ブロックチェーンのデータ構造と動作原理

小出俊夫　Toshio Koide　NEC セキュリティ研究所

1 はじめに

「ブロックチェーン」が何を意味しているかは，人により大きく異なるだろう．ブロックと称するデータの「かたまり」がチェーン状につながったデータ構造のことや，そのデータ構造を維持する分散システムのことかもしれない．はたまた，データを改ざんできない魔法のようなデータベースや，世の中を大変革してしまう技術のことかもしれない．ここではそのどれが正解であるかは追求しないが，少なくともブロックチェーンという用語を有名にした「ビットコイン」の目的を通して，その意味の輪郭をつかみ取ることはできるだろう．

ビットコインは，インターネット上の支払いシステムである．「サトシ・ナカモト」と称する人物が，ある暗号関係のメーリングリストで発表 [(1)] した論文 [(2)] のアイデアを元に有志が実装し，2009 年 1 月から現在まで動作し続けている．

ビットコインの目的は，第三者を介さずにインターネット上の支払いを可能にすることである．第三者とは例えば銀行に代表される金融機関が該当する．金融機関は不特定多数との取引を安心して行えるよう信用の維持と利用者の保護を図る必要があり，日本では金融庁や財務局の免許や許可の下でサービスを提供している．その安心と引換えに，ルール遵守や信用維持には少なくないコストが掛かっており，厳重な本人確認や送金額の制限，各種手数料の高さなどとなって現れてくる．

ビットコインの主な貢献は，皆が第三者を必要とせずにネットワーク全体を信用する状況を作り出す，トラストレス（trustless）の分散型信用基盤を実現したことにある．これによって，第三者の制約を受けずに誰でも（IoT 機器や AI など人間以外も）口座を持ち，世界をまたがり自由に安心して送金できる状況を作り出した．その一方で，例えばエネルギー効率やトランザクション性能は従来の分散データベースと比較にならないほど劣っている．

しかしその貢献には，性能の悪さをカバーするのに十分なインパクトがある．ビットコインやブロックチェーンが注目される理由は，信用の源泉が変化し様々な発展性と可能性をもたらす社会的インパクトと，それを実現させる技術的インパクトと，投機対象として魅力的価値を持つに至った経済的インパクトが背景にあるとみてよいだろう．

例えば，国籍不明のロボットがインターネット上で自律的にお金を稼ぎ，本人の証明ができず銀行口座を開けない難民の子供たちへ，直接，国際送金して寄付をすることも可能になる．更に，ビットコインでは送金を権利移転として表現するので，これを一般化し，特許，著作権，登記などの権利管理に広げれば，関連する団体や組織といった第三者をプログラムに置き換えて自動化・無国籍化する可能性もある．また，裏付けを持たない単なるビット列が価値を持ち，投機の対象となった事実も驚嘆に値する．

ビットコインの一般的な技術の解説は文献（3）に譲り，本解説記事では，ブロックチェーンの技術的インパクトの理解を深めることを目的とし，**2.** でビットコインのデータ構造と権利移転機能の応用の一つとしての送金の表現，**3.** で二重支払いや改ざんの問題に第三者を介さずに対処するビットコインの巧妙な動作原理をそれぞれ解説し，その知識を元に **4.** でブロックチェーン全般の今後の応用や課題について触れる．読者のブロックチェーンに対する理解を，ビットコインの構造と動作原理の理解を通して深めることができれば幸いである．

2 データ構造と表現

2.1 秘密鍵で作る口座

ビットコインには公開鍵のハッシュ値を文字列表現したビットコインアドレスというものが存在する．例え

ば，「1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa」は，ビットコイン上で初めて記録されたビットコインアドレスである．ビットコインアドレス A は次のように求まる．

$$K = \text{'0x04'},\mathrm{ECDSA}(k)$$
$$A = \mathrm{Base58Check}(\text{'0x00'},\mathrm{RIPEMD160}(\mathrm{SHA256}(K)))$$

