学生のページ
Student's page

ブロックチェーン技術
～学生の視点から現状と期待～

取材／**村松久圭**（慶應義塾大学），**薗部達哉**（千葉大学），**東山和寿**（早稲田大学），**松野俊文**（横浜国立大学），**松本哲明**（芝浦工業大学）
エディタ／**名取賢二**（千葉大学）

ブロックチェーン，コンセンサスアルゴリズム，ビットコイン

1．はじめに

インターネットが大きく普及した現在，IoT（Internet of Things）をはじめとするインターネットを応用したさまざまな技術が注目されている。ブロックチェーン技術もまたネットワーク環境を利用した技術の一つであり，さまざまな取引へ信頼性を与える技術である。ブロックチェーン技術の代表的な適用先としてはビットコインが有名である。ブロックチェーンを用いたビットコインの特徴を，法定通貨および電子マネーと比較してまとめたのが**表 1** である。ビットコインのはじまりは 2008 年における Satoshi Nakamoto によって投稿された論文[1]であり，2009 年に運用が開始された。その後現在までビットコインのシステムは停止状態になったことはなく，これはゼロ・ダウンタイムとも呼ばれている。

さらに近年，ブロックチェーン技術はビットコインにとどまらず後述するシェアリングエコノミーやスマートコントラクトなどへの応用も進められている。特にビットコインのブロックチェーンでは下記の三つのメリットが注目されている。

・データの改ざんが困難な信頼性
・取引の透明性と匿名性
・中央管理者を必要としない合意形成

本稿では野村総合研究所への取材（**図 1**）で得られた知見をもとにブロックチェーン技術を紹介し，学生の目線からブロックチェーンの今後の応用について提案したい。構成として，まず第 2 章でブロックチェーン技術の仕組みを紹介する。次に第 3 章でその応用を紹介し，学生の目線か

共享經濟　　智能合約

図 1　インタビュー風景

表 1　ビットコイン，法定通貨および電子マネーの特徴[2]

	特徴	ビットコイン	法定通貨（日本円）	電子マネー（第三者型前払式支払手段）
発行・管理	発行者	■システム	■日本政府（通貨） ■日本銀行（紙幣）	■電子マネー事業者（第三者型前払式支払手段）
	管理者	■ P2P ネットワーク参加者	■日本政府 ■日本銀行	■電子マネー事業者（第三者型前払式支払手段）
価値	発行上限数	■決まっている（2,100 万 BTC）	■なし	■事前入金された金額の範囲で発行
	価値の裏付け	■システムへの信用	■日本政府への信用	■供託された日本円（入金額の 1/2） ■電子マネー事業者への信用
送金処理	送金の方向	■双方向	■双方向	■一方向（利用者⇒加盟店）
	送金の処理時間	■約 10 分間隔でブロックを作成 ■約 60 分で確定と見なす	■直接の受取であれば即時 ■長距離・大量だと時間がかかることもある	■加盟店に支払われるまで数日～ 1.5 か月程度
	送金の手数料	■少額 ■送金者負担	■高額 ■場合によって両方負担	■受取者（加盟店）負担
匿名性	取引の匿名性	■取引履歴は明らかだが，匿名性がある	■高い	■低い（履歴は電子マネー事業者が管理）
	取引履歴の公開	■公開	■非公開	■一般に非公開

ら提言する今後の発展と応用について第4章で述べる。

2. ブロックチェーンの仕組み

2.1 ブロックチェーンとは

ブロックチェーンとはP2P（Peer-To-Peer）ネットワーク上に形成され，一定時間ごとに形成されるブロックが時系列順につながりを持ったデータ構造である。P2Pネットワークは複数の端末間がサーバなどを介することなく直接的に通信を行う方式であり，特定の中央管理者を必要としない特徴を有している。そのためブロックチェーンは中央管理者が保持しているのではなく，P2P参加者全員が各々保持することとなる。ブロックチェーンは物事の遷移（トランザクション）を記録することが多いため，このような形態を分散型台帳と呼ぶ。次節より，これらの特徴がどのような技術によって保障されているのかを説明していく。

2.2 ハッシュチェーン

ブロックチェーンにおいて，ブロック間のつながりを形成しているのがハッシュチェーンである（図2）。ハッシュチェーンを形成するハッシュは暗号学的ハッシュ関数によって生成された文字列であり，ハッシュ関数は同じ入力に対して常に一定の出力を行う。この際，入力から出力を算出することは容易だが，出力から入力を推測することは数学的に困難であるため，この文字列はIDに似た性質を持つ。つまり，ほんの少しでも改ざんを受けたデータは本来のものとは異なったハッシュが得られるため，データの真正性を検証できる（図3）。

