ブロックチェーン

川村 航平，高谷 友貴
Kohei KAWAMURA，Yuki TAKAYA

1　はじめに

仮想通貨を支える技術としてブロックチェーンがある．ブロックチェーンは仮想通貨の 1 つであるビットコインを実現するために誕生した．ブロックチェーンは P2P ネットワークを使用し，全ての利用者のコンピュータに同じデータを保存している．現在は汎用的な分散基盤として仮想通貨以外の領域への利用が拡大しようとしている．さらに，ブロックチェーンは参加するノードの利用形式によってパブリック型，コンソーシアム型，プライベート型に分類できる．

2　ブロックチェーンの概要

ブロックチェーンはネットワーク上での取引において高い信頼性を維持する技術である．ブロックチェーンは 1 つの中核的なサーバがデータを管理するのではなく，全ての利用者が同じデータを共有している．よって，データの改ざんを行うには全てのノードのブロックを改ざんしなければならない．そのため，改ざんは容易ではない．また，中核的なサーバがないため，大規模な障害が起こりにくい．さらに，高性能なサーバが不要であるため，低コストで勘定取引システムを実現することができる．ブロックチェーンの仕組みを Fig.1 に示す [1]．

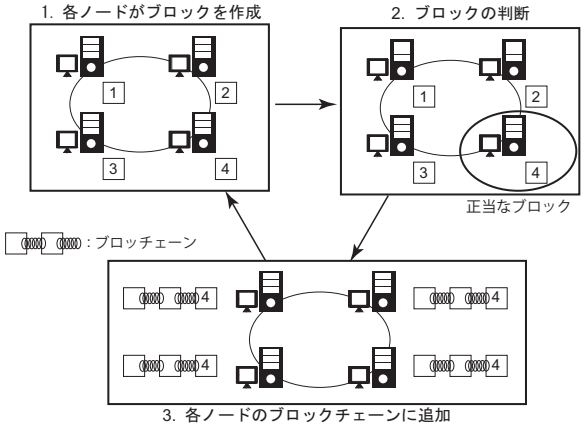

Fig.1　ブロックチェーンの仕組み

ブロックチェーンでは，取引であるトランザクションを各ノード間で共有している．そして，各ノードは一定時間ごとにトランザクションをまとめて 1 つのブロックを作成する．そして，コンセンサス・アルゴリズムを用いることで作成されたブロックに正当性があるかどうかを判断する．ブロックに正当性があると判断すると，そのブロックをブロックチェーンの最後に連結する．ブロックの連結はハッシュ関数を用いて行う．

3　ブロックチェーンの基盤技術

3.1　P2P ネットワーク

ブロックチェーンは P2P ネットワークを利用しており，全てのノードが同じデータを保有する．そして，あるノードでトランザクションが発生すると全てのノードにトランザクションのデータを送信する．また，全てのノードが同じ内容のブロックチェーンを保有しているため，ノードの一部に破壊，改ざんがあった場合でもデータを復旧することが可能となる．また，中核的なサーバがないため大規模な障害が起こりにくい．さらに，高性能なサーバが不要であるため，低コストでサービスを実現することも可能である．

3.2　コンセンサス・アルゴリズム

コンセンサス・アルゴリズムとはブロックチェーンにおいて各ノードが作成するブロックの中から正当なブロックを判断するアルゴリズムのことである．現在，ブロックチェーンの主な利用分野が仮想通貨の分野であるため，コンセンサス・アルゴリズムは仮想通貨の分野における使用を前提としたアルゴリズムとなっている．代表的なコンセンサス・アルゴリズムを以下に示す．

- PoW（Proof of Work）
- PoS（Proof of Stake）
- PoI（Proof of Importance）

PoW は主にビットコインにおいて使用する．各ノードが作成したブロックの正当性をビットコインの利用者全体で検証・承認することで，管理者を介さずに通貨（コイン）の移転を可能にする仕組みである．PoW ではトランザクションを承認し，ブロックを生成するノードをマイナー（採掘者）と呼ぶ．ブロックの生成にはナンスと呼ばれる任意の値とトランザクションにハッシュ関数を使用し，ハッシュ値を生成する．そのハッシュ値が指定した値以下となる場合にマイニングが完了する．マイニングとはブロックチェーンの信頼性を高める処理で，膨大な数の数学的計算を繰り返し，条件を満たすナンスを探すことを指す．マイニングでは総当たりによってナンスを求めるため，非常に多くのコンピュータ資源を必要とする．不正なブロックを追加するにはそのブロックを正当化する必要がある．しかし，不正なブロックを正当化するには膨大なコンピュータ資源が必要となるため，改ざんは事実上不可能である．

PoS は，PoW を応用したアルゴリズムである．通貨の保有量が大きく，通貨保有期間が長いほどマイニングの難易度を低くすることで PoW におけるコンピュータ資源の利用を抑えることが可能となる [2]．しかし，通貨保有量

が多い参加者ほどマイニングの難易度が低いため，大量にコインを保有する参加者が現れる可能性がある．

PoI は PoW と PoS を応用したアルゴリズムである [3]．通貨の保有量・保有期間に加え，直近の通貨の使用頻度の高さによってマイニングの難易度を低くする．そのため，大量のコインを保有する参加者の出現を解消することができる．

