

bitcoin と ripple

田村 聡明, 山下 大輔

Satoaki TAMURA, Daisuke YAMASHITA

1 はじめに

仮想通貨とは、インターネット上でやりとりされる実体のない通貨である。仮想通貨は、面倒な手続きをなくすことで、世界中の人が手軽に取引することを目的に生まれた。仮想通貨は両替が不要であり、国境を越えて早い送金が可能である。また手数料がほとんどかからない。このため、国外との取引が容易になり、グローバル化の促進が期待できる。

現在、仮想通貨には様々な種類がある。世界で最も使われている仮想通貨は bitcoin である。bitcoin のシステムには中央機関が存在せず、通貨の発行や取引の全てをネットワーク参加者全体がそれぞれ管理するという特徴がある¹⁾。その bitcoin の改良版として注目されているのが ripple である。ripple は IOU、つまり借入書を使うことによって取引を簡潔にするという特徴がある。

2 bitcoin

2.1 bitcoin の概要

bitcoin は世界で最も利用されている仮想通貨であり、P2P の仕組みを利用して分散処理を行い、暗号化の技術と組み合わせることで信頼性を保証している。²⁾

帳簿は 1 カ所管理するのではなく、bitcoin を利用している世界中のコンピュータが、全体の帳簿をそれぞれ保管している。そのため、1 つの帳簿を書き換えたところでおよそ 1000 万個の帳簿と照らし合わせると矛盾が起きる。その場合、書き換えた帳簿は多数決の原理により、間違った記述だと判断され、書き直される。

2.2 ブロックチェーン

ブロックチェーンとは、時系列順に繋がった取引記録である。ブロックチェーンは、多数の取引データの塊をブロックという単位で表す。ブロックはネットワーク全体で正しいと認められたとき、時系列順に繋がられ、ブロックチェーンに加えられる。これにより、ブロックチェーンは一貫した取引履歴をネットワーク全体で共有できる。

ブロックのデータを改竄したとしても、ブロックチェーンによって時系列順に繋がっているため、後続のブロックと矛盾が起きる。したがって、最新のブロックまで改竄して繋ぎ直す必要があり、膨大な量の計算を行わなければならない。さらに、その計算中も 10 分に 1 つブロックが加えられるため、10 分以内にすべての計算を終える必要がある。そのため、改竄は容易ではない。

2.3 ビットコインマイニング

ビットコインマイニングとは、新たなブロックをブロックチェーンに繋ぎ、取引データを更新することである。そ

れぞれのブロックはハッシュ関数をもっており、入力値を変えることで、ブロック全体のハッシュ関数の出力が変化する。ハッシュ関数の出力が条件を満たす値になったとき、正しいブロックとしてネットワーク全体で認め、直前のブロックと繋ぐ。このようにして、取引データを更新する。

ビットコインマイニングの実行は、インターネット上で無料配布されている「発掘プログラム」をコンピュータにインストールすることで可能となる。ビットコインマイニングには膨大な計算コストが必要となる。誰よりも早くビットコインマイニングに成功すれば、報酬として bitcoin を得る。つまり、ビットコインマイニングはネットワーク参加者が報酬を得るために、bitcoin の運営に協力するシステムである。ビットコインマイニングの概要図を Fig. 1 に示す。

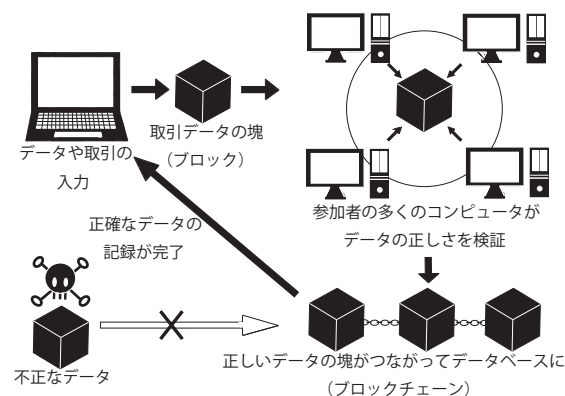


Fig.1 ビットコインマイニングの概要図

2.4 bitcoin の課題

課題の一つは、麻薬で得た不正資金や賄賂、テロ資金の出所やその受領者がわからなくなることである。これは bitcoin が匿名で使用出来るためである。また中央機関が存在しないため、これらを取り締まることができない。

二つ目に、価値が安定しないことが挙げられる。bitcoin を安いときに買い、高いときに売ることによって差額を収益とする人もいる。このため需要と供給による価格変動を繰り返す。さらに中央機関が存在しないため、これに対して金融政策が行われず、暴騰暴落が生じている。

3 ripple

3.1 ripple の概要

ripple は bitcoin の改良版として注目されている。ripple は仮想通貨ではなく、金融取引を行うためのインターネットプロトコルである。

ripple では、IOU（借書）を用いて取引を行う。IOU は受け手が了承すれば、色々な通貨に対応して発行できる。1XRP（ripplecoin の単位）の料金を支払えば、ドル、ユーロ、円、さらに bitcoin でさえ、金銭を受け渡しできる。つまり、IOU を用いることで両替が容易になる。