ここで，k は 256bit の秘密鍵，K は secp256k1 をパラメータとする楕円曲線暗号を用いた署名アルゴリズム ECDSA の出力 512bit の前に 8bit のプレフィックスとして非圧縮を意味する 4 を追加した 520bit の公開鍵，Base58Check は入力にチェックサムを加えて人間が扱いやすい文字列にエンコードする関数，RIPEMD160 と SHA256 は暗号学的ハッシュ関数である．

ビットコインアドレスは口座にたとえられる．口座の基本的な要件である口座の開設は秘密鍵の生成，暗証番号や銀行印は秘密鍵，口座番号は秘密鍵に対応するビットコインアドレスに相当する．ビットコインアドレスからは秘密鍵を生成できないので，送金先として安心して公開できる．なお，秘密鍵は暗証番号や銀行印のような気軽さでは変更できないため，新たなビットコインアドレスを作って対応する．秘密鍵は誰でも自由に作成でき，誰が持っているかを記録することもないため，ビットコインアドレスの所有者の確認が困難である点は，銀行口座の要件とは大きく異なる点である．

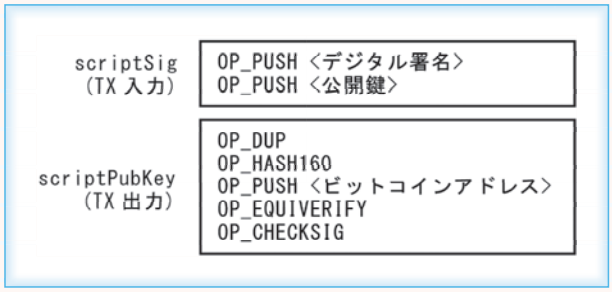

図 1　P2PKH 形式のスクリプト

2.2　UTXO による残高の表現

ビットコインの基礎となるデータ構造は，UTXO（Unspent transaction output）である．UTXO はビットコインの量と，scriptPubKey というフィールドを含んでいる．ビットコインの量は最小単位である satoshi で表現する．10^8 satoshi = 1 BTC である．scriptPubKey は，Locking Script とも呼ばれるスタックベースのスクリプトである．

2019 年 12 月現在，ビットコインのネットワーク上には有効な UTXO が約 1 億個存在し，誰でも読み取ることができるが，誰でも使用できるわけではない．そのビットコインを使用できるのは，scriptPubKey の前方に Unlocking Script とも呼ばれる scriptSig スクリプトを付け加えて実行した結果が True になるときに限る．

スクリプトには幾つかの慣例がある．P2PKH（Pay to Public Key Hash）と呼ばれる形式を図 1 に示す．動作手順の解説は文献（4）に譲るが，この二つのスクリプトを連結して実行した結果を True とするのは，scriptPubKey に指定されたビットコインアドレスに対応する秘密鍵によるディジタル署名と公開鍵を scriptSig に指定した場合のみである．すなわち，ビットコインアドレス A は対応する秘密鍵 k を持つ者への支払先のように利用でき，scriptPubKey 内に A を含む UTXO のビットコインの総和を A の残高と表現できる．つまり，全ての残高は全て公開されており，この特徴は銀行の残高の秘匿性の要件とは大きく異なるところである．

P2PKH 以外にも様々な表現が可能である．ビットコインのスクリプトはチューリング完全ではないが，チューリング完全なプログラム（スマートコントラクトと呼ぶ）を記述可能な Ethereum に代表されるプラットホームも存在する．

