情報管理 JOHO KANRI 2017 vol.60 no.3 6 June
Journal of Information Processing and Management
http://jipsti.jst.go.jp/johokanri/

ブロックチェーン(分散型台帳)最新事情
第4次産業革命を牽引する革新的な技術への期待と課題

What blockchain means for the current society?
Expectations and hurdle of revolutionary technology leading the fourth industrial revolution

青木 崇[1]
AOKI Takashi[1]

1 株式会社日本政策投資銀行
1 Development Bank of Japan Inc.

ブロックチェーンはビットコインの中核技術として登場した。ビットコインは2008年にサトシ・ナカモトと名乗る人物がインターネット上に掲載した文書を基に考案された電子通貨である。その背景としては，日進月歩で進化するIT技術に取り残された中央集権型システムの非効率性への不満や，プライバシー情報の取り扱いに関する不信感などがあり，中央集権型システムから個人が中心となる分散型システムへの移行が期待された。分散型システムを機能させるネットワーク技術にブロックチェーンを適用すれば，新たな社会が誕生する可能性がある。一方で，ブロックチェーンに関するさまざまな情報がそれぞれの立場で語られている状況であり，必ずしもビジネス実務や金融業務を正確に把握しないまま，過度にブロックチェーンを礼賛している風潮もあるので冷静な議論が必要である。また，技術的な観点だけではなく，社会科学的なアプローチによる議論の必要性にも言及した。

ビットコイン，ブロックチェーン，分散型台帳技術，フィンテック，インターネット，第4次産業革命，P2P，PoW，ハッシュ値，マイニング

原稿受理（2017-03-21）
情報管理. 2017, vol. 60, no. 3, p. 166-174. doi: http://doi.org/10.1241/johokanri.60.166

1. はじめに

ブロックチェーンに関する報道が増えている。たとえば，福岡県にある産学官民一体のシンク＆ドゥタンクである福岡地域戦略推進協議会は，2017年1月24日，東京海上日動火災保険（東京都千代田区）と，Planetway Corporation（米国カリフォルニア州サンノゼ）の非常にセキュリティーの高いデータ連携技術を活用することで，福岡市内の医療機関などにおけるブロックチェーン技術の活用に向けた実証事業を始めると発表した[1)]。

このように先進的な取り組みが開始されている一方で，報道によっては，ブロックチェーンを正確に理解しないまま記事にしていると思われるものも散見され，ブロックチェーンに関するさまざまな情報が混在している状況である。さらに，ビットコイン（Bitcoin）やフィンテック（FinTech）といった概念が混ざると，何がどうなっているのか理解が難しく，混沌（こんとん）とした状態になっているのではないだろうか。筆者はブロックチェーンの革新的なアイデアは第4次産業革命を牽引（けんいん）するものだと考えているが，ビジネス実務や金融機関の業務を正しく理解しないまま，ブロックチェーンですべてが解決するような論調もあるので，慎重な整理が必要であると思っている。

本稿では，ブロックチェーンに関連するさまざまな言葉が氾濫している中で，まずは情報整理から始め，ブロックチェーンのメリットや応用事例，今後の課題などについて考えたい。

2. ビットコインからみる，ブロックチェーン（分散型台帳）の概念

ブロックチェーンの概念を理解するには，ビットコインの理解から始めなくてはならない。なぜなら，「ビットコインの中核技術」として発案されたものがブロックチェーンであり，ブロックチェーンが単独で登場したわけではないからだ。

2.1 ビットコインとは何か

ビットコインとは，2008年にサトシ・ナカモトと名乗る人物がインターネット上に掲載した文書[2]（**図1**）を基に考案され，2009年1月に運用開始された画期的な仮想通貨である。サトシ・ナカモトが誰なのか，現在でも謎のままである。

