利得を最大化するために）、複数のマイナーがグループになり、マイニングの作業を分担するということが現実には行われている。このグループのことを、一般に「マイニングプール（mining pool）」と呼んでいる。複数のマイニングプールのハッシュパワーを足すと全体の過半数となる場合には、当該マイニングプール群による 51%攻撃が可能となる。ビットコインにおいては、本稿執筆時点では 51%攻撃は発生していないが、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。

Proof-of-Work などのゲームへの参加のインセンティブを付与するために、前述のとおり、ビットコインをはじめとする暗号資産のプロトコルでは、ゲームの勝者に一定額の暗号資産を付与することにしている（マイニング）。この結果として得られる暗号資産の価値が利用者にとって十分に大きければ、その計算能力を使って暗号資産を攻撃するインセンティブがなくなる。このようなインセンティブの設計には、ゲーム理論を用いて設計・評価が可能となるという長所があるものの、どのようなゲームを設計すれば、持続的に安全性を保つことができるかについては、研究途上の段階である。

ロ．その他の攻撃

51%攻撃のほかに、二重支払いを引き起こす可能性がある攻撃の例として、Finney Attack と Brute Force Attack がある。

・Finney Attack：まず、支払者が、自分でマイニングしたコインを自分のアカウントへ支払い、そのトランザクションが入ったブロックを作成して他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。商店がトランザクションの結果を受け入れる（商品を発送する）タイミングが、トランザクションが承認されるタイミングよりも早ければ早いほど、この攻撃が成功する確率が高まる。

・Brute Force Attack：十分なハッシュパワーをもつ攻撃者が、あらかじめ 2 つのブロックチェーンを事前にマイニングして別々に用意しておく。それらのうち長い方のブロックチェーンには、自分がコントロールするノードへの送金を記録しておき、短い方のブロックチェーンには、同じコインの商店への支払いを記録しておく。短い方のブロックチェーンで商店への

支払いを完了し、それが確定した後に、長い方のブロックチェーンを他のノードに送信して、商店への支払いを上書きする（短い方のチェーンに記録されている支払いを無効化する）。

また、ブロックチェーンのプロトコルの適切な実行を妨げる攻撃の例として、Selfish Mining Attack と Sybil Attack が有名である。

・Selfish Mining Attack：あらかじめ長いブロックのチェーン（公開されているブロックチェーンからある時点で分岐したもの）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後で公開することによって、公開されていて合意される前のチェーンを覆す攻撃である。この攻撃によって、正しいと思っていた（公開されていた）ブロックをマイニングする善意の利用者のハッシュ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おそれがある。

・Sybil Attack : 攻撃者がアカウントを大量に生成するなどして多くの利用者のコピーを作り出し、分散合意アルゴリズムにおいて有利な立場を得ようとする攻撃である[2]。分散合意アルゴリズムの既存研究において一般的に想定されている攻撃であり、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、攻撃の成功の確率が完全にゼロになるわけではない[3]。

４．セキュリティの６つのレイヤーと研究の現状

（１）ブロックチェーンを利用したシステムを支えるレイヤー

一般に、暗号技術を用いるシステムにおいて、あるセキュリティ目標を達成するには、暗号技術とその組合せ、実装、そして運用にいたる異なるレイヤーにおいて適切な検討がなされることが必須である。あるレイヤーで正しく構築された技術は、他のレイヤーで正しく使わ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。例えば、安全な暗号技術を使っ

---

2 攻撃者が大量のアカウントを生成してそれらに対応するノードを準備しておくことができれば、特定のノード（攻撃対象）からの P2P による通信を遮断し、トランザクションの成立を妨害するといった攻撃が想定される。また、攻撃者が有するハッシュパワーの総量が不変であるならば、マイニングの処理には影響しないと考えられる。

3 Proof-of-Stake は、ブロックチェーンによって記録される取引の持ち分（stake）に応じてブロックを生成するノード（「リーダー」と呼ばれる）が決定される。Proof-of-Work に比べて計算量を節約できるという利点がある一方、リーダーの決定方法の検討とその安全性の証明、現実のブロックチェーンの実装環境になるべく近いモデルの構築などが主な課題となっている。

ていても、暗号鍵の運用がずさんであれば、暗号技術の効果は無となる。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、ずさんな暗号鍵の運用に起因している。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、全てのレイヤー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、おおむね図表 2 のような 6 つのセキュリティに関係するレイヤーが存在する。下のレイヤーから順番に説明する。

一番下にあるのが、基盤的な暗号アルゴリズムと呼ばれる技術であり、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 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 において評価され、汎業界向けのセキュリティ技術の標準化を担当する ISO/IEC JTC1 SC27 などで標準化が行われている。

下から 2 番目のレイヤーであるバックボーン・プロトコルは、ブロックチェーン技術の根幹となるプロトコルである。P2P ネットワークや、分散合意プロトコルが安全であるかどうかを確かめる必要がある。