2.3　トランザクションによる送金の表現

scriptPubKey の書かれた UTXO と，その使用権を主

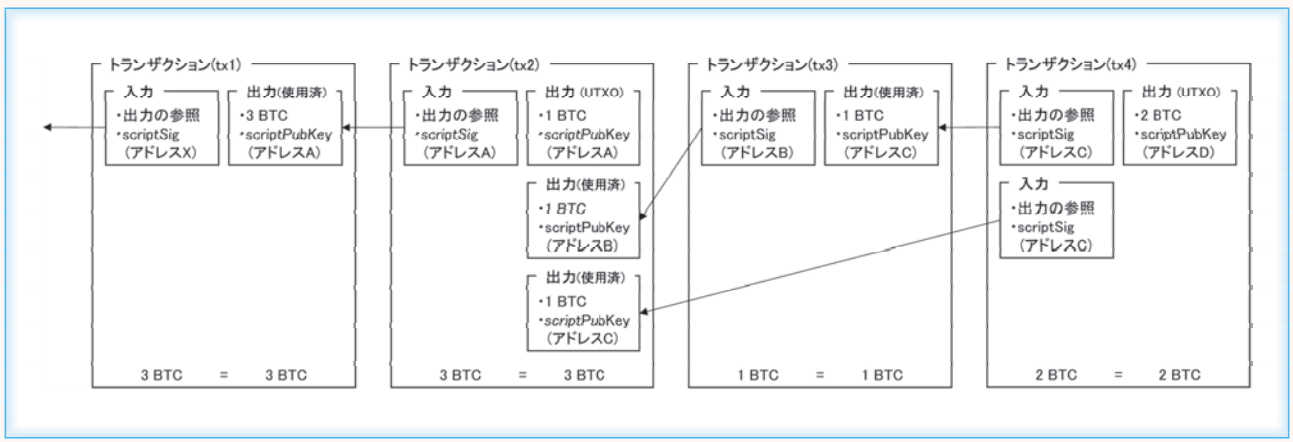

図 2　UTXO とトランザクションの例

張する scriptSig は，それぞれ個別のトランザクションというデータ構造に記述される．トランザクションは，一つ以上の入力と出力を含み，入力は UTXO への参照と scriptSig，出力は新規の UTXO である（図 2）．入力の scriptSig が正しければ，参照された出力は UTXO から使用済み出力へ変化する（図 2 の tx2 を参照，矢印は参照関係を示す）．

トランザクションの出力のビットコインの総量は，後述の例外を除き，入力で参照した他のトランザクションの出力のそれを超えてはならないというルールがある．一般的に送金は，送金元から引かれる額よりも送金先に到達する額が増えてはならない要件があるが，この特徴を用いれば，自分が使用できる UTXO のビットコインの総量の範囲内で，相手が使用できる UTXO を作ることでこの要件を満たし，ビットコインにおける送金を表現できる．

例えば，図 2 の tx1 の作成時には UTXO が一つあり，ビットコインアドレス *A* を含んだ scriptPubKey が 3 BTC とともに存在していた．このとき，*A* には 3 BTC の残高があるとみなされる．次に，*A* の秘密鍵を持つ者が tx2 を書いた．入力の scriptSig が正しければ，参照された tx1 の UTXO は使用済み出力となる．tx2 には UTXO が三つあり，それぞれビットコインアドレス *A*，*B*，*C* を含んだ scriptPubKey が 1 BTC とともに存在している．これは，*A* の 3 BTC を使って *B* と *C* へ 1 BTC ずつ送金し，お釣りを *A* に戻したことを意味し，*A*，*B*，*C* それぞれに 1 BTC の残高があるとみなされる．同様に tx3 は *B* から *C* へ 1 BTC 送金し，tx4 は *C* から *D* へ 2 BTC 送金したことを意味する．ここで，tx2 は一つの UTXO を分割し，tx4 は複数の UTXO を一つに統合した例であり，最終的に *A* に 1 BTC，*D* に 2 BTC の残高があるとみなされる．

2.4　ブロックチェーンによる履歴管理

トランザクションは，ブロックと呼ばれるデータ構造に書かれる．ブロックには，一つ以上のトランザクションと，一つ前のブロックへの参照が含まれている（図 3）．ブロックの参照には ID を用いるが，ブロック内には ID のフィールドはなく，ブロックのヘッダに対して暗号学的ハッシュ関数を 2 回適用した値を ID として使用する．

> ブロック ID = SHA256（SHA256（ブロックヘッダ））

図 3 右下のように，ブロックは参照によって過去に向かってつながった木構造となり得るが，最終的には後述の手法によってその中から 1 本のチェーンが選択されるような構造に収束することから，これをブロックチェーンと呼んでいる．

ブロック内のトランザクションを一部分でも書き換えると，ヘッダに含まれるマークル木のルートハッシュが変化し，定義に従いそのブロックの ID も変化する．すると，その次のブロックが参照するブロック ID と不一致になる．よって，ブロック ID さえ保持しておけば，そのブロックまでに含まれる全てのトランザクションに対して，後から改ざんされたかどうかを検証できる．送金や残高の履歴管理の一般的な要件として求められる改ざん検知はこのようにして実現されている．