さて，ビットコインの技術的な説明の前に，なぜビットコインが登場し現在まで支持されているのか，その背景について触れたい。

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

図1　サトシ・ナカモトによるビットコインの考案文書

2.2 中央集権型機関への不信感や不満の台頭

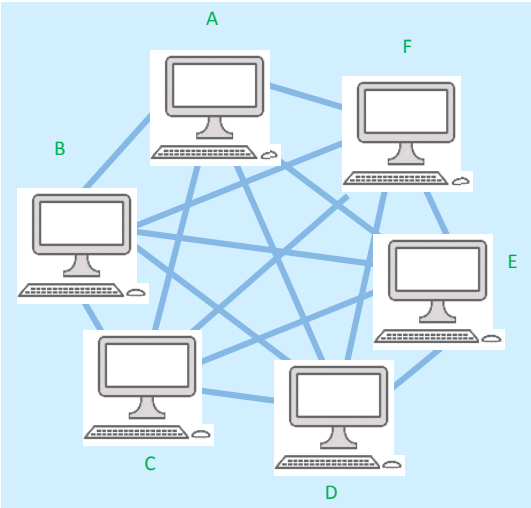
ビットコインが誕生した背景としては，世界的にIT革命が進んでいるにもかかわらず，旧態依然とした中央集権型機関の非効率性への不満や，米国EFF（Electronic Frontier Foundation）[注1)]や独ZF社が主張するような，中央集権型システムにより大手IT企業に収集される個人情報の取り扱いに関する不信感など，さまざまな要因が重なって主権を個人に取り戻そうとする動きが顕在化したことが考えられる。このようなムーブメントがインターネット社会を起点として，現在のさまざまな産業のあり方を問い直しているといえるだろう。

2.3 ビットコインの概念や技術

ビットコインの中核となる概念や技術を以下に簡単に記載する。

2.3.1 P2P（peer to peer）ネットワーク

ビットコインの登場の背景には，前述した中央機関への不信や個人にプライバシーを取り戻すという考えがあるため，ビットコインは中央管理者を置かないことが特徴の一つである（**図2**）。そのため，ビットコインを使用する各個人のPCがサーバーのような役割を果たす。各個人のPCには，ビットコインのすべての取引がダウンロードされ同期するため，一つ



中央管理者を置かないので，特定のサーバーに保存されるのではなく，世界中のコンピューターそれぞれが保存し共有している。

図2　ビットコインのP2Pネットワーク

のPCからデータが消失したり，データが改ざんされたりしても，他の参加者のPCにデータが残っているため，中央管理者にデータが集まる中央集権型よりもリスク分散が図れることになる。このようなネットワークのことを，P2P（peer to peer）ネットワークと呼ぶ。ビットコインは，このP2Pネットワークを使って運用されている。

2.3.2 ブロックチェーン

ビットコインに実物はなく，BTCという単位で取引されるデータである。なお，1BTCは1億分の1まで分割することが可能である。ビットコインの取引はP2Pネットワークで行われ，送金などの取引の一つひとつは，ある程度の固まり（ブロック）で処理される。「ブロック」と呼ばれるこの固まりは，直前のブロックのハッシュ値と呼ばれる数値でつながっている（**図3**）。つまり，取引情報の固まりが，ハッシュ値を介して鎖（チェーン）のようにつながっているのである。世界中のビットコインの取引が固まりとなってつながっていることから，それを「ブロックチェーン」と呼ぶ。ブロック内には，複数の取引が重複せず格納されており，データは元帳のように保存されるため，ブロックチェーンは「分散型台帳技術」とも呼ばれる。

しかし，分散型台帳技術という言葉を使うと，分散型DB（データベース）とどう違うのか，という議論になりやすい。ブロックチェーンを指す分散型台帳と従来の分散型DBはシステム設計の思想が違うので，その違いについては2章5節で述べる。

