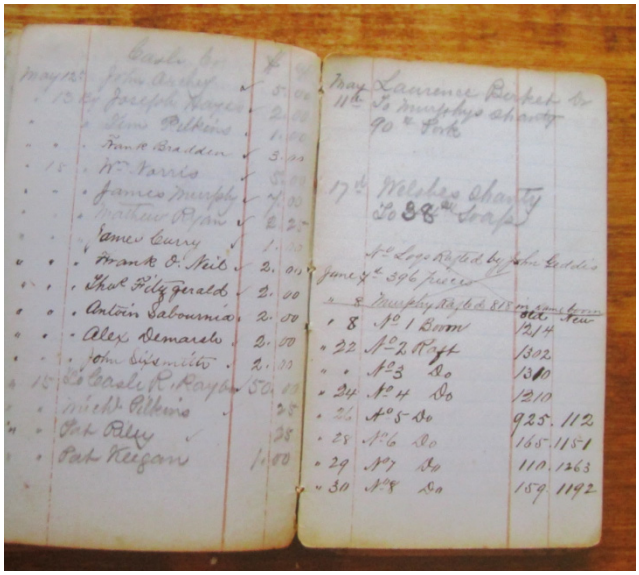
ブロックチェーン(分散型台帳技術)とは

1. ブロックチェーン（分散型台帳技術）、ビットコインの概念整理

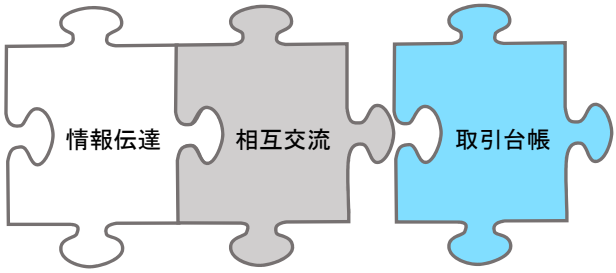
- 2017年3月にドイツで開催された国際情報通信技術見本市CeBIT2017において、グローバルカンファレンスの主要テーマとしてブロックチェーンが取り上げられた。カンファレンスの登壇者であるBolten Consulting社のFrank Bolten氏による講演では、ブロックチェーンはインターネットに「取引台帳」という価値を付加したものであると定義された。ここで、インターネットの価値は、「情報伝達」と「相互交流」であると定義している（図表1、図表2）。また、当社のブロックチェーンのプロジェクト件数の紹介もなされ、金融機関向けが一番多いことがわかる（図表3）。
- ブロックチェーンの概念を理解するには、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だからである。

図表1　取引台帳のイメージ図（Frank Bolten氏講演資料）



（備考）CeBIT2017にて筆者撮影

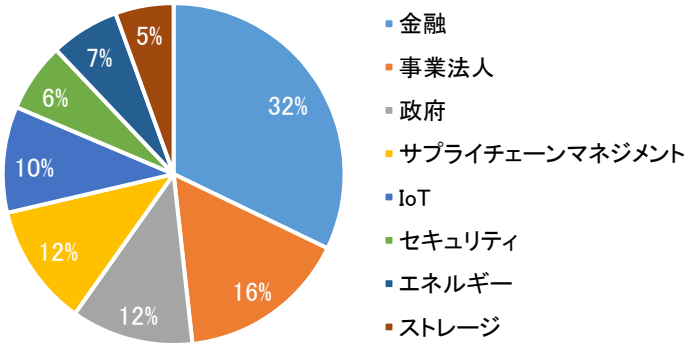
図表2　ブロックチェーンの価値イメージ



（備考）Bolten Consulting社資料により日本政策投資銀行作成

図表3　Bolten Consulting社のブロックチェーン業種別プロジェクト件数

業種	プロジェクト件数
金融	64
事業法人	32
政府	23
サプライチェーンマネジメント	23
IoT	20
セキュリティ	13
エネルギー	13
ストレージ	11



（注）2017年3月16日時点。プロジェクト総数232（重複あり）

（備考）Bolten Consulting社資料により日本政策投資銀行作成

1. ブロックチェーン（分散型台帳技術）、ビットコインの概念整理　（続き）

（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（図表4）をもとに考案され、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。

（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関わらず、旧態依然とした中央集権型機関の非効率性への不満や、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扱いに関する不信感など、様々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、現在の様々な産業の在り方を問い直していると言えるだろう。

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。

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。そのため、ビットコインを使用する各個人のPCがサーバのような役割を果たす。
- 各個人のPCには、ビットコインの全ての取引がダウンロードされ同期するため、1つのPCからデータが消失しても、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（図表5）。

図表4　サトシ・ナカモトによるビットコインの考案文書

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.