ブロックチェーンの各ブロックは直前のブロックから算出されたハッシュを要素として保持している。ブロックチェーンはすべてのブロックが連なって形成されており，このハッシュが正当なものであるかを遡って検証することができるため，データの改ざんや欠落などの検出が可能である。このようにして，ブロックチェーンは自身の真正性を検証することが可能となっている。

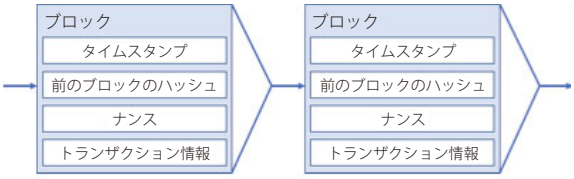

図2　ブロックチェーン[2]

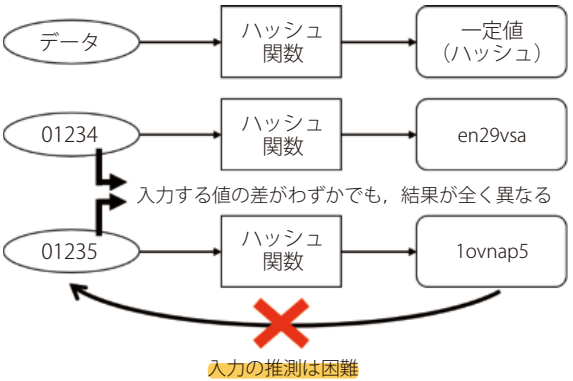

図3　ハッシュ関数[2]

2.3 公開鍵暗号方式とトランザクション

情報の機密性や安全性を高めるための暗号化技術には公開鍵暗号方式が用いられている。この方式では，「本人だけが用いる鍵（秘密鍵）」と「誰でも利用できる鍵（公開鍵）」を用いて暗号化・復号を行う。これらの鍵は対になっており，一方の鍵で暗号化された情報はもう一方の鍵でないと復号はできない（図4）。第三者に閲覧されたくない情報を転送する場合，送信者側は受信者の公開鍵で暗号化した情報を転送し，受信者側は自分の秘密鍵で復号を行うことで平文を得ることができる。したがって，送信中に盗聴があったとしても復号を行うことは困難であり機密性は保持される。

さらに暗号通貨では公開鍵を口座番号，秘密鍵を暗証番号に見立てたユーザ管理も行われる。暗号通貨ではすべての送金履歴が保管されており，トランザクションの中には送金元と送金先のアドレス（公開鍵のハッシュ）も保持される。加えて送金には電子署名と呼ばれる改ざん検出アルゴリズムを必要とするので，本人以外による不正な送金が生じる可能性は極めて低い。そのため，すべてのアドレスに対して正確な出納が参照可能であり，システムの透明性が高いといえる。一方で秘密鍵を公開鍵から推定することは非常に困難であるため，匿名性の確保も同時に達成される。

2.4 コンセンサスアルゴリズム

ブロックチェーン技術は取引履歴であり，各ユーザが保持するブロックチェーンは整合性が取れている必要がある。そこでネットワーク全体で整合性の取れた同一のチェーンを承認／確認する方法がコンセンサスアルゴリズムである。その一手法としてProof of Work（PoW）がある（図5）。