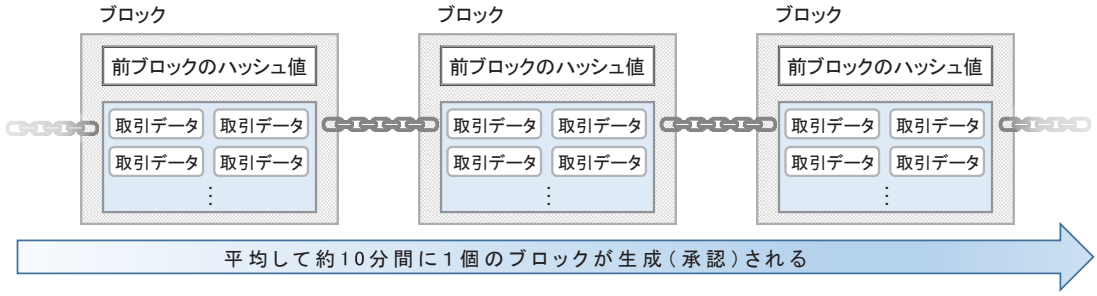
また，ビットコインはブロックチェーンの一種という言い方がされることもあるが，あくまでブロックチェーンはビットコインの中核技術の呼称であり，ビットコインの考案時に，すでにあったブロックチェーンを使用した，というものではない。このあたりが非常に混同しやすいので注意が必要だ。なお，ブロックチェーンには，「パブリック型」と「プライベート型」があるので，これも混同しやすく情報整理が必要である。これについては3章1節で述べる。

ブロックチェーンは，取引情報の固まりの生成とその承認によって成り立っている。直前の取引について所定のアルゴリズムで算出されるハッシュ値を格納し，生成された新しい取引情報の固まりは，P2Pネットワークにおいてブロックごとに承認される。ブロックは，この承認をもって完成する。承認（採掘・マイニング）作業は誰でも参加でき，一番早く承認できた者にはビットコインで報酬が与えられる。

ちなみに，ブロックの承認作業への報酬の金額は，ビットコインが2009年に登場してから最初の4年間は50ビットコインであったが，現在（2017年）は12.5ビットコインとなっている。基本ルールでは，21万ブロックが作成されるごとに半減することになっている。ビットコインの総額は2,100万ビットコインと決められている。現状のペースだと，ブロック作成報酬は2140年になくなることが予想される。

2.4 承認の正当性をどう認めるか

では，P2Pネットワークにおいて，どのようなルールで承認の正当性を認めるのであろうか。



日本政策投資銀行作成

図3 ブロックチェーンイメージ図

2.4.1 Proof of Work（PoW）とは

「ビザンチン将軍問題」という，P2Pネットワークにおいて，正確な情報伝達の難しさを扱った課題がある。ネットワーク参加者に裏切り者がいた場合，不正行為をいかに防げるかという難問で，ネットワーク理論上では，裏切り者が全体の3分の1以上いればネットワークは正しい伝達ができないというものである。このビザンチン将軍問題を解決する手段として考案されたのが，Proof of Work（PoW）と呼ばれる作業である。PoWの原型は，1997年にAdam Back氏がスパムメール対策として考案したhashcashである。

これまで難題とされていたビザンチン将軍問題を解決する画期的なアイデアは，前述のように承認作業に金銭的報酬というインセンティブを与え，計算上のハードワークを要求するというものである。改ざん等の不正を働いた場合は，不正を隠すための作業にさらなるハードワークが必要になるという仕組みを構築したところが，画期的である（改ざんするとハッシュ値が変わるため，つながっているブロックとの整合性が取れなくなってしまう）[注2)]。

2.4.2 具体的なPoWの方法

ブロックチェーンのブロックには，直前のブロックのハッシュ値が格納されていることはすでに述べたが，そのハッシュ値は取引を文字列にしたものをハッシュ関数で変換して算出する。ハッシュ関数としては「SHA-256」などが使われている。SHAはSecure Hash Algorithmの略で，その名のとおりアルゴリズム（計算手順）を定義するものである。

また，ブロックにはナンス（Nonce: Number used once）と呼ばれる1回限りの数値も格納されている。ナンスは計算されるハッシュ値がある一定の条件（最初から一定個数だけゼロが並ぶという条件）を満たすよう要求される。PoWの参加者は，この条件を満たすナンスの値を計算する。先ほど，計算は早い者勝ちと述べたが，この「計算」こそが難解であり，相当な労力を要するのである。難解といっても複雑な計算式を解くのではなく，ひたすら答え（一定の数値よりも小さい値）を見つけるために，トライアンドエラーを繰り返すのである。このため，PCの演算能力が高性能なものほど有利となる。この行為は「金の採掘」になぞらえてマイニングと呼ばれ，作業者はマイナー（採掘者）と呼ばれる。