また，全ての UTXO はブロック内のトランザクションの出力に含まれている．もう一つの要件として，それらの履歴と最終的な残高の整合が取れていることが挙げ

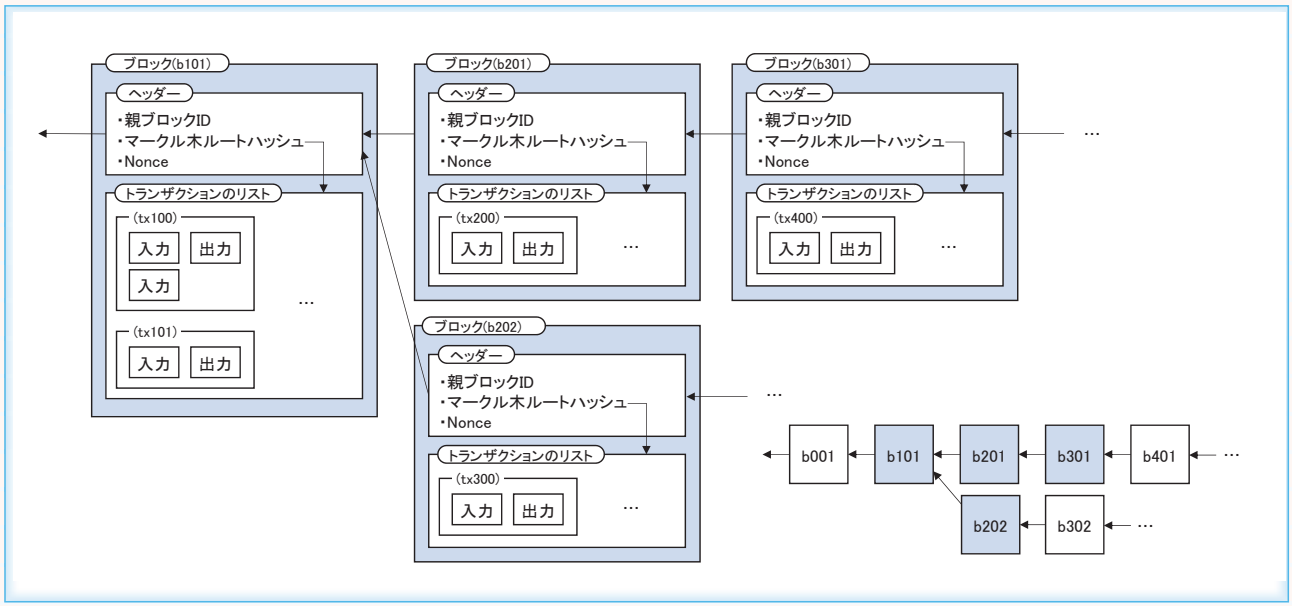

図 3　ブロックとブロックチェーンのデータ構造

られるが，アドレスの残高や送金の履歴は，ブロックチェーンを最初から順番に読み取ってトランザクション間の関係を追い掛けていくことで表現でき，誰にでも追跡可能であり，その計算結果が現在の残高として表現されるのでそもそも整合を取る必要がなく，要件は満たされている．

2019 年 12 月現在，ビットコインのブロックチェーンとして，60 万個以上のブロックが存在している．初めて作成されたブロックは genesis ブロックと呼び，2009 年 1 月に作られた．全てのブロックは，過去に遡ると必ず genesis ブロックにたどり着く．

3　第三者を介さない仕組み

3.1　利用者が提供者にもなるシステム

ビットコインには，公式の実装も，公式の Web サイトも存在しないし，そもそも発案者のサトシ・ナカモトが誰なのかも分かっていない．そして，ビットコインの仕組みそのものも，P2P（Peer-to-Peer）技術を応用し，徹底的に第三者に依存しないシステムになっている．P2P 技術は，第三者に相当する中央サーバやクラウドの代わりに，ノードが互いに同等な仲間（Peer）として接続し合うネットワーク構造を作り，全体として一つの目的を達成可能とする技術である．ノードは参加も脱退も自由だが，ネットワーク全体としては与えられたサービスを維持するように各ノードが協調動作する．