下から 3 番目のレイヤーは、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ーである。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。

下から 4 番目のレイヤーは、支払いやスマートコントラクト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ーである。ビットコインやイーサリアム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。

下から 5 番目のレイヤーは、安全な実装に関するものである。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エア・コードや、暗号鍵を保

図表 2　ブロックチェーンを利用したシステムのセキュリティレイヤー

【セキュリティレイヤー】	【保護対象、要素技術の例】	【標準・ガイドラインの例】
運用レイヤー	鍵管理、監査、バックアップ	ISO/IEC 27000
実装レイヤー	プログラムコード、 セキュア・ハードウェア	ISO/IEC 15408
アプリケーション ロジック	金融取引やスマートコントラクト向けのスクリプト言語	セキュア・コーディング・ガイド
アプリケーション プロトコル	プライバシ保護、セキュア・トランザクション	ISO/IEC 29128
バックボーン プロトコル	P2P、分散合意アルゴリズム、マークル・ツリー	ISO/IEC 29128
暗号技術レイヤー	ECDSA、SHA-2、RIPEMD160	NISTやISOの標準規格

護しながら暗号処理を行うハードウエアなどの安全性を確認するレイヤーである。

最も上のレイヤーは、鍵管理、監査などを行う運用のレイヤーである。

各レイヤーの保護対象や要素技術は、ISO/IEC（International Organization for Standardization/International Electrotechnical Commission）などにおいて、標準的な技術や運用手法が標準規格やガイドラインとして定められている。ブロックチェーンにおいても、これらに適合しているか否かを確認する必要がある。

以下では、各レイヤーについて、より詳しく説明する。

（２）暗号技術のレイヤー

イ．ハッシュ関数と電子署名

暗号技術は、ブロックチェーン技術の安全性を構成する重要な要素である。暗号資産というアプリケーションにおいては、主にトランザクションの前後関係、およびブロック間の前後関係を証明するためにハッシュ値の連鎖が用いられているほか、同時に個々のトランザクションに電子署名が付与されている。電子署名アルゴリズムによって、トランザクションが改ざんされていないことを保証し、トランザクションの作成者が支払いを実行できる署名鍵を確かに有していたことを証明する。つまり、暗号アルゴリズムそのものは、ブロックチェーン上の情報が改ざんされていないことを保証するレイヤーであると言える。ビットコインでは、2 種類のハッシュ関数（SHA-2、RIPEMD-160）と電子署名アルゴリズム ECDSA が用いられている。

ハッシュ関数は、任意の長さのデータを一定のサイズのデータに圧縮する関数である。これに加えて、「暗号学的ハッシュ関数」と呼ばれるハッシュ関数においては、①ハッシュ値から元のデータ（原像）を復元できない（一方向性。原像困難性とも呼ばれる）、②同じハッシュ値になる、元のデータとは異なる別のデータ（第二原像）を見つけられない（第二原像困難性）、③同じハッシュ値になる 2 つの元データの組（衝突）を何でもよいので 1 組でも見つけることができない（衝突困難性）という性質をそれぞれ満たす必要がある。

電子署名技術は、あるデータが秘密鍵を所有している人によって確かに作られたことと、確認のためのデータ（電子署名）が作成された後に改ざんされていないことを保証する。電子署名の安全性としては、すでに存在している特定の公開鍵、署名対象のデータ、電子署名の組から、新たなデータに対する電子署名の偽造に成功しないという性質（「選択文書攻撃に対する存在的偽造不可能性」と呼ばれる）を満たすことが求められる[4]。

---

4 これらの安全性については、長年の暗号アルゴリズムの安全性評価の成果により、証明可能安全性（provable security。安全性を数学的に証明することができるという性質）というフレームワー

ロ．危殆化による影響の評価と対策

（イ）影響の評価

ブロックチェーン技術において暗号技術が危殆化したときにどのような影響があるかについては、Giechaskiel らが評価を行っている（Giechaskiel, Cremers and Rasmussen [2016]）。まず、ハッシュ関数に脆弱性が見つかった場合、以下のような影響があることが示されている。ここで、n はハッシュ関数の出力ビット長である。

・利用者のアドレスを生成するためのハッシュ関数（アドレス・ハッシュ）に脆弱性が見つかったケースでの影響
- 衝突あるいは第二原像を発見できると、支払いの否認が可能になる。
- 原像を発見できると、アドレスの解読が可能になる。
- 特定のフォーマットのデータに対する原像を発見できると、支払いの否認、および、アドレスの解読が可能になる。

・ブロックのチェーンを生成する際のハッシュ関数（メイン・ハッシュ）に脆弱性が見つかったケースでの影響
- 衝突を発見できると、コインの盗難およびコインの無効化が可能になる。
- 第二原像を発見できると、二重支払いおよびコインの盗難が可能になる。
- 原像が発見できると、$2n$ 回のハッシュ関数の処理に匹敵する計算量によって、ブロックチェーン全体を無効化することが可能になる[5]。