マイニング作業は，当初は一般的なPCで行われていたが，競争が激しくなるにつれて演算能力を上げるためにCPUからGPUの並列処理に代わり，一部ではCPUやGPUのオーバークロック（CPUやGPUを液体窒素等で冷却することで，PCの演算能力を上げること）という手法もみられるようになった。その後は個人では競争できないレベルまでマイナーの演算能力が上がっており，巨大なマイニングセンターを設置する団体が現れている。マイニングセンターの冷房コストを削減するため，寒冷地であるジョージア（2015年4月21日までは，グルジア）やアイスランドに設置するマイナーが多い。現在では圧倒的な資金力でマイニングセンターを構築した中国の複数企業が，主要マイナーとなっている。

なおこの寡占化により，ビットコインの基本設計思想である「中央集権型の排除」という概念が揺らいでいるのではないかとの指摘もある。

その他，ビットコインには次のような基本的ルールがある。

・最長のチェーンが有効

ビットコインでは，たとえば数人のノードが計算に成功し周知するタイミングが同時だったときや，悪意で複数のブロックが一つのブロックの後に追加されたときなど，チェーンは枝分かれする。これをフォークと呼ぶ。この場合，最長のブロックチェーンが有効とされる。

・手数料が高いものから優先的に

ユーザーが取引（振り込みなど）を実施するとき，マイナーに手数料を支払う必要がある。その手数料が高いほど，優先的に承認される。

2.5 分散型台帳と分散型DBの違いは何か

分散型台帳と分散型DBの大きな違いは，取引履歴の保有の仕方である。

分散型台帳は取引を積み重ねて保有しているので，

過去の履歴を確認するのも簡単だが，分散型DBは現在の値（結果）しかわからない。履歴を見るには過去のログを参照する必要がある。そうなると，分散型DBは現在の値を改ざんしても過去の履歴は変わらないため，改ざんに気づかない可能性がある。

それに対し，PoWでも述べたとおり，分散型台帳の場合，現在の値を改ざんすると過去の履歴にあるハッシュ値が変わるため，履歴を改ざんし続けなくてはならない。また，分散型台帳はダウンタイムがない堅牢性が高いネットワークであるため，分散型DBのようにシステムの保守運用に多額のコストをかけなくてもよい，というメリットがある。

2.6 ビットコインの課題

一方，ビットコインには以下のような課題が指摘されている。

(1) 即時性について

ビットコインの取引が承認されるまでには，約10分間かかる。これは，即時性を求める取引には向いていない。たとえば，株式市場や為替市場などでの取引は高速な決済が要求されるが，10分もかかっていては使えない。

(2) 取引のファイナライズ決済確定時刻の法的効力について

ビットコインのブロックにはタイムスタンプと呼ばれる時刻が格納されるが，これは参加者の作成するトランザクションおよびブロックの承認者の申告をベースとしている。ビットコインの特徴として，1つのブロックが完全に承認される前に次のブロックが処理され始めることがあるため，完全な承認を得る（ファイナライズ）まで，およそ6つのブロックの承認を待つ方がよいとされている（この時間が約10分である）。承認前に次のブロックを処理するというコンセプトは斬新ではある。ただし，承認者の申告ベースの時刻が決済を確定する時刻として法的に効力があるかは，課題とされている。

(3) 暗号技術の進歩による脆弱性

ビットコインに使用されているハッシュ関数はSHA-256などであるが，ハッシュ関数の暗号解析は着実に進歩している。SHA-256の代替関数として含まれているSHA-1関数は，Google社によって，すでに暗号解析上の弱点を発見されている。

