ブロックチェーンの安全性と運用にまつわる諸問題

Review of blockchain and its issues and limitations

田中 覚 [1)]

Satoru Tanaka[1)]

Abstract ：暗号技術と分散ネットワーク技術によって構成された分散型台帳技術であるブロックチェーンは，高い安全性を持つと考えられ，仮想通貨を始めとした各種サービスや電子データベース，ゲームなどの応用に利用が進められている．一方で，サービス提供開始後に攻撃を受け，多大な損害を受けたシステムも存在し，概念検証段階からサービス提供の段階までには考慮すべき課題が存在する．本論文ではブロックチェーンを構成する理論的背景，ネットワーク技術について概説した上で，ブロックチェーンの実装・運用における問題について，実際に生じた問題を基に解説を行う．

Keywords ：ブロックチェーン，ハッシュ関数，仮想通貨，分散ネットワーク

1. 緒言

サトシ・ナカモトによるビットコインの発表[1]後，多数の仮想通貨の乱立とともに，通貨システムを実現するブロックチェーンに対しても注目されるようになった．ブロックチェーンが実現する技術そのものは，クライアント―サーバ方式のネットワークではない，ピア・ツー・ピア方式で構成される分散型ネットワーク上に構成されたデータベースに過ぎない．一方で，ブロックチェーン上に記録されるデータは，データ本体から計算されるハッシュ値によって連鎖が構成され，ハッシュ値の計算困難性に基づく改ざん不可能なデータが形成される．また，トランザクションのデータにノイズを混ぜ，ハッシュ値が特定の値を持つように設計することで，合意を得るようにチェーンを構成する．この結果，既存のサーバで実現していたデータベースそのものを分散型ネットワーク上で実現できるだけでなく，時系列を維持したデータを格納したり，合意を得た情報のみを貯蓄したりすることができる．

ブロックチェーンの応用先は仮想通貨だけに限定されない．各種のポイントサービス，電子カルテやチケットサービスやオークションシステムなどの既存のデータベース管理されていたサービスに適用するなどの検討がなされている[2]．一方で，ビットコインを皮切りにブロックチェーンを基盤とした多数の仮想通貨が誕生したが，理論上の安全性とは異なる，実装・運用上発生しうる脆弱性を衝かれて様々な事件が発生している．ブロックチェーン自身の研究，あるいはブロックチェーンを用いる開発はブロックチェーンの性質や安全性だけでなく，実装・運用における問題点も理解した上で実施することが重要である．

本論文では，ビットコイン等仮想通貨に用いられるブロックチェーンに関する技術的な動向を解説し，実装・運用上生じうる諸問題について，現実に発生した事件を踏まえつつ解説する．分散型台帳技術としてのブロックチェーンは，暗号，ネットワーク分野の複合技術である．実際に概念検証（Proof of Concept）としてブロックチェーン実装を試みる際に理解すべき要点を総括する．2節ではデータ構造と付随する暗号技術について解説する．3節はブロックチェーンで採用される分散型ネットワークモデルについて解説する．4節ではブロックチェーンの生成に係る，ネットワーク上での合意形成について解説する．5節ではブロックチェーン実装によって生じる種々の問題について，現実に起こった事件を踏まえて概説し，6節でまとめと今後のブロックチェーンについて述べる．

2. ブロックチェーンの定義

本節では，ブロックチェーンを構成する理論と技術について述べる．ここではデータ構造とブロック生成について主に取り扱うこととする．通信やデータ生成時に利用される共通鍵暗号，公開鍵暗号やデジタル署名等については[3]を参照されたい．図 1 に，ブロックチェーンのデータ構造を示す．

ブロックチェーンの各ブロックはノードとも呼ばれ，ブロック内のデータにトランザクションデータ，タイムスタンプ，直前のブロックのハッシュ値が格納されている．トランザクションデータはビットコイン等ならば取引情報等，ブロックに格納される主たる情報が含まれ，ブロックを作成した時点のタイムスタンプが記録される．