また、電子署名アルゴリズムが危殆化した場合には、以下のような影響があることが示されている。

・特定のデータに対する署名が偽造可能である場合、（その署名に対応する）公開鍵の情報を用いることによって、コインの盗難が可能になる。
・特定の署名に対応するデータの改ざんを検知できない場合、特定の支払いが

クに基づいて設計・評価されている。具体的には、現代のコンピュータの標準的なモデルである多項式時間チューリング機械（polynomial-time Turing machine）において、セキュリティ・パラメータ（ハッシュ関数の出力値のサイズ、電子署名アルゴリズムの鍵長など）に対して、そのパラメータの指数関数によって攻撃の難易度を示すことができるか否かを数学的に証明するというものである。このフレームワークは、アカデミアでは標準的な安全性評価手法として確立しており、ISO/IEC の国際標準、NIST（National Institute of Standards and Technology）の米国連邦政府標準、そして日本における電子政府推奨暗号リストの評価においても用いられている。

5 ある特定の原像を発見することができれば、n 回のハッシュ関数の処理に匹敵する計算量でブロックチェーン全体を無効化することが可能になる場合がある。

行われていない（そのためのコインを受け取っていない）と主張することが可能となる（否認を防止できない）。

さらに、ハッシュ関数の危殆化と電子署名アルゴリズムの危殆化が同時に発生したときには、その程度によって、上記の影響に加えて、すでに実行された支払いの内容の改ざんが発生することが示されている。

（ロ）対策

佐藤と筆者は、暗号技術に脆弱性が発見された際に、ブロックチェーン上のデータの有効性を延長するための方式を提案している（Sato and Matsuo [2017]）。この提案方式は、欧州連合における電気通信分野の標準規格を策定する ETSI（European Telecommunications Standards Institute）によって標準化されている長期署名方式の考え方をブロックチェーンに応用している。長期署名方式では、PKI（Public-Key Infrastructure）などで用いられる公開鍵証明書について、危殆化による鍵長の変更の際に、以前に発行した公開鍵証明書にタイムスタンプを付与し、そのタイムスタンプに対して、より安全な電子署名アルゴリズムで電子署名を付与することで有効期間の延長を実現している。佐藤と筆者の提案方式では、暗号技術の危殆化が発生した場合に、分散タイムスタンプを用いてデータの存在を証明するデータ（Proof-of-Existence）を作成し、それを新たに作成されるブロックに順次含めることで、危殆化したハッシュ関数や電子署名アルゴリズムで作成された古いブロックの有効期間の延長を実現している。

ハ．研究課題

安全ではない暗号アルゴリズムの使用によって脆弱性が発生した例として、以下のようなものがある。厳密にはブロックチェーンではないが、有向非循環グラフ（DAG）を用いた暗号資産である IOTA において、SHA-2 などの安全性が確認された標準的なハッシュ関数ではなく、独自のハッシュ関数（SHA-3 のアルゴリズムを変形したもの）が使われていた。そして、この独自のハッシュ関数の脆弱性を用いると、二重支払いを簡単に行うことができることが示されている[6]。このような独自方式のブロックチェーンにおいては、前述の長期署名方式の考え方を適用した危殆化対応を行うことができないため、別途、対応の研究が必要である。

長期的な課題としては、大規模な量子計算機が実用化されると、素因数分解

6 この研究成果は Heilman らによって発表されている（https://www.slideshare.net/cisoplatform7/a-tangled-curl-attacks-on-the-curlp-hash-function-leading-to-signature-forgeries-in-the-iota-signature-scheme、アクセス日：アクセス日：2020 年 3 月 9 日）。

問題や離散対数問題が解かれてしまい、電子署名の有効性が損なわれてしまうことへの対応が必要である。本稿の執筆時点では、米国連邦政府標準を定めるNIST が、量子計算機が存在しても安全な暗号アルゴリズムに関する標準化に向けたコンペティションを行っている。将来的には、このような耐量子計算機暗号をブロックチェーンに組み込む必要が出てくることが想定される。一方で、多くの耐量子計算機暗号は、鍵長や署名データ長が長くなるため、ブロックチェーンのスケーラビリティに大きな影響があることが予想される。そのため、耐量子計算機暗号のブロックチェーンへの応用は今後の大きな研究課題である。

（３）バックボーン・プロトコル

イ．セキュリティ目標に関する性質

2015 年に、Garay らは、ビットコインで提案された Proof-of-Work を利用した分散合意アルゴリズム（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（Garay, Kiayias, and Leonardos [2015]）。common prefix とは、「正直な（プロトコルに従う）参加者の任意の 2 者のペアは、ある一定のラウンド以前のブロックチェーンを共有している」という性質である。chain quality とは、「正直な参加者が作成し合意するブロックの全ブロックに対する比率が十分に大きい」という性質である。