(4) 匿名性の保持

コンピューター科学上，匿名とは，偽名性と非連結性をもつものをいう。ビットコインは偽名性をもつが，非連結性は完全ではない。ビットコインのブロックチェーンは公開されているので，特定のアドレスが関与したビットコイン取引を誰でも追跡することができる。行動を追跡することで，ある程度の特定が可能になるといわれている。

(5) スケーラビリティー問題

ビットコインの1ブロックのサイズは，1MBに制限されている。1つの取引は約250Bあるので，1つのブロックには，4,000程度の取引が格納される。約10分で1つのブロックが生成（承認）されるので，1秒当たりでは約6，7件程度の処理件数である。ちなみに，クレジットカード会社のVISAの1秒間当たりの処理件数は1万件以上といわれている。

ビットコインの処理件数があまりに少ないので，ブロックサイズの上限を2MBに上げることが検討されたが，マイナーの多数を占める中国勢の反対で実現できていない。中国勢が反対する理由としては，ネットワークインフラの問題が挙げられている。ネットワークインフラが弱い中国では，大きなデータの送受信に時間がかかるため，ブロックサイズが大きくなると，その分マイニングが不利になるからである。ちなみに，2016年時点でビットコインのコア開発者の一人とされるAdam Back氏は，ブロックサイズを圧縮して取引処理量を増やす技術である「SegWit (Segregated Witness)」を開発し，スケーラビリティー問題に取り組んでいるとしている。

(6) 少数のマイニングプールによる寡占問題

ネットワークの脆弱性でよく問題に挙げられるのが，参加者の過半数が結託すれば，そのネットワークを乗っ取ってしまうことができるという問題である。これを「51％攻撃」という。ビットコインでは主要マイナーが中国勢であるため，P2Pの分散性が損なわれていると指摘されている。

3. ブロックチェーンの利点・課題

3.1 パブリック型・プライベート型

ブロックチェーンには，パブリック型とプライベート型がある。

パブリック型は，今までみてきたとおりビットコインに使われている技術であり，P2Pネットワークで誰でも参加でき，第三者に依存せず（中央集権型ではなく），参加者間で承認作業を行う形態である。

これに対し，プライベート型はClosed型とも呼ばれ，許可されたメンバー間でのみ取引が行われ，承認は権限をもった限定メンバーによって行われる形態をいう。これにより，パブリック型のデメリットであった，即時決済に不向きである（約10分かかる）点が解消されるとともに，相当な作業量を要求される（電力コストもかかる）PoWが不要になる。一方で，サトシ・ナカモトが発案した従来のビットコインの思想（中央集権型からの脱却，誰でも参加できるという自由な世界）とはまったく異なったものになるので，プライベート型ブロックチェーンは邪道であるという意見もある。

しかし，ビットコインのブロックチェーンという技術に着目し，システムの堅牢性やトータルコストの大幅な削減などのメリットを引き継ぐことは，その呼称はどうであれ，さまざまな産業で活用され，発展していく可能性が高いだろう。

3.2 2つの「D」

ブロックチェーンは分散型台帳技術とも呼ばれ，「Distributed Ledger Technology: DLT」と表記される。一方，スマートコントラクト[注3)]をブロックチェーン上で用いて自律的に事業を運営する考え方がある。このような自律的組織を分散型自律組織（Decentralized Autonomous Organization: DAO）という。ＤＡＯでは，意思決定や実行などは，あらかじめプロトコルで定められたルールにしたがって自律的に行われる。

日本語では，「Distributed」と「Decentralized」はともに「分散」と表現されるが，英語では，明確に区別して使用されている。この区別については，1964年に米国The Rand CorporationのPaul Baran氏が発表した「On distributed communications」[3)]に記載された内容が引用されることが多い（**図4**）。

報告書の中では，Distributedは「grid or mesh」と表現され，Centralizedは「star」と表現されている。**図4（C）**では，ブロックチェーンは「grid or mesh」という特徴をもつため，Distributedに該当するだろう。また，報告書では，実際のネットワークでは，DistributedとCentralizedの混合型もみられるとし，そのことをDecentralizedと表現している。

