

知っておきたいキーワード

ブロックチェーンとその応用

河村 岳[†], 足立 崇彰[†][†] パナソニックノースアメリカ株式会社 Panasonic β

"Blockchain and Its Applications" by Takashi Kawamura and Takaaki Adachi (Panasonic Corporation of North America, United States)

キーワード：ブロックチェーン、分散管理、P2P取引、仮想通貨、スマートコントラクト

まえがき

筆者らはシリコンバレーで活動しており、ここでは、魅力的なサービスが次々と生まれています。

これらは、スタートアップ企業が、既存の産業を破壊（ディスラプト）することにより、ユニコーンと言われる巨大な成功者となることで実現されて

います。そのコアとなるものは、ディスラプティブ（破壊的）なビジネスモデルの場合もあれば、ディスラプティブな技術の場合もあります。今回は、ブロックチェーンを上記の観点で紹介します。シリコンバレーでブロックチェーンの状況を聞くと、今回のAI（人工知能）ブームの初期と同じだという答えが返ってきます。半分の人

はAI同様にブームが来ると信じて、起業、投資、開発が行われています。サンフランシスコを中心に、特徴あるスタートアップも多くあり、大手IT企業は自社のサービスへのブロックチェーンによるさまざまな機能の提供を始めています。

ブロックチェーンとは？

ひとことで言えば、分散管理された取引データベースです。過去の取引はすべて記録されます。またネットワーク上に分散管理されますので、一部データが棄損しても復元性が高いという特徴があります。

さらに、後に説明するデータ構造と技術特徴、また運用ルールにより、取引記録に対する透明性・信頼性が高いのも特徴です。その運用ルールとは、取引を参加者同士でチェックし合うことで、正しさを適宜検証するものです。したがって、中央集権型のシステムが不要となるので、信用を要するP2P（Peer to Peer）取引に向きます（図1）。

銀行や重要商取引の中には、これまで巨額の投資とメンテナンスを必要と

する中央集権型システムが採用されてきましたが、ブロックチェーンはこれらの分野に大きなパラダイムシフトを起こすと言われています。

すなわちブロックチェーンのメリットは、「分散環境化による高いセキュリティ」と、「莫大な数の参加者が存在する場合の圧倒的な低コスト化」で

す。このメリットを活かすことによって、低コストで大規模なサプライチェーンの構築、オープンかつ安全に個人情報管理ができる電子カルテシステム、24時間365日停止することの許されない公共インフラシステムなどを実現することができます。

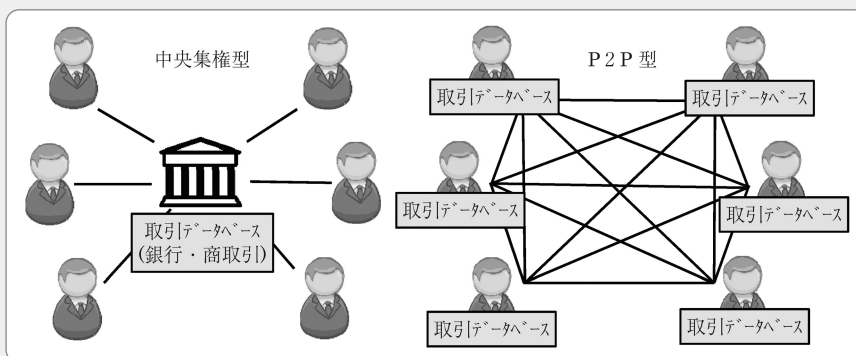


図1 中央集権型とP2P型の取引形態

ブロックチェーンの技術

取引記録に対する信頼性を高めるため、データ構造と技術に工夫が施されています(図2)。

ブロックチェーンでは、Hash関数(要約関数)と呼ばれる技術を使って、データベースの特徴を適切に要約します。要約方法、つまり具体的な関数設定そのものは、データベースの内容に応じて設計されます。