1)東京都立産業技術高等専門学校　ものづくり工学科，電子情報工学コース

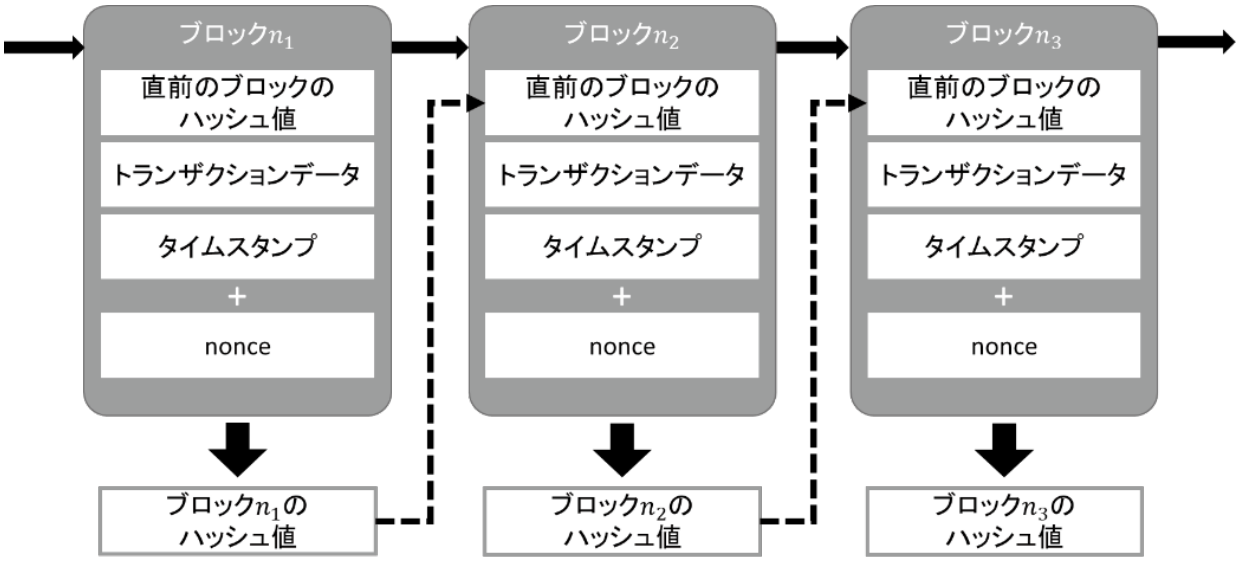


図 1　ブロックチェーンのデータ構造

ブロックチェーンで用いられるハッシュ値の計算は暗号学的ハッシュ関数，すなわち

$$\mathcal{H}: \{0,1\}^* \to \{0,1\}^n$$

で定義される，任意の入力長のデータに対して出力長が高々nで固定されたデータを返す関数を用いて計算される．暗号学的ハッシュ関数は，

① 与えられたハッシュ値$\mathcal{H}(m)$から元の入力値を計算することが困難であること（原像計算困難性）

② ある入力m_1に対して，$\mathcal{H}(m_1) = \mathcal{H}(m_2)$を満たす別の入力$m_2$，すなわちハッシュ値が一致する別の入力を見つけることが困難であること（第 2 原像計算困難性）

③ ハッシュ関数$\mathcal{H}$が与えられたとき，$\mathcal{H}(m_1) = \mathcal{H}(m_2)$を満たす異なる入力$m_1, m_2$を見つけることが困難であること（強衝突耐性）

が必須である．近年のブロックチェーン実装では，主に RIPEMD-160[4]，SHA-256[5]などのハッシュ関数が用いられ，これらは上記性質を満たした暗号学的ハッシュ関数である．生成されたハッシュ値を次のブロックのデータとして含むことで，ブロック及びチェーンを改ざんすることの困難さを高めている．