また、Garay らは、分散台帳に必要な性質として「persistence」と「liveness」を定式化している。persistence とは、「あるトランザクションが承認されてから一定数のブロックが生成されれば、ある 1 人の正直な参加者が所持するブロックの合意は覆ることがない」という性質である。liveness とは、「正直な参加者が作成したトランザクションは一定のブロックが作成された後に正直な参加者によって承認される」という性質である。これは、攻撃者による Denial of Service 攻撃が成功しないという性質といえる。

さらに、Garay らは、攻撃者のハッシュパワーが全体の 2 分の 1 以下であり、かつ、全ての通信の同期が取れているという強い前提のもとで、ビットコインの分散合意アルゴリズムが上記の 4 つの性質を満たしていることを数学的に証明した。

Pass らは、上記の Garay らの結果を拡張して、分散台帳に必要な新たな性質として「chain growth」を定義した（Pass and Shi [2017]）。chain growth は、「正直な参加者の間では、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（「全ての通信の同期が取れている」という前提）を少し緩め、通信遅延の上限が設定される範囲において、

ビットコインが chain growth を満たすことを示している（Giechaskiel, Cremers and Rasmussen [2016]）。

現在のブロックチェーンの安全性証明は、基本的にはこれらの定式化のもとに議論されている。もっとも、ビットコインの分散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。

ロ．その他の研究課題

（イ）51%攻撃を防ぐためのインセンティブの付与

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、悪意のあるノードのハッシュパワーを上回る正直なノードのハッシュパワーが常に必要であり、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、大きな研究テーマの 1 つとなっている。

マイニングプールの存在は、オリジナルのビットコインの論文では想定の範囲外であったが、本稿の執筆時点では、ビットコインにおいては、トップ 4 のマイニングプールのハッシュパワーを合計すると、全体の 51%を超える。このため、これらのマイニングプールが結託した場合、ブロックチェーンに記録されるデータをコントロールすることができるようになる。現時点のブロックチェーンのプロトコルの仕様には、マイニングプールの存在をなくすための手段が実装されているものはほとんどない。しかし、現実には全体のハッシュパワーが少ない暗号資産に対して、51%攻撃が成功している事例がみられる。マイナーが局所最適としての利得を最大化しようとする行為を防ぐとともに、マイニングプールによる 51%攻撃も防ぐためのインセンティブ作りは今後の研究課題である。

上記は Proof-of-Work についての状況であるが、Proof-of-Stake を利用したブロックチェーンにおいては、Brute Force Attack による二重支払いが想定されるなど、別のタイプの攻撃も存在する。Proof-of-Stake を利用したブロックチェーンおけるインセンティブ構造についてもさらなる研究が必要である。

（ロ）インターネットへの攻撃と対策

また、ビットコインをはじめとする暗号資産のバックボーン・プロトコルそのものではないが、ブロックチェーン技術が暗黙のうちに「自由に利用できる」

と仮定しているインターネット自体にも、そもそも攻撃の余地がある。インターネット自体の脆弱性を悪用することで、ブロックチェーンのバックボーン・プロトコルの動作に悪影響を与える可能性は否定できない。

例えば、Apostolaki らは、BGP（Border Gateway Protocol）の脆弱性を用いて、P2P を利用したブロックデータの伝播をコントロールするという攻撃を発表している（Apostolaki, Zohar, and Vanbever [2017]）[7]。任意の（AS を操作可能なレベルの）攻撃者は、50%までのハッシュパワーを隔離することができ、その結果として二重支払いの攻撃が容易に実行できることが示されている。また、Apostolaki らは、この攻撃に耐性のあるビットコイン用のリレーネットワークの提案を行っている（Apostolaki *et al.* [2018]）。

（４）アプリケーション・プロトコル

このレイヤーでは、安全なトランザクション処理、トランザクション処理のスケーラビリティ確保やプライバシ保護を実現することが期待される。

イ．トランザクション処理

トランザクション処理については、パーミッションレス・ブロックチェーンでは、原理的にスケーラビリティの強い制約を受けており、これを解決するための研究が数多く行われている。主要なものは、ライトニング・ネットワーク（Lightning Network）に代表される「Layer 2 技術」と呼ばれるものである（Poon and Dryja [2016]）。これは、メインのブロックチェーン（バックボーン・プロトコル）そのものの処理はそのままに、ブロックチェーンの外（オフチェーン）で支払行為を実施し、一定期間に行われた最後の差引きの結果だけをメインのブロックチェーンに書き込むというものである。

このようなペイメント・チャネル（Payment Channel）と呼ばれるプロトコルは、ブロックチェーン（バックボーン・プロトコル）そのものの処理には影響を与えない。しかし、ペイメント・チャネルのネットワーク自体に、単一障害点が存在しうることが指摘されており（Rohrer, Malliaris, and Tschorsch [2019]）、ビットコインなどのパーミッションレス・ブロックチェーンの信頼モデルを毀損する可能性がある。また、ライトニング・ネットワークを導入することにより、ビットコインが本来目指していたプライバシ保護のレベルが低下することも指摘されている（Beres, Seres, and Benczur [2019]）。