いま、新たな取引内容(ブロック)を作成しようとしたとします。そのとき、前の取引内容(ブロック)のデータすべてのHash値を算出し、新たに追加するブロックに書き込みます。一連の手続きの詳細は省きますが、このようにあたかもチェーンのように、前後の関係性を使うことで、改竄すると

過去のデータの内容にも影響が及ぶ設計となっている点が特徴です。ただしこれを適宜、参加者がチェックするので、チェックに計算時間を要するとい

う課題があります。また、利用者数が増えた場合のスケーラビリティの課題も指摘されています。

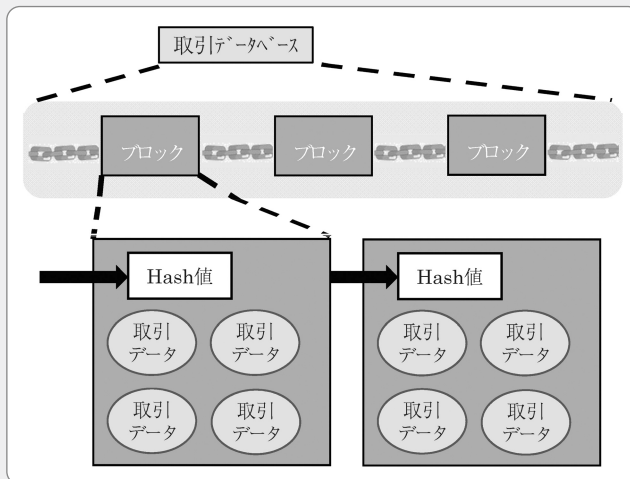


図2 ブロックチェーンの構成

アプリケーションと期待されるイノベーション

以下、実際のアプリケーションを例に挙げて、その特徴を説明していきます。

(1) 仮想通貨

- ・金融資産として
(例: Bitcoin)



仮想通貨の名前のとおり、通貨として流通することへの期待がありますが、前述のとおり中央管理者が存在しないため、例えば、通貨に必要な政府介入(景気に応じて流通量を増やす量的緩和策や、為替市場介入など)が難しく、国の通貨代替には本来は向いていません。ただし、安定した信用通貨が流通していない発展途上国では、代替となる可能性もあります。流通量をコントロールできない、金などの金融資産に近いイメージです。

- ・金融取引の手段として
(例: Ripple, MUFGコイン)



今まで専用の管理システムが必要であった金融ネットワーク・サーバ管理

システムをWebクラウド上へ実装できるため、海外送金などの手数料を大幅に安くできます。さらにRippleは、Bitcoinの欠点である計算時間(10分)を大幅に短縮(数秒)しているため、金融取引への適用が現実味を帯びてきています。Rippleベースでの銀行仮想通貨の例としてMUFGコインが挙げられます。クローズドな世界で使われることから、上記のメリットを備えたマイレージポイントのようなものと思えばよく、既存通貨との間で固定した価値が付与されるのが一般的です。これは、変動相場リスクを抑えて、安心して金融取引を実施してもらうためと思われる。

(2) スマートコントラクト

- ・流通のトレーサビリティとして
(代表例: Ethereum)



ブロックチェーンの改竄耐性を活用し、流通品の生産者・生産時期証明や、流通ルートの証明に使うことが提案されています。データベース管理システムを個別に構築するよりコストの低減につながる事が期待されています

が、比較的商品単価が高く、トレーサビリティのニーズが高い品目から導入が進んでいるのが実情です。なおBtoB(Business to Business:企業間)の取引では、誰もが使えるパブリックブロックチェーンなどの仮想通貨とは異なり、参加者を限定したプライベートブロックチェーンが使われることも多いのが特徴で、前述のスケーラビリティの課題が小さい応用先としても注目です。

- ・決済を伴うP2P商取引として(代表例: IOTA)