ビットコインはこの P2P 技術を応用し，サービスの利用者としてのノードが，同時にサービスを提供する側の一部に組み込まれるよう設計されている．あなたがビットコインのプログラムを起動すると，世界のどこかで誰かが動かしているビットコインのプログラムと接続する．そしてそのノードに他の接続先を聞いて，更に多くのノードと接続する．こうして，あなたのノードもビットコインのネットワークの一部として動作し始める．ブロックチェーンを構成するトランザクションなどのデータは，このネットワーク内でコピーされて維持される．2019 年 12 月現在，世界中で 1 万前後のノードによって，ビットコインネットワークが維持されている．

3.2　ビットコインが解決する重要な問題

ここで，そのコピーされるトランザクションが全て同一ではなく，悪意をもって本物とは異なったデータにしてコピーするノードがいたらどうなるだろうか．例えば図 4 にあるように，アドレス *A* からあなたが所有するアドレス *B* へ送金するトランザクションが入ったブロック Y を見て，あなたは納得して *A* の所有者へサービスを提供したとする．しかし *A* の所有者はブロックをわざと二つに分岐させており，あなた以外には，あなた宛に使われていたはずの UTXO を使って *C* 宛に送金するトランザクションを含めたブロック Z を送信していた．もしブロック Z が世界中に拡散するとそれが正しい履歴となり，ブロック Y の方は無効となり，あなたは無料でサービスを提供したことになってしまう．

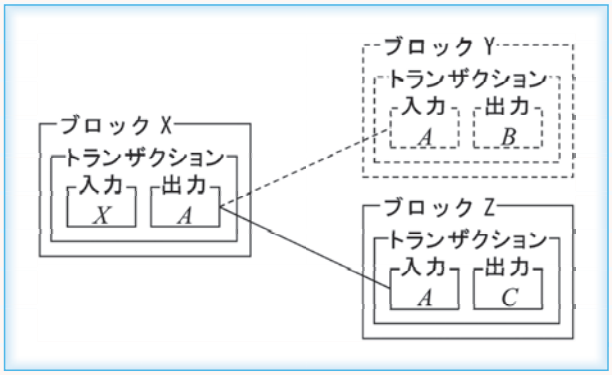

図 4　二重支払いの例

これは，ネットワークを分割してブロックの追加（ねつ造）と削除（隠滅）を行った例であるが，時間差を使ってもブロックの変更（改ざん）を行うことができる．例えば，あなたのノードが，ブロック Y をいち早く同期して手に入れたとする．その後，送金者はブロック Y をブロック Z に改ざんしたとする．あなたはその検知ができてもその行為を止めることはできない．同期が遅れて改ざん後のコピーを初めて受け取ったノードからすれば，ブロック Z が正当に見える．こんなシステムでは安心して使うことができない．

この問題は「二重支払い問題」と呼ばれるが，全てのノードが一本に収束したブロックチェーンを全ての瞬間で完全に同期して持っていれば解決する．だが，そんなことを実現する方法がビットコインには実装されているのだろうか．答えは現時点では「ノー」である．現在のビットコインは改ざんの定義を少し変えることで，この問題を事実上解決している．

3.3　ビットコインにおける悪意の定義

システムとしてはデータの変更にすぎない操作が改ざんと呼ばれるのは，そこに悪意が介在するからである．第三者に紛争解決を求めることを放棄するならば，システムが人間の「悪意」を客観的な数値で判定し自動的に解決しなければならないが，ビットコインは多数派に反することを悪意とみなすこととした．木構造状に分岐するブロックから多数派が 1 本のチェーンを選択するとき，それ以外のチェーンの作成や選択はこの定義のおかげで悪意と判定できる．