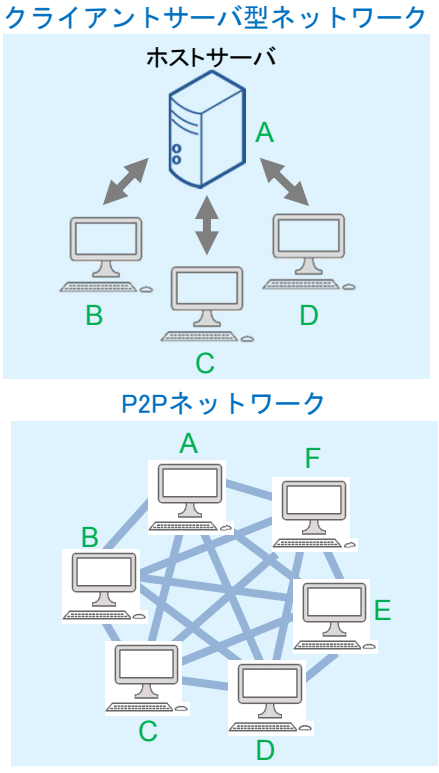
1. Introduction

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.

（備考）ウェブサイト https://bitcoin.org/bitcoin.pdf より

図表5　クライアントサーバ型ネットワークとP2Pネットワークのイメージ図



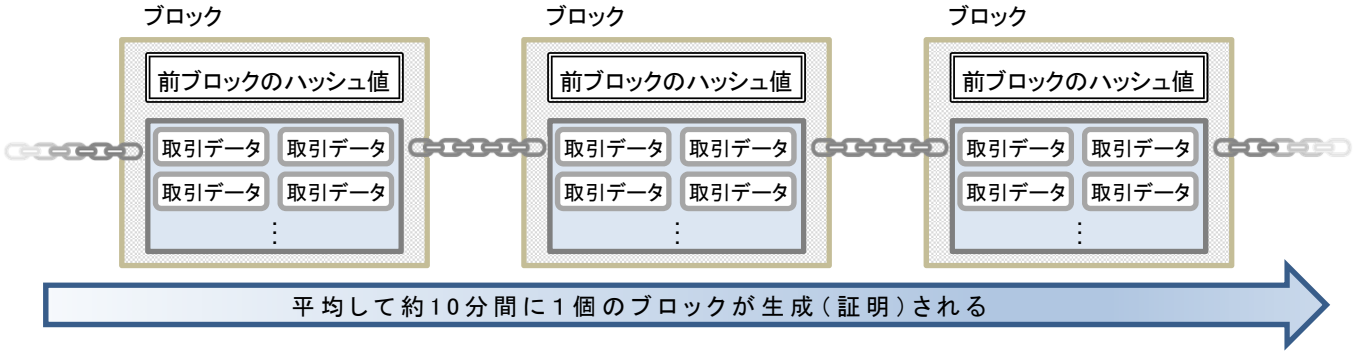
（備考）日本政策投資銀行作成

1. ブロックチェーン（分散型台帳技術）、ビットコインの概念整理　（続き）

ブロックチェーン

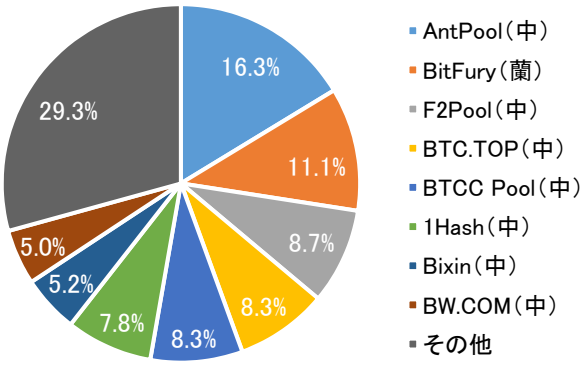
- 「ブロック」と呼ばれる取引の固まりは、ハッシュ値と呼ばれる所定のアルゴリズムで算出される、ブロックを識別する固有の値でつながっている。つまり、取引情報の固まり（ブロック）が、ハッシュ値を介して鎖（チェーン）のようにつながっているため、その形状から「ブロックチェーン」と呼ばれる（図表6）。
- ブロックの中には、複数の取引が重複せず格納されており、データは元帳のように保存されるため、ブロックチェーンは分散型台帳技術とも呼ばれる。
- ブロックチェーンは、取引情報の固まりの生成と、その取引情報が正しい（二重譲渡がない等）という証明作業によって成り立っている。この証明作業には基本的に誰でも参加でき、一番早く証明できた者にはビットコインの報酬が与えられる。
- 証明作業には、計算上のハードワークが要求され（Proof of Workという）、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。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（プロ集団）が、主要マイナーとなっており（図表7）、通常のPCでは到底かなわないレベルになっている。
- ブロックチェーンの特徴として、改ざんが困難であることが挙げられる。取引データを改ざんすると、ハッシュ値も変わるため、チェーンが切れてしまうためである。