---

[7] BGP は、インターネットを構成する AS（Autonomous System）間で経路情報を交換するプロトコルである。ここで、AS とは、統一された運用ポリシーによって管理されたネットワークの集まりを指す。

ロ．プライバシ保護

プライバシ保護の要件について、暗号資産やブロックチェーンにおいては、代替可能性（fungibility）という用語が使われる。これは、2 つのトランザクションにおいて使われたコインの間に関連があるか否かを示す概念であり、「お金に色はない」という性質を表している。例えば、ゼロキャッシュ（ZeroCash）の論文（Ben-Sasson *et al.* [2014]）では、プライバシを確保した暗号資産の方式を指す言葉として、「decentralized anonymous payment scheme（DAP scheme）」という用語が定義され、その中で、「ゼロコイン（ZeroCoin）は代替可能（fungible）である」と主張されている。

この論文では、プライバシ要件の定式化として、「ledger indistinguishability」が定義されている。これは、「2 つの台帳があり、その両者にランダムな支払いのトランザクションを行った時に、攻撃者がトランザクションと台帳の関係を見分けられない」という要件である。本稿執筆時点では、代替可能性の定式化された定義はないが、この論文における ledger indistinguishability の定義は、プライバシ要件の議論の基礎となると考えられる。

暗号資産において、プライバシ要件を求める一方で、マネーロンダリングの防止（Anti-Money Laundering : AML）が金融当局にとっての必須の要件となっている。G20 配下で AML に関わる規制を定める FATF（Financial Action Task Force）は、トラベルルールと呼ばれる新しいルールを暗号資産や仮想通貨を扱う事業者に課すことを決めて 2020 年よりこのルールが発効することになっている。しかし、プライバシと AML の要件を両立するように暗号資産の技術仕様の要求を定式化したものは、本稿の執筆時点では存在しない。

（５）アプリケーション・ロジック

アプリケーション・ロジックは、決済やその他のビジネス・ロジックを設計するレイヤーである。ビットコインの支払いは三式簿記によって行われるが、ビットコインにおいてはこの帳簿の書換えがビジネス・ロジックに当たる。イーサリアムでは、「Solidity」というスクリプト言語が存在し、Solidity を利用して、スマートコントラクトのような、支払いよりも高度なプログラムを記述し、実行することができる。

イ．セキュリティ要件と各種の攻撃

このレイヤーにおけるセキュリティ要件は、アプリケーションとして正しく動作し、セキュリティ上の問題が生じないことである。いくらブロックチェーンのバックボーン・プロトコルが記録を改ざんされずに更新し続けたとしても、ブロックチェーンに記録されるトランザクションの情報が間違っていれば、ア

プリケーション全体のセキュリティを保つことはできない。

2016 年に発生した The DAO 事件は、イーサリアム上のプラットフォームである The DAO において、トランザクションのロックの機構にバグが存在し、スマートコントラクトにおける処理の再帰的呼出しを悪用されてイーサリアムが引き出され続けることで発生した。一般に、金融取引の処理においては、ロックの機構や再帰的呼出しの設計は慎重に行われるが、Solidity の言語仕様がそのための機構を持っていなかったために、この事件は発生した。

スマートコントラクトにおいては、このような言語仕様とプログラムの脆弱性を突いた攻撃がいくつか提案されている。The DAO 事件のような再帰的呼出しが発生する脆弱性は Reentracy Attack と呼ばれる（Grincalaitis [2017]）[8]。

ロ．研究課題

（イ）形式検証

スマートコントラクトは、ブロックチェーン上で自律的に実行される可能性があるため、状態遷移の管理を厳密に行う必要がある。このレイヤーで安全なプログラムを作成するための 1 つの方向性として、形式検証を利用して、スマートコントラクトのプログラムが安全でない状態遷移をしないことを確認する研究がある（Mavridou and Laszka [2017]）。これらの研究では、Solidity などのスクリプト言語で書かれたプログラム・ロジックの状態遷移を、モデル・チェッカなどの形式検証が可能な環境でチェックし、あらかじめ決められた（安全でない）状態にたどり着く可能性があるどうかをチェックする。

形式検証は、一般的には、検証環境の制約があるため、安全性を保証するものではない。むしろ、制約がある検証環境において、攻撃の成功に繋がるパスがみつからなかったことを確認することができる。また、攻撃の成功に繋がるパスがみつかった場合には、その攻撃に至る道筋がみえるため、その情報を元に、プロトコルやプログラムの設計を見直すことができる。Mavridou らのグループの研究も、スマートコントラクトの開発者が形式検証によるフィードバックを元により安全なプログラムを作成するための方法を提案している。