多数派を決めるために，ビットコインでは PoW (Proof of Work) [5], [6] を用いる．ビットコインにおけ

るPoWとは，ブロックIDが一定の範囲内に収まるときのブロックのヘッダのNonceのことである．Nonceとは，ブロックヘッダに含まれる4Byteの数値であり，値そのものには意味を持たないが，Nonceが少しでも変化するとブロックID（前述のブロックヘッダを入力として暗号学的ハッシュ関数を2回適用した値）が全く違う値に変化する．暗号学的ハッシュ関数の特徴である原像困難性（与えられたハッシュ値に対応する入力を見つけることが困難な性質）によって，条件に合うNonceは条件を満たすまでその値を変化させながらブロックIDの計算を繰り返すよりほかに見つける方法がない．

この性質により，そのブロックIDが一定の範囲内に入っているときのブロックヘッダのNonceは，その計算をし続けたことの証明となる．与えられたNonceが条件に一致しているかは素早く検証できるが，条件に一致するNonceの発見には時間が掛かる．2019年12月現在，ビットコインのネットワーク全体がたたき出すことが可能な計算回数は毎秒10^{20}回前後と推定されており，その力を持ってしても条件に合うNonceを発見するまでには平均10分ほど掛かる．（そうなるようにブロックIDの一定の範囲が自律的に調整される．）

ここで，一つの興味深い現象が発生する．チェーンの選択基準が同一なノード集合は，ノードのどれがNonceを発見しても同じ基準のチェーンを選択するから，結果的に一つのグループとしてまとまっていくのである．Nonceの発見は確率的なので同一グループのノードが同時に計算するとNonceの発見も早まる．そのため，最大の計算能力の総和を持つグループが最も素早くチェーンを伸ばしていくことになる．結果として，ビットコインネットワークにおける多数派は，同一のチェーン選択基準を持った，計算能力の総和が最も大きいノードグループということになる．よって，安定して信用できるビットコインネットワークを形成するには，チェーンの選択基準を収束させることが重要となる．

3.4　人間の欲望がチェーンを収束させる

ブロックには入力のないトランザクションを含められるというルールがある．出力量に一定の制限が存在するが，ノードはUTXOを自分のアドレス宛にした入力のないトランザクションをブロックに含めることで，そのノードはビットコインを発行して自分で所持できる．

実はこのルールによって，人間の欲望とチェーンの選択基準がつながる．大変な思いをして運良くNonceを発見し有効なブロックを作成したノードの運用者は，そのブロックによってビットコインを発行した事実をより強固にブロックチェーンに刻みたいと考えるのが自然である．そのためには自分の作ったブロックの後ろに多数のブロックが連なってほしいし，他のノードも同じ動機で動いているという推測が働くので，計算量が最も多く注ぎ込まれかつ有効なデータ構造を持った，最も覆りにくいチェーンを選択し自分もその作成に寄与することが基準となる．よって，少しでも多くの利益を得たい運用者には，その基準で動作するノードを運用する動機が生まれる．そして，その欲望は人間の大多数に共通しているため，その選択基準が多数派となる．

こうして，ブロックチェーンの分岐が一時的に発生したとしても，計算量が最も多く注ぎ込まれた有効なチェーンに収束し，それ以外のチェーンの選択は悪意であるという基準がネットワークに安定的に生まれ，ノード間の紛争が自律的に解決される．少数派がデータを改ざんするために過去に遡って矛盾なくブロックチェーンをつなごうとしても，それを上回るスピードで多数派によるブロックチェーンが成長するため，データの改ざんが事実上不可能となる．もちろん，多数派を牛耳れば過去のトランザクションの変更は可能だが，多数派の全てのノードを特定の運用者が牛耳ることは事実上困難であり，データの「変更」も事実上困難となる．

ブロックチェーンが正しく有効なブロックをつないでネットワーク全体で一つに収束することも，改ざんが事実上不可能となることも，ノードを運用する人間の利益を得たいという欲望によって結果的に起こっている振る舞いにすぎない．人間の欲望が改ざんできないブロックチェーンを安定的に維持する力となって今も動き続けているのであって，これは驚くべき事実である．