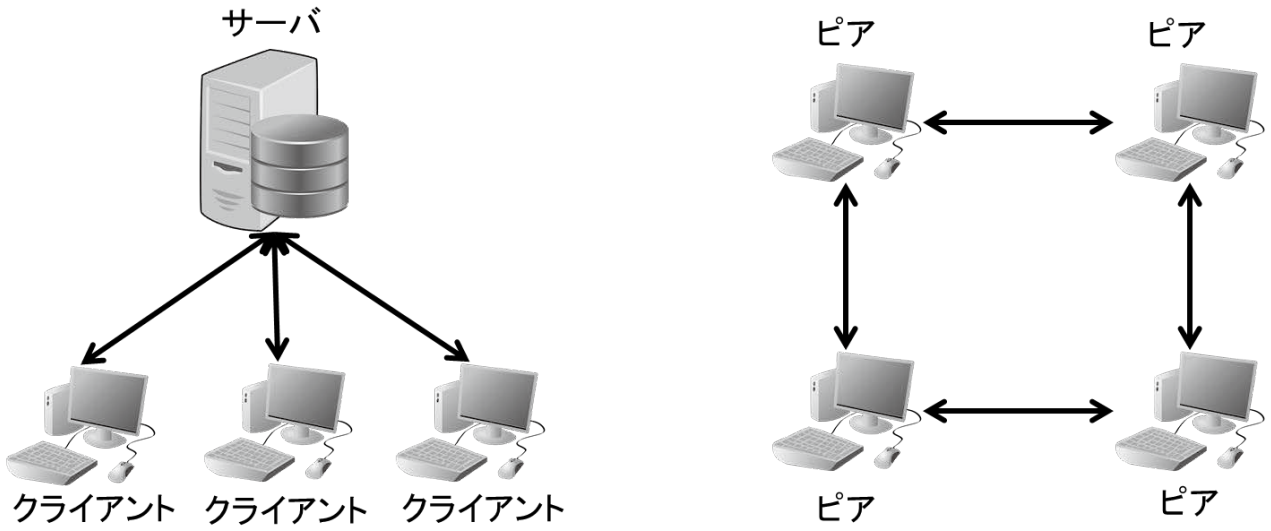
ブロックに付与するハッシュ値の計算には，トランザクション，タイムスタンプに加えて直前のデータのハッシュ値があれば計算は可能である．これらに加え，生成されるハッシュ値の上位nビットが全て 0 である等の制約条件を加えることで，ブロックチェーンに新たなブロックを生成することができる．ハッシュ関数から出力される値は入力によって一意であるから，制約条件を満たすハッシュ値の生成にはトランザクション等のデータと異なり，変更してもよい値が必要である．このような一時的に用いる値を nonce（Number of once，ノンス又はナンス）と呼ぶ．nonce を変更した場合，ハッシュ関数は異なる値を返すため，ブロックを生成するにはハッシュの計算能力が必要となる．この無数の nonce から制約条件を満たすハッシュ値を探し，ハッシュを計算して新たなブロックを生成する行為は，鉱山から鉱石を掘り当てる行為に見立ててマイニングと呼び，採掘を行うユーザはマイナーと呼ばれる．マイニングには計算機資源の他，それを動かすための電力と膨大な計算に必要なコストが必要となるため，計算対象となるハッシュ関数に対して専用のハードウェア（ASIC :Application Specific Integrated Circuit）が用いられる．

3.　分散型ネットワーク技術

本節では，ブロックチェーンの実装におけるネットワーク技術に関して述べる．図 2 にインターネットを含め普遍的に用いられるネットワークモデルを示す．

インターネットを含む通常のネットワークでは，World Wide Web を含めたサービス提供者と受益者が別個に存在するため，図 2（1）のようなサーバ―クライアントモデルによるシステムが用いられる．一方で，ブロックチェーンはしばしば分散型台帳技術と呼称される通り，中核となるシステム提供者の存在を仮定しない．また，システムの利用者・受益者自体がブロックを生成することができるため，システムの提供者たり得る．このようなネットワークは，図 2（2）のような各計算機間で直接通信を行うピア・ツー・ピア(Peer to Peer, P2P)モデルにより構成される．

ネットワークでのサービスは概して一貫性（Consistency），可用性（Availability），分断耐性（Partition-tolerance）の 3 性質を満たすことが要求される．P2P ネットワーク上のブロックチェーンは，ネットワークに参加している全部のノードであるピアがそれぞれブロックチェーンを共有することから，高い可用性を持つシステムである．また，ネットワーク内の特定の計算機が特別な用途，例えば，サーバ―クライアントモデルにおけるサーバの役割を担うことがないため，たとえ一部のピアが動作不能となった場合でも，ネットワーク内で残存したピアでブロックチェーンを維持することができる．ゆえに，ブロックチェーンは分断耐性をも持つシステムである．



（1）サーバ―クライアントモデル　　（2）ピア・ツー・ピアモデル

図 2　ネットワークモデル

ブロックチェーンは可用性と分断耐性を強く持つ一方で，データの冗長化を実現するためにはチェーン情報を全てピアが保有することで実現している．しかし，ブロックの生成後にチェーン情報を全てのピアが保有するためにはタイムラグが存在する．このため，一貫性については比較的弱く，順序性を要求する取引や，瞬時に手続きが完了することが期待できる業態での応用には対策が必要である．