（ロ）Domain Specific Language

もう 1 つの研究の方向性は、スマートコントラクトを記述するプログラミング言語に一定の制約を課して、形式検証しやすくする、あるいは、攻撃の成功に繋がるパスをあらかじめ限定するというアプローチである。アプリケー

8 このほかに、Overflow Attack、Replay Attack、Short Address Attack、Balance Attack などが存在する。これらの攻撃については、Grincalaitis [2017]や「Ethereum Contract Security Techniques and Tips」（https://github.com/ethereum/wiki/wiki/Safety、アクセス日 : 2020 年 3 月 9 日）に記載されている。

ションの目的に沿った言語を作るという意味で、Domain Specific Language と呼ばれる。

（６）実装レイヤー

このレイヤーは、前述の 4 つのレイヤーを、プログラムコードやハードウエアに落とし込むレイヤーである。

このレイヤーでは、バグによって脆弱性が引き起こされる可能性が常に存在し、そのような脆弱性が存在しないか否かをチェックすることが重要である。脆弱性を引き起こしにくいプログラム処理系を利用することも 1 つの方法である。これはセキュリティだけでなく、プライバシ保護においても同様である。

現実には、ハードウエア／ソフトウエアを問わず、実装に対する攻撃が存在する。例えば、①電力消費や処理時間など暗号処理に直接関係ないが副次的に取得できる情報（サイドチャネル）から暗号鍵を類推する、②ハードウエア上の回路に意図的にデータを仕込んで鍵を類推するための情報を取得する（フォールト・インジェクション）、③メモリーチップを冷やしてメモリー内に存在している情報の残留時間を延ばした上で、その情報を取得する（コールド・ブート）などの攻撃への対応を考える必要がある。

暗号資産において、最も重要な実装上の保護ポイントは、暗号鍵を保持しながら暗号処理を行うモジュールである。PKI など、一般的な暗号技術のアプリケーションにおいては、ハードウエア・セキュリティ・モジュール（Hardware Security Module）がこのような処理を行うモジュールになっている。一方で、暗号資産においては、もともと各利用者の責任で署名鍵を管理することになっているため、ハードウエアによる鍵管理モジュール（ハードウエア・ウォレット）を利用することが推奨されている。

これは一般的には正しい方向性ではあり、「FIPS140-2 に準拠している[9]」と宣伝している製品がある。しかし、これらの宣伝がなされている製品を含めて、サイドチャネル攻撃への耐性があるか否かを実際に試験・認証することが困難な状態にある。例えば、ソフトウエア製品や情報システム一般を対象としたセキュリティの試験・認証の国際的な枠組みであるコモン・クライテリア（Common Criteria。ISO/IEC 15408 として国際標準化されている）や CMVP において試験・

9 FIPS 140-2 は、暗号モジュールが満たすべきセキュリティ要件に関する米国連邦政府標準である。FIPS 140-2 に基づくフレームワークにおいては、製品化された暗号モジュールがこの標準規格に適合しているか否かを第三者機関が試験・認証するための制度として CMVP（Cryptographic Module Validation Program）が準備されている。通常、こうした試験等は、対象の暗号モジュールが、その設計段階において想定されていたセキュリティ要求仕様を満たしているかどうかという観点で実施される。したがって、試験等を実施するためには、セキュリティ設計仕様（protection profile）を準備することが前提となる。

認証を実施することが考えられる。もっとも、こうした試験・認証を行ううえでの前提となる（ハードウエア・ウォレットの）セキュリティ要求仕様（protection profile）が存在しておらず、試験・認証の対象とすることができない。そうした中で、現実のハードウエア・ウォレットのなかには、脆弱性を有するものが存在することを示した研究成果が発表されている（Volokitin [2018]）。

他方、ブロックチェーンのスケーラビリティ問題を解決する方法として、鍵管理が厳密に行われていることを前提に、TEE（Trusted Execution Environment）上でペイメント・チャネルのプロトコルを実行する方式などが提案されている[10]。しかし、この場合、TEE そのものの安全性が製造者によって担保されていること、つまりサプライチェーン・リスクが存在しないことを別の手段で保証することが必要となる。

また、3 節（1）で示したように、ブロックチェーンのプロトコル自体の（ハードウエア／ソフトウエア）実装においても、脆弱性は常に存在しうる。このようなケースに対して、実際の攻撃を防ぐための「責任ある開示（Responsible Disclosure）」の方法を確立する必要がある[11]。また、すでに指摘しているように、51%攻撃を防ぎながら、新しいソフトウエアに更新するための、ネットワーク参加者の間での合意方法を確立することが必要である。