4　これからのブロックチェーン

4.1　技術的な課題

ブロックチェーンの技術的な課題として，スケーラビリティはよく話題に挙がる．例えば，ビットコインが処理できるトランザクションが実質的に1秒間に約4件で頭打ちとなる問題があるが，これはブロックの承認頻度が10分ごとでサイズ上限が1MByteであることに原因がある．Litecoin [7] のようにブロックのサイズや承認回数を増やせば処理性能は向上できるが，それと引換えに改ざん耐性の劣化やDDoS攻撃などのセキュリティリスクが高まる．そこで，チェーンの選択基準 [8] や，ネットワーク層の改善 [9] を通して，セキュリティリスクを緩和する方法や，トランザクションのサイズを圧縮する方法 [10], [11] が提案されている．

また，エネルギー消費に関する議論も盛んである．例えば，PoWのために全世界で大量のエネルギーが消費されている問題がある [12], [13]．現在のエネルギー消費

の推計を可視化するサイトもあり[14]，これによれば2019年12月現在のビットコインネットワーク全体の消費電力は約73TW･h，全世界の電力消費の約0.3%，日本の電力消費の約7.8%に相当する．この問題を解決するため，PoWではなくPoS（Proof of Stake）[15],[16]という通貨の保有量や年齢の証明，PoI（Proof of Importance）[17]という重要性の証明を活用してチェーンを収束させるブロックチェーンを構築する動きがあるが，これもセキュリティとのトレードオフの解決が課題となっている．

セキュリティそのものの研究もある．例えば，量子コンピュータの発展により暗号学的ハッシュ関数や楕円曲線暗号が危たい化し安全性が保たれなくなる問題への対処を目指した，量子コンピュータに対する耐性を持ったブロックチェーンの研究がある[18],[19]．また，ビットコインには管理者がいないのでどの改善手法を選択するかは利用者次第であり，互換性のない実装を持ったノードが同時に存在しつづけた結果，恒久的にチェーンが分岐するハードフォーク（Hard Fork）という現象が発生することもある．これは悪意の定義が異なるネットワークができたことを意味する．例えば，スケーラビリティの改善手法に関する対立によってビットコインキャッシュ[20]などの新たな暗号資産が誕生しており，これは技術の発展や多様化の一現象である．また，The DAOの資金流出事件への対応でEthereumの歴史を巻き戻すために起こったハードフォーク[21]は，第三者が強制的に介入した改ざんという見方も，善意の資金流出を悪意とみなす多数決によって善悪が変化したという見方もできる例である．

その他の話題も含めて最新情報を追うには，コミュニティの中でどのような議論がされているのかを知るのが一番である．ビットコインの改善提案を行う場としてBIP（Bitcoin Improvement Proposals）[22]や，開発者コミュニティの中でアイデアを議論できるメーリングリスト[23]などがインターネット上に存在する．また，ブロックチェーン関連の各種ワークショップ[24],[25]もある．オンライン・オフラインで技術的な議論や人脈を形成することも効果的な情報収集につながるだろう．

4.2　ビットコイン以外への応用

ビットコインのブロックチェーンとは，人間の欲望によってインターネットに浮かび上がったUTXOという価値の塊，すなわちビットコインの価値そのものと表現できるだろう．この価値をビットコイン以外へと一般化し，分散型の信用基盤としてブロックチェーンを成立させるには，少なくとも次の三つが注意深く設計されていることが望ましい．①は**2.**，②と③は**3.**で解説したビットコインが成立するための仕組みの本質に相当する．

①扱うべき価値とその表現方法
②サービス利用者の活用すべき動機
③①と②から継続性や改ざん耐性への変換方法

有望な応用の一つに特許，著作権，登記などの権利管理の自動化がある．権利はお金の価値と近く，人間には権利を欲するという共通の動機があるため，ビットコインのブロックチェーンと類似した設計で，分散型の信用基盤を構築できる可能性が高い．

ブロックチェーンを暗号資産以外に有効に応用できた例はまだ少ない．ブロックチェーン活用をうたう実証実験が散見されるが，新しい目的に適った分散型の信用の設計が不完全で第三者の信用を部分的に借りる必要があるか，そもそも目的が第三者の排除を前提としておらず，ブロックチェーンではなくクラウド上に実装した方が目的を効率的に達成できる場合が多い．