IoTのエッジデバイス上に実装し、計算リソースの限られた環境でも取引を実現させる提案もされています。データの整合性を証明する承認者は取引をする者同士とすることで、通信が効率化でき、承認作業を極めてスムーズにできるのが特徴です。ただし、技術的にまだ完成しておらず、今後の発展が期待されています。これ以外にも、行政関係の公的書類代替(土地登記簿や各種証明書)やC2C(Consumer to Consumer:消費者間)のオークションなど、幅広い応用が期待されています。

ブロックチェーンの今後

インターネットが情報交換のインフラなのに対し、ブロックチェーンは価値交換の新しいインフラと言われています。

さまざまな仮想通貨やブロックチェーンの流派が存在する現在は、技術的にも社会のインフラシステムとしても過渡期だとの指摘があります。Bitcoinは大量の技術者が参加しており、進歩も日進月歩ですが、通貨としての信頼性保持のため、大胆なバージョンアップ（分岐、ハードフォーク：互換性のない仕様変更）を頻繁に行えないという足かせもあります。

ブロックチェーンの産業破壊性は、分散型アプローチによる、P2P（C2C）取引の信頼性の飛躍の向上にあると思われます。既存の金融機関、商取引のゲームチェンジを引き起こす可能性が高く、「金融分野」、「エネルギー分野」、「流通分野」での注目度が高まっています。

一方で、すべての商取引がC2Cで実現されるようになれば、ある人にとって不要なものを別の人へシェアする、シェアリングエコノミーがより加速するかもしれません。また、あらゆる情報を一元的に手に入れ、AI技術により競争力の高いサービスを提供してきた巨大IT企業たち（Google、

Apple、Facebook、Amazon）も、見方によれば中央集権型の管理者であり、C2C取引の一般化により、情報交換もC2Cが一般的となれば、その存在意義が脅かされかねない、との危機意識を持ち始めています。

このように、世の中のありようを大きく変えてしまう可能性を秘めたものがブロックチェーン技術です。ここでは技術の詳細な解説は省略しましたが、興味のある方はこれをきっかけに、ぜひ勉強してみてください。

（2018年6月8日受付）

参考文献

- 1) 伊藤穰一、アンドレー・ウール：“教養としてのテクノロジー AI、仮想通貨、ブロックチェーン”，NHK出版
- 2) A. Mine: “ブロックチェーンの仕組み～初心者のためのわかりやすい解説～”，<http://gaiax-blockchain.com/blockchain-first-book>
- 3) F. Graillot: "The Blockchain Might Be the Next Disruptive Technology", <https://techcrunch.com/2015/10/03/the-blockchain-might-be-the-next-disruptive-technology/>
- 4) J.D. Rowley: "With at Least \$1.3 Billion Invested Globally in 2018, VC Funding for Blockchain Blows Past 2017 Totals", <https://news.crunchbase.com/news/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/>
- 5) 片淵陽平：“「お祭りにはしたくない」-「MUFGコイン」生かすアイデア，ベンチャーから募集，三菱UFJの“本気度””，<http://www.itmedia.co.jp/news/articles/1803/05/news082.html>



河村 岳 1997年、東京大学工学部電気工学科修了。同年、松下電器産業（株）入社。以来、収音技術（雑音除去、指向性制御）、音声速度変換技術のほか、コンピュータショナルフォトグラフィー（DFD）を用いた民生カメラ用AF技術や、Deep Learningを用いた画像認識技術の開発に従事。Panasonic Silicon Valley 研究所長を経て、2018年、Panasonic β Director



足立 崇彰 1998年、成蹊大学大学院工学研究科修了。NTTエレクトロニクス（株）を経て、2004年、松下電器産業（株）（現パナソニック（株））入社。通信用半導体を中心に次世代のIoT通信基盤の開発に従事。2014年より、北米にて、コーポレートベンチャーキャピタルの業務に従事。

キーワード募集中

この企画で解説して欲しいキーワードを会員の皆様から募集します。ホームページ（<http://www.ite.or.jp>）の会員の声より入力可能です。また電子メール（ite@ite.or.jp）、FAX（03-3432-4675）等でも受け付けますので、是非、編集部までお寄せください。（編集委員会）