（7）運用レイヤー

このレイヤーは、暗号資産等のブロックチェーンのシステム全体を、人を含めてどのように運用し、監査するかを定めるレイヤーである。

システムとしてのセキュリティ・ポリシーを定めるところから始まり、そのセキュリティ・ポリシーを実際の作業項目に落とし込み、実現可能な形にすることが必要になる。また、運用は常に監査とセットになっており、監査の方法も規定する必要がある。改善のための PDCA ポリシーをどう回すか、例えば The DAO 事件における対応においても議論になった、脆弱性による問題にどのように対応するのか、という点もこのレイヤーに含まれる。セキュリティ・ポリシーは誰かが規定する必要があり、それを規定するコミュニティの存在を仮定する必要があるが、非中央集権的なコミュニティでうまく規定するのは簡単ではない。

このレイヤーにおいても、暗号資産の文脈で一番クリティカルなのは、署名鍵

---

10 TEE は、主にソフトウエアを用いて、通常の実行環境から論理的に分離された実行環境を実現する技術である。通常、サイドチャネル攻撃等の物理的な攻撃が想定されていないことから、セキュア・エレメントなどの物理的な攻撃への耐性を有するデバイスと共に利用される。

11 Responsible Disclosure は、ホワイト・ハッカーや学界の研究者が脆弱性を発見した際の対応の標準的な手続きである。一般的な情報システムの場合であれば、それを開発ベンダーに連絡し、開発ベンダーが修正プログラムを作成してセキュリティを確保する道筋を確立させる。その後、脆弱性を発見した研究者等が関連する論文を発表する。

の管理である。Martin は、Firefox のゼロデイ攻撃を用いた暗号資産取引所への攻撃の実例を紹介している[12]。また、3 節（1）イ．で示したように、暗号資産取引所のインシデントの多くは鍵管理の不備によって発生している。これらのインシデントのいくつかは、標的型攻撃などの、いわゆるサイバー攻撃を皮切りに発生している。そのため、一般的な利用者のコンピュータ・ノードを含め、ネットワーク・セキュリティの観点で適切な運用が求められる。

ただし、現実には、暗号資産取引所のシステムは、それぞれの取引所が独自の実装をしており、共通のアーキテクチャや安全性が確認された実装が存在しないというのが現状である。ISO/IEC 27000 シリーズ[13]に規定されているような情報セキュリティ・マネジメント・システムに対応した、システムのリスク分析を行い、必要なセキュリティ対応策（Security Controls）を設計、実装、運用することが求められる。このような試みは、すでに CGTF（Cryptoasset Governance Task Force）において始まっている[14]。CGTF は、ISO/IEC 27002 に従って、暗号資産取引所のシステムのモデル化、セキュリティ目標の明確化、およびリスク分析とセキュリティ対応策の提案を行った文書を作成し、ISO におけるテクニカルレポートの作成に貢献している[15]。

前述したハードフォークについても、ブロックチェーン全体の持続的な安全な運用のために考慮すべき点であり、ハードフォークの実施についてのガバナンスも検討される必要がある。

５．ブロックチェーン技術におけるセキュリティとのトレードオフ

ブロックチェーン技術には、セキュリティに関係する様々なトレードオフがある。一番重要なのは、スケーラビリティとセキュリティのトレードオフである。スケーラビリティを向上させるためには、単純にはブロックサイズを増やせばよいが、ブロックサイズを増やすと各ノードで記録すべき情報量が増えるために、マイニングを行うフルノードの運営コストが増加する。その結果、全体の

---

12 URL は、https://blog.coinbase.com/responding-to-refox-0-days-in-the-wild-d9c85a57f15b である（アクセス日：2020 年 3 月 10 日）。

13 ISO/IEC 27000 シリーズは、企業等における情報システムのセキュリティ管理の枠組み（情報セキュリティ・マネジメント・システム）に関する国際標準群である。これらのうち、ISO/IEC 27002（code of practice for information security management）は、情報セキュリティ・マネジメント・システムのベスト・プラクティスを規定している。

14 CGTF は、暗号資産の取引等に関するリスク管理のための安全対策基準の策定を目的として 2018 年に設立された研究会である。セキュリティ技術の専門家や暗号資産の交換業者の実務者等によって構成されている。

15 これは ISO TR 23576（blockchain and distributed ledger technologies – security management of digital asset custodians）として標準化が進められている（https://www.iso.org/standard/76072.html。アクセス日：2020 年 3 月 10 日）。

ハッシュパワーが減少し、パーミッションレス・ブロックチェーンにおける 51%攻撃の成功確率が上がる。この問題への対処として、ライトニング・ネットワークのような Layer 2 技術が考案されているが、前述のように、ライトニング・ネットワークには、トラフィックの偏りの問題があり、ビットコインと同等の信頼モデルを実現できないことに注意が必要である。

また、パーミッションレス・ブロックチェーンでは、トランザクションの finality がない。つまり、トランザクションは 100%確定することはなく、一定の合意のもと、現実的に覆る可能性はないとみなすことで取引を続ける。ビットコインの場合、6 ブロック（1 時間）経過すると、トランザクションはもう覆らないとみなす。しかし、finality を必要とした場合、PBFT のような別の分散合意アルゴリズムが必要となる[16]。そして、パーミッションレス・ブロックチェーンが前提としたような、信頼できるノードの存在を前提としない自由参加型のモデルを諦めることが求められる。