4.　ブロックチェーンにおける合意形成

ブロックチェーンでは，チェーンの生成には同時にネットワーク内の全てのピアにおいて同一の計算を実施する．全てのピアの計算結果が一致する場合には問題とならないが，結果が一致しない場合は何らかの合意形成を行い，記録の整合性を取る必要がある．

ブロックチェーンでは，ブロック生成のルールによってチェーンの形式を大別でき，パブリック型とプライベート型の 2 種類に分別される．それぞれの特徴を表 1 にまとめる．

表 1　ブロックチェーンの種別による合意形成

	パブリック型	プライベート型
参加者の母数	不定	一定
ブロック生成権	任意のノード	特定の管理者ノード
合意形成	Proof of Work(PoW)等	リーダー提案による多数決

通常，ビットコイン等に代表される仮想通貨ではパブリック型チェーンが採用されるため，任意のノードがブロック生成権を得る．一方で，自由なノード参加により参加者の母数は不定である．このため，プライベート型チェーンで行われる，リーダー提案による多数決による合意形成を行うことができない．

パブリック型チェーンでの合意形成は，Proof of Work や Proof of Stake 等のチェーン生成に係る計算によって実現される．2 節で，チェーンの生成にはデータを基としたハッシュ値を生成することに触れた．特定の制約条件を満たすハッシュ生成を行うための nonce の確定は，ハッシュ関数の一方向性のために多大なリソースを必要とする．一方で，生成されたブロックの正当性検証は，元

データと計算に用いられたnonceが与えられたとき，ハッシュ関数に入力としてハッシュ値を計算すれば良く，検証は容易である．このとき，ブロック生成，検証において信頼性を必要としないため，パブリック型チェーンはトラストレスな合意形成を実現し，公共性・真正性・透明性に優れたシステムを構成する．

Proof of Work で生成するハッシュ値の制約条件によっては，制約条件を満たすハッシュ値で異なる複数のハッシュ値を生成することが起こり得る．このようなブロックの分岐（フォーク）が起こった場合は，各ノードが適切と判断したブロックを基に新たなブロックを生成し，チェーン長が一番長いもののみが最終的に有効となる．ブロック生成にはリソースが必要となるため，生成時に利益を付与されるものがいわゆる仮想通貨である．分岐が発生した場合，最終的に最大チェーン長を持つブロックを生成しなければ利益は全て失われるため，一時的な計算結果の食い違いが起こった場合でも必ず分岐は収束し，最長のチェーンの最終ブロックから合意形成を行っていく．

ブロックチェーンにおける分岐は合意形成の段階で一時的に発生するものの他，ソフトウェアアップデート等によるチェーン生成における規則の変更によっても生じ得る．既存の規則と互換性のある規則による分岐はソフトフォークと呼ばれ，通常起こる一時的な分岐と同様にネットワークで合意形成が行われ，分岐が収束した時点で新旧の規則の統一が図られる．一方，既存の生成規則と互換のない規則変更はハードフォークと呼ばれる．ハードフォークが生じた場合，チェーンの分岐はチェーンの分裂となり，仮想通貨におけるハードフォークは新たな通貨の誕生を意味する．

5. ブロックチェーンにまつわる諸問題

前節までででブロックチェーンの技術的背景について述べた．ブロックチェーンを構成するハッシュ関数の性質により，ブロックチェーンの生成されたブロックの改ざん等，直接攻撃は極めて困難である．また，チェーンの存在する P2P ネットワークは耐障害性も高い．これらの性質から，ブロックチェーンの応用が期待されるのも事実であるが，一方で現実の実装と運用によって生じている問題も存在する．多くの問題が，仮想通貨に関連するブロックチェーンで起こった問題であり，甚大な経済的被害を引き起こしている．以降で述べる問題は，実際に起こった具体例を挙げつつ，多くは仮想通貨に由来する問題ではなく，ブロックチェーンで構成されたシステムが抱えている問題として認識する必要がある．