図表6　ブロックチェーンイメージ図



（備考）日本政策投資銀行作成

図表7　ビットコイン採掘プール（マイナー）の市場シェア



（注）2017年4月7日現在

（備考）ウェブサイト https://blockchain.info/pools により日本政策投資銀行作成

2. ブロックチェーンの有望性と課題

ブロックチェーンは有望な技術であるが、課題も指摘されており、必ずしも万能ではない。ここでは、ブロックチェーンの有望性と課題について整理する。

(1) ブロックチェーンの有望性

ブロックチェーンの活用例として、トレーサビリティの観点、プライバシー保護の観点から以下に事例を挙げる。

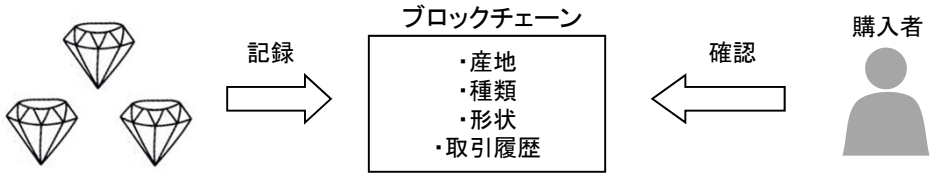
①トレーサビリティの観点

- オバマ政権時代に、米国防総省が納入した軍事製品に中国製の偽造部品が混じっていたことが問題となった。ネットワークにつながるルータにも偽造品が見つかり、厳重なセキュリティが施されている米国の軍事システムに中国の情報工作員が侵入できる可能性があったと報道された。
- このような問題の場合には、ブロックチェーンで「トレーサビリティ」（追跡可能性）を導入することが有効であろう。例えば、英国のEverLedger（エバーレッジャー）社は、ダイヤモンドの取引にブロックチェーンを応用するシステムを開発している。ダイヤモンドの産地や形状などの情報をブロックチェーン上に登録し、取引履歴もすべて記録することで、不法に取引されるダイヤモンド（ブラッド・ダイヤモンド）や盗品の購入を回避できるというものである。このようなアイデアは応用が可能なので、メイドインジャパン製品を守ることにも有効なアプリケーションとなるであろう（図表8）。

②秘匿性が高い領域（医療機関等）への応用例

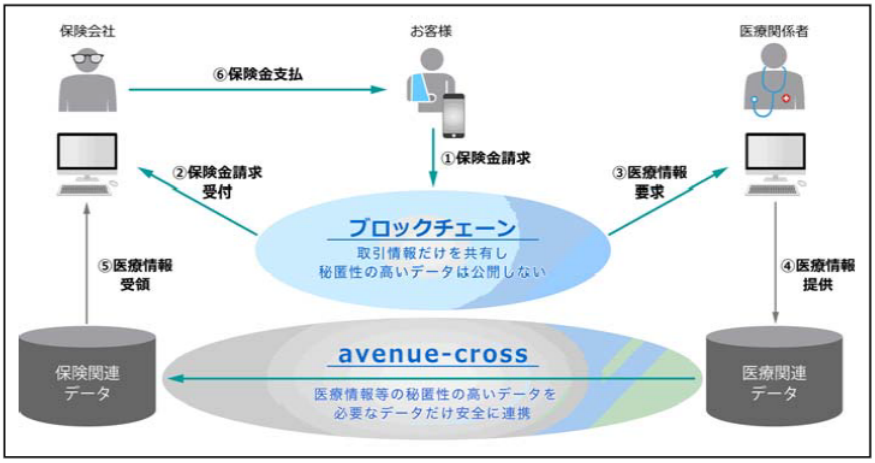
- 福岡地域戦略推進協議会（FDC）と東京海上日動は、保険業務で取り扱う契約内容や医療情報など、長期に亘って非常に高い秘匿性が求められる領域でのブロックチェーンの実証実験を2017年1月に開始すると発表した（図表9）。具体的には、東京海上日動はFDCの協力のもと、福岡市域の医療機関と連携し、傷害保険金請求書に記載の医療機関に対し、ブロックチェーンを通じて入通院期間などの医療情報の提供を要求し、データ連携基盤を通じて医療情報等のデータを受領することで、医療情報に対するセキュリティを確保しつつ、保険金支払業務の簡略化、迅速化が可能かを検証する。
- ここで使用するデータ連携基盤は、エストニアの国民番号制度を支える非常に高いセキュリティ技術を適用したデータ連携基盤であるPlanetwayの「avenue-cross」と従来のブロックチェーン技術を合わせて設計している。