６．おわりに

本稿では、暗号資産を支える技術であるブロックチェーン技術と、それに基づいて構成される暗号資産のシステム全体におけるセキュリティ目標とその構造を述べ、セキュリティ目標を達成するための 6 つのレイヤーについて、セキュリティ研究の現状とセキュリティ対策の方向性を述べた。

セキュリティの評価や比較を行うためには、定式化されたセキュリティモデルと、セキュリティの評価方法が必要であるが、ブロックチェーン技術と暗号資産においては、バックボーン・プロトコルにおいて定式化されている部分はすでに存在するほか、ベースとなる暗号技術の危殆化の影響評価とその対応に関する方式も提案されている。一方で、スケーラビリティを得るための Layer 2 技術や、より広い応用のためのスマートコントラクトのセキュリティについては、今後の研究が必要である。特に、セキュリティの定式化のための取組みは、まだ始まったばかりであり、今後の大きな研究課題であると言える。

以　上

16 PBFT（Practical Byzantine Fault Tolerance）は、ビザンチン故障（Byzantine Fault）への対応を目的として提案された分散合意プロトコルの 1 つであり、ノード間で相互に通信しつつ（ブロックチェーンに接続する）新しいブロックを投票で決定する（一定数以上のノードの承認が必要）という手法である。ビザンチン故障とは、複数のノードが相互に通信しながら一定の処理を実行する分散ネットワークにおいて、あるノードが故意または不作為によって不適切な処理結果を生成し他のノードにそれを送信する状態を指す。

参考文献

Apostolaki, Maria, Gian Marti, Jan Müller, and Laurent Vanbever, “SABRE: Protecting Bitcoin against Routing Attacks,” arXiv:1808.06254, 2018.

————, Aviv Zohar, and Laurent Vanbever, “Hijacking Bitcoin: Routing Attacks on Cryptocurrencies,” *Proceedings of IEEE Symposium on Security and Privacy (SP) 2017*, IEEE, 2017, pp. 375-392.

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” *Proceedings of IEEE Symposium on Security and Privacy (SP) 2014*, IEEE, 2014, pp. 459–474.

Beres, Ferenc, Istvan Andras Seres, and Andras A. Benczur, “A Cryptoeconomic Traffic Analysis of Bitcoin’s Lightning Network,” arXiv:1911.09432, 2019.

Garay, Juan, Aggelos Kiayias, and Nikos Leonardos, “The Bitcoin Backbone Protocol: Analysis and Applications,” *Proceedings of EUROCRYPT 2015*, *Lecture Notes in Computer Science*, 9057, Springer-Verlag, 2015, pp. 281-310.

Giechaskiel, Ilias, Cas Cremers, and Kasper B. Rasmussen, “On Bitcoin Security in the Presence of Broken Cryptographic Primitives,” *Proceedings of European Symposium on Research in Computer Security (ESORICS) 2016*, *Lecture Notes in Computer Science*, 9879, Springer-Verlag, 2016, pp. 201-222.

Grincalaitis, Merunas, “The Ultimate Guide to Audit a Smart Contract,” 2017 (available at: https://medium.com/ethereum-developers/how-to-audit-a-smart-contract-most-dangerous-attacks-in-solidity-ae402a7e7868、2020 年 3 月 6 日).

Haber, Stuart, and Wakefield Scott Stornetta, “How to Time-Stamp a Digital Document,” *Journal of Cryptology*, 3(2), 1991, pp. 99-111.

Mavridou, Anastasia, and Aron Laszka, “Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach,” arXiv:1711.09327, 2017.

Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008 (available at: https://bitcoin.org/bitcoin.pdf、2020 年 3 月 6 日).

Pass, Rafael, and Elaine Shi, “FruitChains: A Fair Blockchain,” *Proceedings of ACM Symposium on Principles of Distributed Computing (PODC) 2017*, Association for Computing Machinery, 2017, pp. 315-324.

Poon, Joseph, and Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016 (available at: https://lightning.network/lightning-network-paper.pdf、2020 年 3 月 6 日).

Rohrer, Elias, Julian Malliaris, and Florian Tschorsch, “Discharged Payment Channels: Quantifying the Lightning Network’s Resilience to Topology-Based Attacks,”

arXiv:1904.10253, 2019.

Sato, Masashi, and Shin'ichiro Matsuo, "Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography," *Proceedings of International Conference on Computer Communication and Networks (ICCCN) 2017*, IEEE, 2017, pp. 1-8.

Volokitin, Sergei, "Software Attacks on Hardware Wallets," Black Hat USA 2018, 2018 (available at: https://i.blackhat.com/us-18/Wed-August-8/us-18-Volokitin-Software-Attacks-On-Hardware-Wallets-wp.pdf、2020 年 3 月 6 日).