5.1 Proof of Work における 51%攻撃に係る問題

4 節で述べた通り，Proof of Work におけるブロックチェーンの合意形成はブロック生成に係る計算によって行われ，チェーンの分岐が発生した場合でも最長のチェーンが有効なチェーンであることから，利益を得るためには最長のチェーンの生成を支持する必要がある．換言すれば，有効なブロックチェーンを維持するには常にネットワーク内の過半数以上の計算能力を用いてマイニングを行い続ける必要がある．一方で，単独のユーザがネットワーク内の過半数以上の計算能力を保有した場合，過半数の計算能力を用いることで任意のトランザクションによるブロック生成を行うことができ，常に最大長のチェーンを支配できてしまう問題が発生する．株式会社における議決権に係る問題と同様に，過半数を占めたユーザによりチェーンの独占を行うことから，51%攻撃と呼称されている．

51%攻撃が最初に認識されたのは 2014 年，ビットコインにおいて，マイニングプール ghash.io の計算能力が 50%を超えたことにより顕在化した[6]．通常，Proof of Work でのマイニングには多大な計算資源と電力を消費するため専用のハードウェアや設備が必要になるが，複数のユーザが協力してマイニングを実施することで各ノードのコストを軽減できる．このようなマイニングの連合をマイニングプールと呼ぶが，悪意の有無によらずチェーン上での計算能力が過半数を占めた時点で 51%攻撃が成立してしまったことで問題となった．現実に 51%を占めたユーザが発生した場合，ユーザによりチェーン生成を制御可能になってしまうため，仮想通貨への不正使用が可能となり，究極的にはチェーン自体の価値が無価値になってしまう問題が生じる．ghash.io によって生じた危機的状況は，最終的に ghash.io プールを構成するユーザが自発的に別のマイニングプールへ移動することで計算能力を削減したことで回避された．

51%攻撃は，マイニングプールによる計算能力超過の他にも，以下の例が実際に想定される．

① 各々のマイニングプールが 51%を占めていない状況でも，複数のマイニングプールが結託した場合に計算能力が 51%を超えた場合．

② ハードフォークが発生し分岐が起こった結果，分岐前に 51%を占めていなかったマイニングプールが分岐後に 51%を占めてしまった場合．

2019 年現在において， Proof of Work を採用する如何なるブロックチェーンでは①②いずれの場合でも攻撃が起こり得る問題である．特に，②における状況は，形成されたブロックチェーンが多数のノードと計算能力を集められなかった場合でも必然的に発生するため，新規サービスを立ち上げる際に留意する必要がある．

5.2 クリプトジャッキング

ブロックチェーンで利益を得る場合マイニングが不可欠だが，マイニングには計算資源の確保が必要なため個人での実施ではコストは無視できないほど大きなものとなる．要求される過大なコストに対して，計算能力をネットワークの他人に負担させてマイニングを実施する行為がクリプトジャッキングである．

日本国内では，マイニングスクリプトである Coinhive[7]を Web サイトに設置した結果，警察により検挙される案件が発生し問題となった．Coinhive は CryptoNote[8]プロトコルによって設計されたブロックチェーンで実装された仮想通貨 Monero[9]をマイニングするための JavaScript である．マイナーが Monero をマイニングする場合，自前の計算資源で直接マイニングを行うだけでなく，管理する Web サイト上に Coinhive スクリプトを設置し，サイト訪問者がアクセスするたびにスクリプトをダウンロードさせ，訪問者の PC でマイニングを行うことができる．サイト訪問者は，スクリプト設置者の悪意の有無によらず，Coinhive スクリプトをダウンロード，実行させられることになり，マイニングの際の負担となる計算資源，電力を拠出させられることとなり問題となった．

クリプトジャッキングの成立には，

① JavaScript 等，クライアントサイドで実行可能なスクリプト言語でマイニングが可能なブロックチェーン実装であること

② ブロックチェーンのマイニング利益から，Script 制作・提供に係る手数料が十分期待できること

が背景にある．Coinhive での例では，度重なる Monero のアップデートの結果，ネットワーク全体の計算能力が低下し，価値が低下したため 2019 年 3 月にサービス終了となり終息した．サイバーセキュリティ的な観点から見た場合，マイニングスクリプトはその対象がブロックチェーンのマイニングであり，実行主体がサイトを閲覧したユーザになるため，マルウェアと認識され，各種マルウェア対策ソフトウェアや Firefox 等の Web ブラウザではアクセスブロックが実施されている．