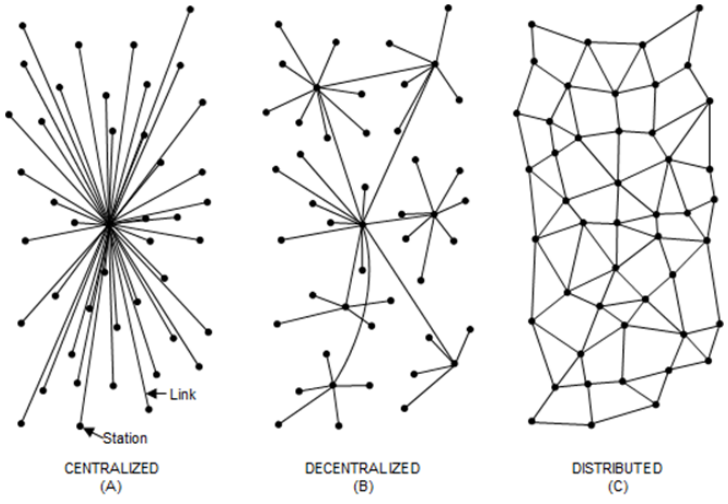


FIG.1 − Centralized, Decentralized and Distributed Networks

出典：Baran, Paul. “On distributed communications”. The Rand Corporation, 1964, 37p.

図4 「Decentralized」と「Distributed」の違い（概念図）

3.3「スマートコントラクト」の課題

スマートコントラクトでは，プロトコルで決められたとおりにブロックチェーン上で取引が執行されるので，機械的に取引が処理される。そこには疑いの余地は生まれない。いわば，自動車のハンドルの「遊び」部分がない，精緻なものである。

しかし，世の中は完全な世界ではない。細部の条件が詰め切れておらず，取引が執行されたことに納得のいかない事態が発生する可能性もある。通常の契約書ではそのような場合に備えて，疑義が生じた場合はお互いに誠意をもって対処する，というような「知恵」が入っているものである。

ビットコインの理念は，中央機関を排除して全員参加で物事を進めるというものであったが，中央機関を排除すれば，責任は当事者同士で負うことになる。紛争が生じた場合は，仲介する機関はなく，あくまで「自己責任」が課される。複雑でない，定型の取引の場合はスマートコントラクトでオペレーショナルコストが下げられるというメリットがあるが，強制執行のマイナス面にも留意する必要があるだろう。

3.4 印紙税の問題

契約がブロックチェーン上で執行されるとなると，そこには当然，紙の書面は存在しない。今後ブロックチェーン上でのスマートコントラクトが増えていった場合，印紙税はどうなるのであろうか。

現時点では，電子媒体に関する印紙税については，2008年10月24日付の福岡国税局の回答が参考になっている[4]。すなわち，「電子媒体であれば書面での契約書の交付がされていないので印紙税は不要」との解釈であるが，今後スマートコントラクトのような取引契約が増加していった場合は，注意が必要だろう（ただし，電子媒体で契約書を交付した後に，現物を別途持参するなどの方法により相手方に交付した場合は，課税文書の作成に該当し，現物の契約書に印紙税が課されるものと考える）。

3.5 金融機能を代替しうるか

では，ブロックチェーンで金融機関の業務を代替するということはできるのであろうか。

金融機関の機能には主に3つの機能がある。(1) 金融仲介機能，(2) 決済機能，(3) 信用創造機能である。

このうち，ブロックチェーンでさまざまな実証実験が行われているのは，(2) 決済機能の部分である。

(1) 金融仲介機能や，(3) 信用創造機能をブロックチェーンで代替するには，さまざまな工夫が必要となるだろう。

(1) 金融仲介機能には，「資産変換機能」と「情報生産機能」がある。「資産変換機能」とは，金融機関が資金調達者からその者に都合のよい金融商品を受け取り，資金提供者にはその者に都合のよい金融商品を受け渡し，選好ギャップを埋めるという働きをいう[5]。金融仲介機能として通常思い浮かべるのは，文字通り金融商品の「仲介」をするこの「資産変換機能」であろう。一般の方が見落としがちなのが，後者の「情報生産機能」である。