PoWは，解を求めることは困難でも，容易に解の正当性を検証できる作業を課し，悪意のある行動を抑制する方

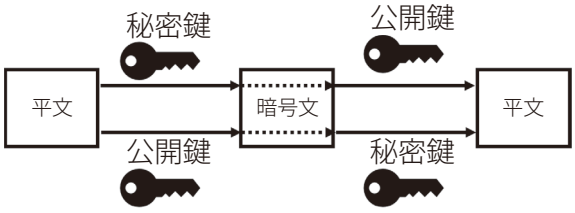

図4　公開鍵暗号方式

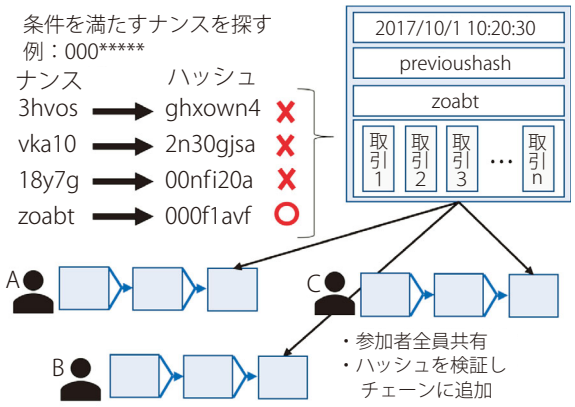

図５　PoW

法である。新たに追加したいブロックをナンスと呼ばれる文字列が欠落した状態で公開し，そのブロックのハッシュが特定の値よりも小さくなるようにナンスを求めさせる。最も早くナンスの導出に成功したユーザは報酬を得て，他の各ユーザもそのハッシュを計算することでブロックの正当性を検証し，問題がなければ自分のブロックチェーンへ追加する。これにより，同一で正当なブロックチェーンを各ユーザが保持する。

ただし，PoW により生成されたブロックチェーンではほぼ同時に計算が成功することにより，一時的に分岐（フォーク）が生じることが想定される。このような場合，ブロックチェーンではブロックが最長のものを正当なフォークとみなす。その理由は，不正を行うには正当なフォーク以上の速度でブロックを生成し続ける必要があり，P2P ネットワーク参加者全体と比べ膨大な計算能力を有する必要があり現実的ではないためである。したがって，仮に不正が行われても最長のものを正当なフォークとみなすことで不正なフォークが通常自然淘汰（とうた）される。また，ハッシュ計算はトランザクションに変更を加えないため，正当なものであればどの計算機によって生成されたブロックを選んでも問題はない。

3. ブロックチェーンのユースケース

「ビットコイン」の基盤となっているブロックチェーン技術は金融のみならず，多くの場面で応用が期待されている。以下にシェアリングエコノミーとスマートコントラクトのユースケースを示す。

3.1　シェアリングエコノミー

シェアリングエコノミーとは個人が保有する遊休資産（スキルのような無形のものも含む）の貸し出しを仲介するサービスのことを指す[3]。つまり個人の所有する資産を使われていない時間帯だけ他人に貸し出し，その資産を有効に活用するサービスである。車や駐車場，空き部屋，労働力，目に見えるものから目に見えないものまであらゆるものが対象となる。

シェアリングエコノミーでは通常貸し出しのやり取りはインターネットを通じて行われるが，そのシステムの構築には非常に高いコストがかかる。例えば車を貸し出す際，本人確認のための個人情報（免許証やパスポート），取引や決済等の記録，利用後の提供者および利用者の評価（口コミ情報）といった膨大な情報を安全に管理する必要がある。そこで，提供者と利用者間の取引や個人情報の管理をブロックチェーン上で行うことで安定したシステムを構築することが可能になる。さらに，取引のみならず，携帯電話から鍵を解除するためのスマートロックや電気自動車が充電するためのコンセント利用権限等の高度なセキュリティー管理が求められる場面において，ブロックチェーン技術の導入が望まれている。新興市場として位置付けられるシェアリングエコノミーだが，ブロックチェーンを導入することで利用拡大が期待される。

3.2　スマートコントラクト

スマートコントラクトはあらかじめ契約条件や執行条件を決めておき取引を自動的に実行する仕組みである。スマートコントラクトの実現にはブロックチェーン技術が得意とする，「真正性が高く（二重支払の防止）透明性が高い（改ざんが困難）」システムの構築が重要である。特に書面としての契約形態をとらない取引において，ブロックチェーンを採用したスマートコントラクトは最適な条件で取引が自動化されるため取引の効率を高めることができる。

例として，ビジネスシーンでは企業間における商品や物流における取引が，行政においてはゴミ量に応じた料金徴収がスマートコントラクトによって自動化されることが期待されている。

これはエネルギー分野においても例外ではない。例えば，住宅における太陽光発電の剰余電力は通常電力会社を介して取引が行われるが，それに対して，ブロックチェーン技術を活用することで，電力会社を介さずに直接住宅間でエネルギー融通を行う取り組みが進められている。消費者と発電事業者間あるいは発電事業者と送配電事業者間の電力取引をブロックチェーン上で行うことで，電力の品質や価格を考慮した複雑な契約の自動的なシステム運用が可能となる。このようにブロックチェーンは消費者や発電事業者が効率的にエネルギーを融通する基盤を確立する技術として期待されている。