また、ripple は分散処理システムでありながら、中央機関が存在する。ripple の仕組みを創り出した ripple Labs が中央機関の役割を担っている。ripple Labs は銀行窓口のような役割を果たすゲートウェイや、特定ユーザのアカウントを利用停止できる。

3.2 IOU を使った取引の仕組み

IOU を使った取引では、実際には借金の付け替えを行っており、現金は動いていない。そのため、IOU を用いて取引を行うことで、一連の取引を簡略化し、手数料を抑える。

IOU は借用している金額に相当する価値があるものとして取引される。1つの IOU は人から人へと渡り、多くの取引に用いられる。しかし、借書書の観点から IOU を発行したゲートウェイがその IOU の現在の保持者に現金を借りているという1つの取引として扱う。つまり、その IOU を用いた数多くの取引が行われたとしても、2者の取引としてみなせる。そのため、多くの銀行や外貨両替所を介して取引するよりも手数料を抑えられる。IOU を使った取引の概要図を Fig. 2 に示す。

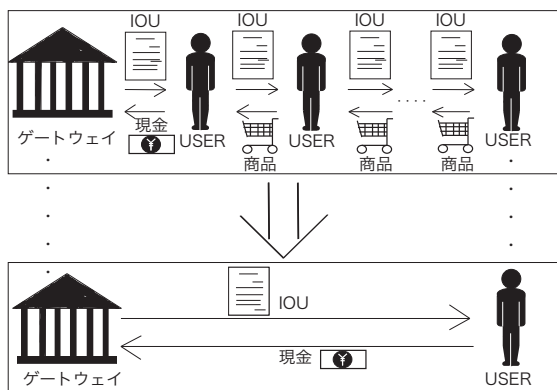


Fig.2 IOU を使った取引の概要図

3.3 bitcoin と ripple の比較

bitcoin と ripple は世界中で使える点、手数料が格安である点、支払いが早い点で共通している。しかし、大きく異なる部分が2つある。

一つ目に、中央機関が ripple のシステムには存在する点で異なる。中央機関が存在することで取引の承認が容易になり、より高速で、格安な送金が可能である。したがって、bitcoin で 10 分程度かかる支払いを ripple では数秒で行える。これは中央機関に提供される不特定のユーザグループが承認することによって、取引が成立するからである。また、ripple は中央機関が存在するため、bitcoin で問題になった不正資金の不透明性を解決している。ripple では匿名での取引ができず、さらに不正な口座を差し押さえることもできる。

二つ目に、bitcoin は通貨、ripple は IOU を用いる点で大きく異なる。bitcoin の場合、bitcoin という通貨で取引し、価値を保存する。しかし ripple では IOU で取引をし、実際の現金に両替することが基本となっている。そのため、ripple は価値の保存を現金で行う。暴騰暴落を繰り返している bitcoin より、国によって価値が保障されている現金のほうが価値の保存に向いている。通貨の取引の概要図を Fig. 3 に示す。

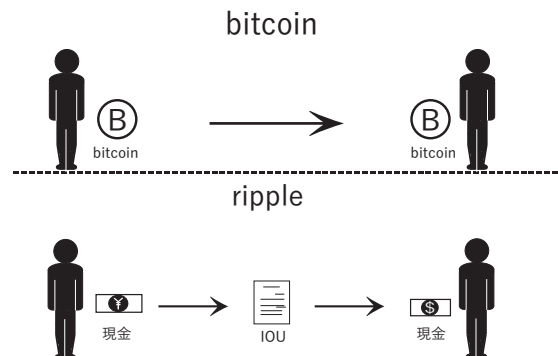


Fig.3 通貨の取引の概要図

4 現状から見る今後の仮想通貨

bitcoin や ripple は Shifts Hybrid card や e-coin のデビットカードが対応し、カードで利用できる。既存の VISA ネットワークを利用するため、VISA カード決算に対応しているならどこでも支払いができる。仮想通貨に対応するカードは増加している。仮想通貨は、カードでの利用に対応することで、より実用的になった。

bitcoin や ripple 以外の仮想通貨も勢いがある。ripple のように改良版として生み出された仮想通貨に Lumen や Litecoin がある。Lumen は ripple を基にしている。ripple との違いは価格変動を抑えるために毎年発行量が 1% ずつ増えることである。それに対して Litecoin は bitcoin の改良版で、ブロックの生成スピードに違いがある。bitcoin は 10 分に 1 つブロックを作っているが、ハッシュ関数が異なるため Litecoin は 2.5 分に 1 つ作っている。ブロック生成間隔が短いことはセキュリティレベルを低くしている。しかし、これにより取引の認証速度が 4 倍になる。どちらも誕生して間もない仮想通貨にもかかわらず、取引件数は首位の bitcoin に迫っている。

仮想通貨は、従来の決済方法に取って代わろうとしている。仮想通貨には送金の早さや手数料の安さなど多くの利点がある。そのため国外との取引が容易になる。今後、仮想通貨の利用が増加し、海外との取引が個人規模で活発になると予想できる。

参考文献

- 1) 岡田仁志, 高橋郁夫, 山重一郎: 仮想通貨-技術・法律・制度, 東洋経済新報社 (2015).
- 2) Satoshi Nakamoto: bitcoin: A Peer-to-Peer Electronic Cash System, (2008).