5.3 一時的ブロック隠匿攻撃

ブロックチェーンの生成には十分なハッシュの計算能力が必要である．計算資源を確保した場合に起こる 51%攻撃については 5.1 節で述べたが，分岐によって生じる問題として 一時的ブロック隠匿攻撃（block-withholding attack）が存在する．一時的ブロック隠匿攻撃は，[10]によって提案され[11]にて攻撃の最適化が検討され，攻撃者の計算能力がネットワーク全体の 51%未満であっても攻撃が成立するとして問題となっていた．

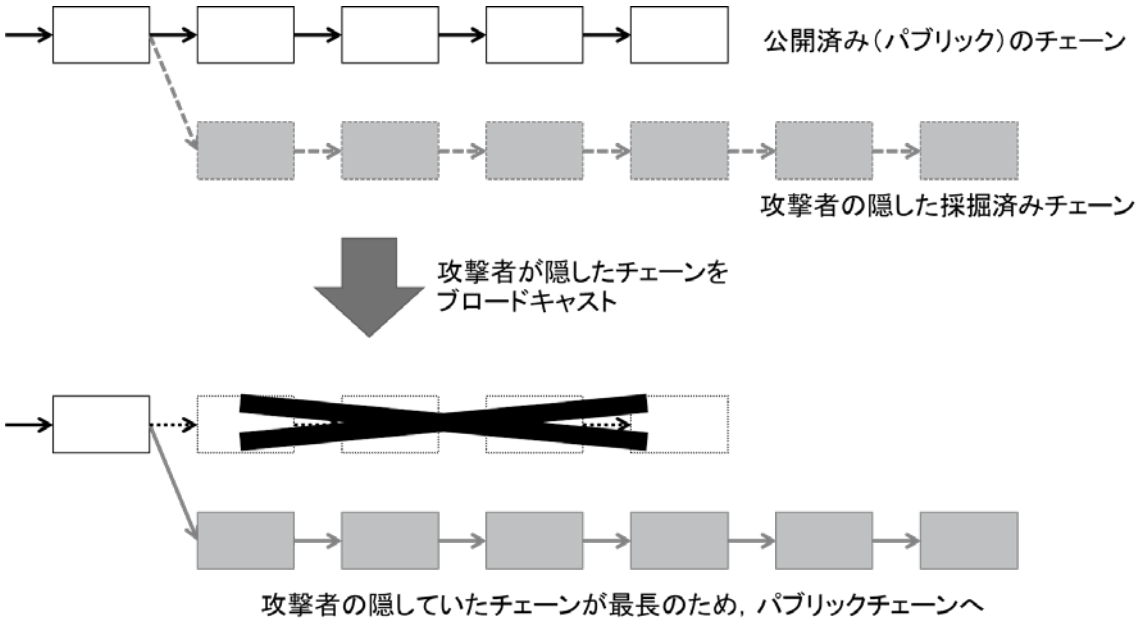


図 3 一時的ブロック隠匿攻撃におけるチェーンの推移

図 3 は，一時的ブロック隠匿攻撃の概要を表したものである．攻撃者は，攻撃する起点となるブロックからブロック生成を行うが，通常ブロック生成時に生成された nonce やハッシュ値をネットワークに公開（ブロードキャスト）する必要がある．しかし，ブロードキャストを行わなかった場合でもブロックは生成できるため，見かけ上は唯一つのチェーンのままでも，ある時点から攻撃者によって隠匿されたブロックが発生し，ネットワーク上から見えない分岐が発生することになる．ブロックチェーンの成立には最長のチェーンが必要なため，時間を経るごとに公開済みのチェーンは長くなっていくが，攻撃者の計算能力が十分ある場合，

十分なチェーンを生成した上で隠匿したチェーンを公開することで，チェーン長が最長となり，既存のパブリックチェーンを無効化することができる．攻撃者は既存のブロックに用いられたハッシュ値に対して，改ざん等の攻撃を試みることなく，またブロック生成の規則に反することなく，既存の同意形成を覆すことができることが本攻撃の脅威である．一時的ブロック隠匿攻撃は，攻撃者の利己的な行為でチェーンを隠匿することから，セルフィッシュマイニングとも呼称される．