「情報生産機能」とは，資金調達者の行動や経済状況についての情報を収集・分析するという活動を中心とするもので，審査と監視（モニタリング）を通じて金融機関が遂行している役割のことをいう[5]。金融機関はただ単に金融商品を仲介しているだけではない。資金調達者に対して，審査をして事後のモニタリングを行うという機能が忘れられ，語られていることが多い。銀行業への新規参入者が失敗しているのも，審査やモニタリングをおろそかにしているケースが多い。

(3) 信用創造機能は，金融機関が預金を貸出（融資）する活動をいうが，(1) 金融仲介機能の情報生産機能（審査・モニタリング）を通じて生み出されるものである。したがって，ブロックチェーンで金融仲介機能を代替できれば，(3) 信用創造機能も代替可能となるだろう。だが，実際には金融仲介機能（情報生産機能）を有効にするには，データの分析だけでは不十分で，実際の（資金調達者の）現場に足を運び，肌感覚で違和感を察知することが重要となる。このようなことから，ブロックチェーンで金融仲介機能をすべてクリアできるかは今後の課題となるだろう。

3.6 金融機関はなぜブロックチェーンを導入するのか

従来の金融機関のシステムには中央管理者が存在する。各部門のPCは情報システム部門が管理するサーバーにアクセスするため，クライアントサーバー方式と呼ばれている。強靭なセキュリティーシステムや緊急時のバックアップなどの運用体制を堅牢に構築する必要がある。そのため，システム構築や保守運用にかかるコストは莫大なものとなるが，それはオペレーション上必要かつ戦略的な経費であるとし，金融機関は多額の情報化投資を行ってきた。

これに対し，ブロックチェーンはP2Pネットワークのため，システムダウンの可能性が著しく低く，改ざん耐性も優れている。つまりシステム構築やバックアップのための初期費用，セキュリティーなどにかかるランニングコストを低く構築できる。これが，金融機関がブロックチェーンの導入を検討する大きな理由である。しかし，システム全体の代替は難しい。トータルコストで考えると，既存システムを置き換えるとさまざまな周辺システムへの影響が考えられ，試行作業にも莫大な時間と費用がかかるだろう。

3.7 カウンターパーティー・リスクに関する議論

ブロックチェーン関連の書籍や情報媒体に接すると，必ずしも金融機関の基本業務や事業法人のビジネス実務について深い洞察がないまま，乱暴な解釈をしているものも散見される。たとえば，ブロックチェーンを導入すればカウンターパーティー・リスクがなくなるとか，売掛金がなくなる，という類いのものだ。

金融取引でいうカウンターパーティー・リスクとは，金融商品の取引相手である金融機関がデフォルト（債務不履行）した場合に，その取引を金融市場で再構築する際のコストである。代表的なものはデリバティブ取引におけるカウンターパーティー・リスクがあるが，金融機関は当該商品を時価評価し再構築コストを把握してさまざまな手法でヘッジ（リスク回避）している。基本的には，金融商品の期限が来るまではカウンターパーティー・リスクは存在し，毎日時価評価してヘッジしなくてはならない。ブロックチェーンを導入すれば即座にカウンターパーティー・リスクがなくなるわけではない。ただし，スマートコントラクトに時価評価やヘッジ手法を定めておけば，業務の効率化が図れ，オペレーショナルコストの低減に寄与する可能性はある。

また，一般に，売掛金とは企業が商品を販売したが，取引先から入金がない売上債権のことを指す。商品を購入した方は，その商品に瑕疵がないか検証し（この場合は買掛金の計上），検証が終了すれば支払いに応じることが一般的である。そのため，ブロックチェーンを導入したからといって，即座に入金がなされ，売掛金が現金に変わるわけではない。このような商取引の実態を無視してブロックチェーンを過剰に礼賛するのは行き過ぎであろう。冷静な議論が必要である。