3.3 ハッシュチェーン

ハッシュチェーンはハッシュ値を使用して各ブロックを連結することである．ハッシュ値とはそれぞれのブロックを連結するために使用する値である．ハッシュチェーンの構造を Fig.2 に示す．

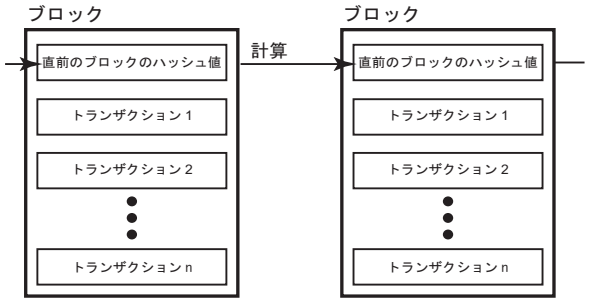

Fig.2　ハッシュチェーンの構造

ハッシュ値はトランザクションをまとめたブロックと 1 つ前のブロックのハッシュ値を用いて算出する．全てのブロックがハッシュ値によって連結しているので，あるブロックを改ざんするにはそのブロック以降の全てのブロックのハッシュ値を改ざんする必要がある．そのため，改ざんは容易ではない．

また，同じタイミングでブロックが作成される場合や，ネットワークの遅延・断絶によって局所的にブロックが作成にされる場合がある．このような場合，複数のブロックが同時にチェーンに連結する場合がある．この状態を分岐（フォーク）と呼ぶ．ブロックチェーンの分岐の概要図を Fig.3 に示す．

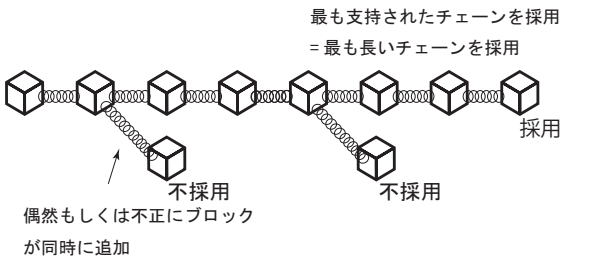

Fig.3　ブロックチェーンの分岐

チェーンが分岐した場合は一番長いチェーンを選択し，そのチェーンに自分のブロックを加える．ただし，短い方のチェーンはそのまま残しておく．

4　ブロックチェーンの分類

ブロックチェーンには不特定多数のノードが参加可能であるパブリック型，複数の組織・グループが参加可能であるコンソーシアム型，単一の組織・グループのみが参加可能であるプライベート型がある．パブリック型はブロックチェーンのデータの閲覧に制限がなく，不特定多数のノードが参加する事が可能である．そのため，悪意を持つノードが存在する可能性がある．よって，そのような悪意を持つノードを排除するためにコンセンサス・アルゴリズムが必要となる．パブリック型のブロックチェーンでは，ブロックを生成する場合にマイニングの難易度を高くすることで悪意を持つノードを排除している．そのため，パブリック型は膨大な計算コストが必要となる．この課題を解決するために，参加するノードを限定するコンソーシアム型とプライベート型が生まれた．コンソーシアム型とプライベート型のブロックチェーンはパブリック型と比較して，信頼性の高い利用者に限定されるため，不正が起こる可能性は低い．そのため，PoS や PoI などのより軽量なコンセンサス・アルゴリズムを使用することで，計算量の負荷を軽減することが可能となる．

5　今後の展望

ブロックチェーンでは P2P ネットワークを利用しており，全てのノードが同じデータを保有する．また，コンセンサス・アルゴリズムを使用してブロックの正当性を確認することができるため，不正が起こりにくい．そして，各ノードが同じブロックチェーンを保有しているため信頼性がインターネット上で確保できる．そのため，改ざんも起こりにくい．さらに，中核的なサーバや管理者が不要なため，性能が高いサーバを用意する必要が無い．そのため，低コストで信頼性の高い取引を実現することが可能となる．

ブロックチェーンによって扱うことが可能な情報には仮想通貨だけではなく，債権・債務，使用権，セキュリティ情報などがある．そのため，現在ビットコインで使用している大規模な取引決済システムだけではなく，様々な用途への応用が期待できる．例として，流通分野での活用が可能と考えられる．製造履歴の情報をブロックチェーン上で共有することで，データ連携も容易となりデータの正当性と一貫性の確保が可能となる．現状，技術的な課題も多いブロックチェーンではあるが，今後は幅広い業界で活用することが期待できる．

参考文献

1) 両角真樹，ブロックチェーン（分散台帳技術），株式会社 NTT データ経営研究所，https://www.mof.go.jp/pri/summary/topics/cy2017/201701a.pdf, 参照 Apr.13, 2017
2) Proof of Work，http://qiita.com/hshimo/items/625d548c61b9cab8d8d0，参照 Apr.13, 2017
3) NEM の説明書，http://nemmanual.net/proof_of_importance.html，参照 Apr.13, 2017