一時的ブロック隠匿攻撃が発生した事案として，Monacoin[12]における攻撃事例[13]を述べる．Monacoin は，2014 年にビットコインから派生した Litecoin[14]をベースにしたブロックチェーンによる仮想通貨である． Monacoin ではブロック生成に係る制限時間は 90 秒とされ，マイナーはこの制限時間内に nonce を探す必要がある．また，ブロックチェーンの性質として分岐が発生するため，ブロックの確定には後続する一定数のブロックが必要となる．よって，通貨取引の成立には実際の起案となるブロック生成から一定ブロックの生成の完了まで待つ必要がある．この取引起案から完了までに必要なブロック生成数を承認数と呼び，Monacoin では 18～24 ブロックと定められていた．攻撃者は①事前にブロック生成した事実をブロードキャストせずにチェーン生成を行ってチェーンを伸ばし，②Monacoin の取引所に対して， 攻撃者の保有する Monacoin を別の仮想通貨に換金する取引を確定させた後，③セルフィッシュマイニングを実行して隠匿したチェーンで確定した自身の取引を含むチェーンを無効化した．この結果，取引所は攻撃者に対して換金先の通貨を支払うだけでなく，攻撃によって無効化された Monacoin の利用も払い戻すこととなり二重支払いが発生することになった．

攻撃の背景に存在する問題としては，①攻撃が成立するための計算能力の確保は，サービス規模が十分でないほど容易に確保できること，②ブロックチェーンの分岐の性質上，取引の確定は確率的であること（確率的ファイナリティ）がある．攻撃の発生後，仮想通貨取引所は一時的に必要な承認数を引き上げ，後者の問題に対する対応を行った．

6. 結言

ブロックチェーンは暗号技術と分散ネットワーク技術を活用した新たなデータベース技術として提案された．既に多数の応用が提案され，現在も新たな研究への取り組みが行われているが，実装・運用上での問題点は 5 節で述べた通り多数の問題が存在する．新たなブロックチェーンを活用するサービスを構築する前に理論的な検証と概念実装を行うことは当然であるが，サービス提供に至るまでは技術的な点よりも現実的な計算能力の確保等，解決すべき課題が残っていることに留意する必要がある．

参考文献

[1] Satoshi N., “Bitcoin: A Peer-to-Peer Electronic Cash System”, Available at https://www.bitcoin.org/bitcoin.pdf , 2009

[2] “ブロックチェーン技術を利用したサービスに関する国内外動向調査”, 経済産業省, 2016. https://www.meti.go.jp/press/2016/04/20160428003/20160428003.pdf

[3] 岡本龍明, “現代暗号の誕生と発展 ポスト量子暗号・仮想通貨・新しい暗号”. 近代科学社, 2019.

[4] Hans Dobbertin and Antoon Bosselaers and Bart Preneel, “RIPEMD-160: A Strengthened Version of RIPEMD”, In: Gollmann D. (eds) Fast Software Encryption. FSE 1996. Lecture Notes in Computer Science, vol 1039. Springer, Berlin, Heidelberg

[5] "Secure Hash Standard (SHS)", FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 180-4, National Institute of Standards and Technology, 2015

[6] Roop Gill, "CEX.IO Slow to Respond as Fears of 51% Attack Spread", 2014, https://www.coindesk.com/cex-io-response-fears-of-51-attack-spread

[7] S. Eskandari, A. Leoutsarakos, T. Mursch and J. Clark, "A First Look at Browser-Based Cryptojacking," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 58-66.

[8] Nicolas van Saberhagen . “CryptoNote Whitepaper”, Available at https://cryptonote.org/whitepaper.pdf , 2013

[9] “Monero - Private Digital Currency”, The Monero Project, https://web.getmonero.org

[10] Ittay Eyal and Emin Gün Sirer. “Majority is not enough: bitcoin mining is vulnerable”. Commun. ACM Vol. 61, Issue 7 (June 2018), 95-102, 2018.

[11] Sapirshtein A., Sompolinsky Y., Zohar A. Optimal Selfish Mining Strategies in Bitcoin. In: Grossklags J., Preneel B. (eds) Financial Cryptography and Data Security. FC 2016. Lecture Notes in Computer Science, vol 9603. Springer, Berlin, Heidelberg

[12] “Monacoin – The first Japanese Cryptocurrency”, Monacoin Project, http://monacoin.org

[13] 星 暁雄, “仮想通貨モナコインへの攻撃が明らかにしたこと、今後すべきこと”. Impress 仮想通貨 Watch. https://crypto.watch.impress.co.jp/docs/event/1125410.html , 2018.

[14] “Litecoin - The Cryptocurrency For Payments”, Litecoin Project, https://litecoin.org