4. おわりに

ブロックチェーンは，IoTやAIとともに第4次産業革命の中枢技術になる可能性がある。ただし，ブロックチェーンですべてが解決できるなどと考えていると，冷静な判断を失ってしまう。中央集権機関を排除し，個人間取引を突き詰めていくと，おのおのが自分の利益を守ろうとするがために，さまざまな障害が発生するはずである。まさに，トマス・ホッブズが『リヴァイアサン』で指摘した“自然状態”が生じるわけである。

キリスト教における“教会”の役割を考えるとどうだろう。教会は，神と個人との契約の間に仲介機関として存在している。プロテスタントはこの仲介機関である教会の腐敗を指摘した。ルターやカルバンの宗教改革である。本稿の冒頭で述べたビットコインの登場の背景，すなわち，世界的なIT革命の進行をよそに，変わらずある中央集権型機関の非効率性への不満や，中央集権型システムの後押しにより大手IT企業に収集される個人情報の取り扱いに関する不信感なども，この宗教改革の背景に近いかもしれない。

ただやみくもに中央集権機関の排除を訴えるのではなく，なぜ中央集権機関が必要とされ誕生したの

か（たとえばホッブズは“自然状態”の発現に当たり，個人の利害衝突をまとめる“国家”の役割をあぶりだした）という社会科学的アプローチによる議論も今後必要となってくるだろう。情報を整理し，冷静な議論を望みたい。

青木 崇（あおき たかし）
1996年慶應義塾大学 理工学部応用化学科卒。東海銀行（現三菱東京UFJ銀行）入行。2006年外資系金融コンサルティング会社に入社。2008年日本政策投資銀行に入行後，クレジットビジネスグループ，企業金融第2部ものづくりサポートチーム参事役，九州支店企画調査課長を経て，2016年6月より日本政策投資銀行 産業調査部課長（現職）。

本文の注

注1) Electronic Frontier Foundation：https://www.eff.org/

注2) **図3**のように，ブロック同士を時系列順でつなぐために，ブロックには前ブロックのハッシュ値が入っている。あるブロックの取引データを変更してしまうと，ハッシュ値も変わるため，前ブロックのハッシュ値との整合性がなくなり，それ以降のブロックもすべて無効になってしまう。

注3) スマートコントラクト（smart contract）とは，コンピューターシステム（またはその他の自動化された手段）を使って契約（contract）を強制執行するものである。この機能を使えば，誰でも手数料を支払うだけでブロックチェーン上でプログラムを実行することができる。

参考文献

1) “ブロックチェーン技術の活用領域拡大に向けた実証事業を開始”. 福岡地域戦略推進協議会. http://www.fukuoka-dc.jpn.com/?p=16793, (accessed 2017-03-13).

2) Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system". https://bitcoin.org/bitcoin.pdf, (accessed 2017-03-13).

3) Baran, Paul. On distributed communications. The Rand Corporation, 1964, 37p.

4) “請負契約に係る注文請書を電磁的記録に変換して電子メールで送信した場合の印紙税の課税関係について”. 国税庁. https://www.nta.go.jp/fukuoka/shiraberu/bunshokaito/inshi_sonota/081024/01.htm, (accessed 2017-03-13).

5) 池尾和人. 現代の金融入門. 筑摩書房, 2012, 260p.（ちくま新書, 831）.

Author Abstract

Blockchain is a key technology of bitcoin. Bitcoin is a cryptocurrency system created based on the document released in 2008 by an unidentified programmer named Satoshi Nakamoto. It seems the appearance of bitcoin partly stems from frustration over centralized system which is inefficient and stays unchanged even though IT has been growing dramatically, as well as distrust on its information-handling capability. While using blockchain technology on social system would be able to generate a new world, robust and low cost, some information about blockchain are too optimistic, or/and generated by each party's standpoint not based on real business. The comprehensive and unbiased argument is necessary not only by technical aspect but also by social scientific point of view.

Key words

bitcoin, blockchain, distributed ledger technology, FinTech, internet, the fourth industrial revolution, P2P, PoW, hash, mining