ブロックチェーンの良い応用例を生み出すには，ブロックチェーンの技術や性質をベースにアイデアを発想するよりは，第三者を介さずに信用が分散して存在する世界をベースに技術や常識抜きに発想したほうがよい．しかしそれは往々にして何らかの利権構造を破壊する結果につながるので，サトシ・ナカモトに倣ってその導入においても徹底的に第三者を排除する配慮が必要となるだろう．若しくは，最初は小さなコミュニティの中で楽しく使うだけでもよいかもしれない．その有用性に気付いたコミュニティの外の人たちよって肯定的に広く普及していく可能性もあるからだ．

■ 文献

(1) S. Nakamoto, “Bitcoin P2P e-cash paper,” Nov.2008, https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html
(2) S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” http://www.bitcoin.org/bitcoin.pdf
(3) A. M. Antonopoulos, “Mastering bitcoin: unlocking digital cryptocurrencies,” O'Reilly Media, Inc., Sebastopol, CA, 2014.
(4) https://en.bitcoinwiki.org/wiki/Pay-to-Pubkey_Hash
(5) A. Back, “Hashcash - a denial of service counter-measure,” Aug.2002, http://www.hashcash.org/hashcash.pdf.
(6) M. Jakobsson and A. Juels, “Proofs of work and bread pudding protocols,” in Secure Information Networks, pp.258-272, Springer, Boston, MA, 1999.
(7) “Litecoin, open source P2P digital currency,” https://litecoin.org
(8) Y. Sompolinsky and A. Zohar, “Secure high-rate transaction processing in bitcoin,” in International Conference on Financial Cryptography and Data

Security, pp.507-527, Springer, Berlin, Heidelberg, 2015.
(9) I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-ng: a scalable blockchain protocol,” 13th USENIX Symposium on Networked Systems Design and Implementation, pp.45-59, 2016.
(10) E. Lombrozo, J. Lau, and P. Wuille, “Segregated witness (consensus layer) ,” https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
(11) J. Poon and D. Thaddeus, “The bitcoin lightning network: scalable off-chain instant payments,” https://www.bitcoinlightning.com/bitcoin-lightning-network-whitepaper/
(12) C. Stoll, L. Klaasen, and U. Gallersdorfer, “The carbon footprint of bitcoin,” Joule, vol.3, no.7, pp.1647-1661, July 2019.
(13) M. J. Krause and T. Tolaymat, “Quantification of energy and carbon costs for mining cryptocurrencies,” Nature Sustainability, vol.1 no.11, pp.711-718, Nov. 2018.
(14) “Cambridge bitcoin electricity consumption index,” https://www.cbeci.org
(15) “Nxt whitepaper,” https://nxtwiki.org/wiki/Whitepaper:Nxt
(16) S. King and S. Nadal, “PPCoin: peer-to-peer crypto-currency with proof-of-stake,” https://www.peercoin.net/whitepapers/peercoin-paper.pdf
(17) “NEM - Distributed ledger technology (Blockchain) - Harvesting & poI,” https://nem.io/xem/harvesting-and-poi/
(18) K. Ikeda, “qBitcoin: a peer-to-peer quantum cash system,” Science and Information Conference, pp.763-771, Springer, Cham, July 2018.
(19) E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, “Quantum-secured blockchain,” Quantum Science and Technology, vol.3 no.3, 035004, July 2018.
(20) https://www.bitcoincash.org
(21) V. Buterin, “Hard fork completed,” https://blog.ethereum.org/2016/07/20/hard-fork-completed/, July 2016.
(22) “Bitcoin improvement proposals,” https://github.com/bitcoin/bips
(23) https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev
(24) “Scaling bitcoin workshops,” https://scalingbitcoin.org/
(25) “Devcon,” https://devcon.org/

小出俊夫（正員）

2004 創価大大学院博士後期課程了．博士（工学）．同年 NEC 入社．OpenFlow 等の分散ネットワーク制御の研究，北米での OSS 開発を経て，帰国後は IoT やブロックチェーンの研究に従事．2002 年度 C&C 若手優秀論文賞，平 16 年度本会学術奨励賞，2013 本会 ICM 研究専門委員会 ICM 研究賞，第 64 回電気科学技術奨励賞各受賞．