図表8　ダイヤモンドの取引にブロックチェーンを活用



（備考）日本政策投資銀行作成

図表9　保険業務にブロックチェーンを活用



（備考）福岡地域戦略推進協議会ウェブサイトより

2. ブロックチェーンの有望性と課題（続き）

(2) ブロックチェーンの課題

一方、ブロックチェーンの課題としては、以下のような課題が指摘されている。

①スケーラビリティ問題

・ビットコインの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（証明）されるので、1秒あたりでは約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秒当たりの処理件数は約2,000件で、忙しい時間帯には約10,000件を処理できると言われている。

・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」を開発し、スケーラビリティ問題に取り組んでいるとしている。

②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暗号解析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SHA256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。SHA256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、既に暗号解析上の弱点を発見されている。

3. プライベート型ブロックチェーン

・上記の①や②のような課題は、ビットコインが誰でも参加できるパブリック型（オープン型）であるため生じている問題である。

・この問題を解決する手段として、ネットワークをプライベート型（クローズド型）にする考え方がある。それは、許可されたメンバー間で取引を行い、証明は権限を持った限定メンバーによって行われる。これにより、パブリック型のデメリットである即時決済に不向きであ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）証明作業も不要になる（図表10）。

図表10　パブリック型ブロックチェーンとプライベート型ブロックチェーンの違い

	パブリック型	プライベート型
管理者	なし	あり
P2Pネットワークへの参加	自由	許可制
証明作業(PoW)	あり	なし(PoWに代替する機能あり)
決済速度	遅い	早い
機能の追加や改修	参加者の半数以上の同意が必要	管理者により柔軟に対応可能

（備考）日本政策投資銀行作成

4. プライベート型ブロックチェーンの国内事例

- プライベート型ブロックチェーンは、金融市場での活用が期待されている。国内の事例を挙げたい。
- 日本取引所グループは、2016年8月にブロックチェーンを用いた実証実験の報告書である「金融市場インフラに対する分散型台帳技術の適用可能性について」を公表した。
- 2016年4月～6月にかけて行った実証実験を通じて、証券市場における発行・取引・清算・決済・株主管理といった一連のプロセスが分散型台帳技術上で実現可能かについて技術評価を実施。
- SBI証券、証券保管振替機構、野村證券、マネックス証券、みずほ証券、三菱東京UFJ銀行の6社が参加し、実験結果としては、「いくつかの課題があるものの、新たなビジネスの創出、業務オペレーションの効率化及びコストの削減等に寄与する可能性が高く、金融ビジネスの構造を大きく変革する可能性を持つ技術であることが分かった。」と報告している。

5. 金融機関が注目するプライベート型ブロックチェーン

- 現状の金融機関のシステムは、前掲の図表5のように中央管理者（ホストサーバ）が存在し、各部門のPCとデータのやり取りを行い、クライアントサーバ方式と呼ばれている。強靭なセキュリティ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。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いる。
- これに対し、ブロックチェーンはP2Pネットワークで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。また、プライベート型ブロックチェーンであれば、証明に時間がかからず、システム構築コストも劇的に低くできる。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。

6. まとめ

- これまでみてきたように、ブロックチェーンはビットコインの中核技術として生まれてきた訳であるが、最近ではブロックチェーンという技術そのものに焦点が当たり、様々な実証実験が行われている。
- 有望性がある一方で、いくつかの課題も指摘されており、まだ万能ではないがIT技術の進歩とともに第4次産業革命には欠かせない技術として成長していくであろう。

補足:ブロックチェーンの詳細な技術については、本稿では割愛している。詳細は科学技術振興機構(JST)の機関誌「情報管理」6月号にて掲載予定である。

【産業調査部 青木　崇】

お問い合わせ先　株式会社日本政策投資銀行　産業調査部
Tel: 03-3244-1840