4. ブロックチェーン技術応用への期待

本章ではブロックチェーン技術の更なる応用の可能性に

ついて学生の視点から述べていく。

4.1　ブロックチェーンを用いたネット投票システム

日本では投票日が近づくと自宅に投票はがきが届き，投票日（通常，日曜日）になると投票所に出向く必要がある。そしてはがきと交換した投票用紙に支持する候補者の名前を記入し，用紙を投票箱に入れるのが一般的である。しかしながら，休日に投票所へ赴く手間は年々投票率が減少することに対して無視できない影響を及ぼしていると考えられる。そこで，ブロックチェーン技術を用いた高い透明性と高い信頼性を有するインターネット投票システムの導入を期待する。その特性から外部からの集計結果の改ざんも困難であり相性が良い。ネット投票が可能となればネットワーク環境が整っている場所ならどこからでも投票が可能になり，選挙に対する意識の向上や人件費などのコストの削減も期待される。

4.2　ブロックチェーンによる勤怠管理システム

昨今，ブラック企業における長時間労働が深刻になっており，その実体もまたなかなか明るみに出ないことが問題になっている。これは企業における労働時間管理の透明性が低く，信頼性に欠けることが原因の一つとして挙げられる。我々学生にとっても他人事ではなく，いずれこのような状況に直面するかもしれない。勤怠管理では，タイムカードに打刻機で出退勤時刻を印字する方法や，パソコンやスマートフォンなどで画面上のボタンをクリック（打刻）することで出退勤時刻を記録する方法などが一般に用いられる。こうした勤怠管理システムにおいてブロックチェーン技術を用いた新たなシステムが期待される。ブロックチェーン技術を取り入れることで，過剰な労働の有無を第三者機関の介入無く監視することが可能となる。さらに，出退勤時刻が不正に修正される恐れもなくなることが期待される。

4.3　ブロックチェーンによる資金記録

現在の日本では政務活動費の問題をはじめとして公的資金や生活保護の不明使途・不正受給等問題は後を立たない。これらお金の管理については信頼性や透明性が求められるにもかかわらず，資金記録の透明性を確保する環境は十分に整っているとは言いがたい。そこでブロックチェーン技術を利用した資金電子管理が期待される。これにより，公的資金などの取引すべてをブロックチェーンを通して記録し，高い透明性と信頼性を確保した資金管理が可能となる。

4.4　カーシェアリング

シェアリングエコノミーのひとつとしてカーシェアリングへのブロックチェーンの応用が期待されている。カーシェアリングを行うにあたり，利用契約などの情報のやりとりをブロックチェーンに紐（ひも）づけすることで仲介サービスを必要とせず実現することができる。紐付ける情報として，利用契約のみならず保険加入や車の電子キー等すべての取引情報を一括して管理することで，簡潔に信頼性の高い取引が可能となることが期待される。

図６　取材後記念撮影（田中様（左から３番目），山口様（左から４番目）と取材陣）

5. おわりに

本稿では，ブロックチェーン技術を紹介し，さらに学生の視点からその応用例を提案した。既存のシステムとブロックチェーン技術との融合あるいはブロックチェーン技術を用いた新たなシステム，いずれも実現は容易でないことが想定される。しかしながら，第三者を必要とせず透明性および信頼性を有することが可能な本技術は，管理や調査が行き届かず不透明のまま放置されている諸問題の解決策となる可能性のある技術である。これからの人々の暮らしや社会の更なる発展にはブロックチェーン技術が一役買ってくれるに違いない。さらに，これまで我々がインターネットに抱いてきた匿名かつ低い信頼性という印象はこのブロックチェーン技術の台頭によって変化していくことが期待される。

〈謝辞〉最後になりましたが，今回の取材において，ご協力いただきました野村総合研究所の田中大輔氏と山口雷太氏に心よりお礼申し上げます。

文　献

（1）S. Nakamoto：「Bitcoin：A Peer-to-Peer Electronic Cash System」, https://bitcoin.org/bitcoin.pdf
（2）(株)野村総合研究所：「平成 27 年度　我が国経済社会の情報化・サービス化に係る基盤整備（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）報告書」, http://www.meti.go.jp/press/2016/04/20160428003/20160428003-2.pdf
（3）総務省：「ICT が拓く未来社会」 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc242110.html.