ethereum

川合 由夏
Yuka KAWAI

1　はじめに

近年，仮想通貨が流行し，仮想通貨を支える基盤技術であるブロックチェーンに注目が集まっている．ブロックチェーンとは，分散型ネットワーク上での取引において，高い信頼性を実現する技術である．現在，ブロックチェーンは主に仮想通貨の情報を扱っているが，仮想通貨以外の情報を扱うことも可能である．そのため，ブロックチェーンは様々な分野で応用が期待され，その結果，誕生したのが ethereum である．本稿では，ethereum の構造と特徴，利用例，今後の展望を述べる．

2　ethereum

2.1　概要

ethereum とは，ブロックチェーンを基盤にした分散型アプリケーションプラットフォームである [1]．分散型アプリケーションとは，中央管理者無しで自律的に動作するアプリケーションのことである．

ethereum の特徴としてスマートコントラクトがある．スマートコントラクトとは契約を実行することである．ethereum では取引情報だけでなく契約の情報を扱うシステムを構築することが可能である．そのため，仮想通貨のような取引決済システムだけでなく，金融やサービスなどの様々な分野への応用が期待されている．

2.2　ブロックチェーン

ブロックチェーンは，P2P ネットワークを利用し，同じ取引記録を全てのコンピュータで管理する [2]．ブロックチェーンの仕組みを Fig. 1 に示す．

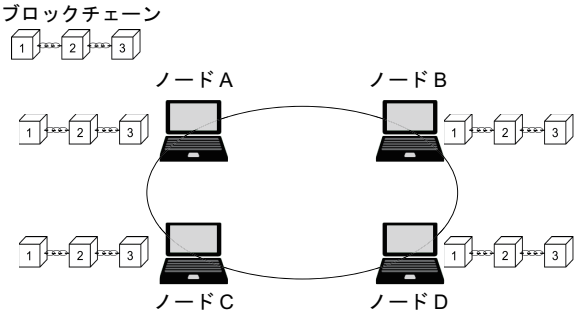

Fig.1　ブロックチェーンの仕組み

ブロックチェーンでは，P2P ネットワーク上の各コンピュータ（ノード）が一定時間ごとに取引をまとめたブロックを生成する．そして，ノードは生成されたブロックが正当かどうか検証を行う．過半数以上のノードが生成したブロックを正当と判断した場合，そのブロックを全ノードが持つブロックチェーンに加える．ブロックチェーン上の各ブロックは、直前のブロックのデータをまとめた値を持つ．

ブロックチェーンでは，全ノードが同じブロックチェーンを保有する．そのため，1 つのデータが壊れた場合でも他のノードが同じブロックチェーンを保有するため，データを復元できる．また，ブロックチェーンのブロックは時系列順に並んでおり，各ブロックが前後のブロックと関連している．そのため，データを改竄した場合そのブロック以降のブロックチェーンに矛盾が生じる．よって，改竄したデータを持つブロック以降のブロックを全て書き換える必要があり，改竄は容易ではない．

2.3　送金の仕組み

ethereum は，ブロックチェーンで取引情報と契約内容を管理する．トランザクションを実行する際に，ユーザはアカウントを使用する．以下に，ethereum の取引が発生した後の送金トランザクションの流れを示す．

1. 送信者がトランザクションを情報を送信する．
2. 送信されたトランザクション情報をまとめたブロックを生成する．
3. 各ノードがブロックの正当性を評価する．
4. 送金処理が完了する．

送信者がトランザクションを生成し，ethereum のネットワーク上に送信する．ネットワーク上に送信されたトランザクション情報は，各ノードの持つブロックに埋め込まれる．各ノードがブロックの正当性を評価し，過半数以上のノードがブロックを正しいと承認すると，全ノードが承認されたブロックをブロックチェーンに加える．その後，送信者が作成したトランザクションで指定した相手に送金する．

3　スマートコントラクト

3.1　概要

スマートコントラクトとは，契約の条件確認から決済までを自動的に実行することである [3]．ブロックチェーン上のコントラクトアカウントが持つプログラムを実行することで，スマートコントラクトを実行可能である．スマートコントラクトによって，ユーザ同士が直接契約を行い，取引を行う非中央集権のサービスを実現できる．Fig. 2 にスマートコントラクトの流れを示す．

コントラクトアカウントのプログラムに，契約内容を記述する．そして，イベントが発生すると，コントラクトアカウントが持つプログラムが契約内容の条件確認，契約の執行，価値の移転，決済をブロックチェーン上で自動で行う．スマートコントラクトを用いるメリットとして，第

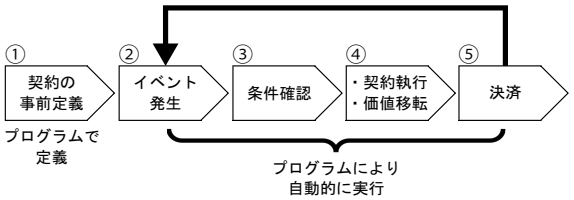

Fig.2　スマートコントラクトの流れ

三者機関を通さないことによる決済期間の短縮，コスト削減，ブロックチェーンを用いることによる不正防止が挙げられる．

3.2　外部アカウントとコントラクトアカウント

スマートコントラクトを実行するために，ethereum ではアカウントを使用する．ethereum のアカウントには外部アカウント（EOA）とコントラクトアカウントがある．EOA はユーザがトランザクション情報を送信する際に使用するアカウントであり，ユーザは秘密鍵でアカウントを管理する．ユーザは EOA を用いて，ethereum のネットワークに参加する．一方，コントラクトアカウントはプログラムを持ち，このプログラムがスマートコントラクトとして機能する．コントラクトアカウントはユーザが所持することはできず，ethereum のブロックチェーン上に存在する．また，EOA は他の EOA やコントラクトアカウントへのトランザクションを開始する．しかし，コントラクトアカウントは自分自身でトランザクションを開始しない．EOA から EOA へのトランザクションは，通貨の送金である．また，EOA からコントラクトアカウントへのトランザクションはスマートコントラクトである．

スマートコントラクトを実行するためにはコントラクトアカウントの生成と実行が必要である．Fig. 3 にコントラクトアカウント生成の流れを示す．

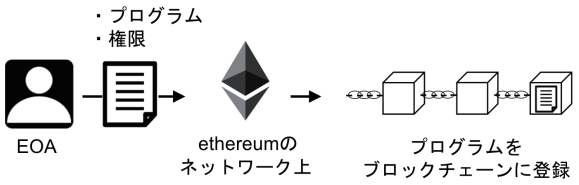

Fig.3　コントラクトアカウント生成の流れ

コントラクトアカウントを生成するために，まず EOA はプログラムを記述したトランザクション情報を，ethereum のネットワーク上に送信する．送信されたトランザクション情報はブロックに埋め込まれ，各ノードがブロックの正当性を評価する．過半数以上のノードに承認されたブロックは，ブロックチェーンに繋がる．このとき，コントラクトアカウントの持つプログラムはブロックチェーンに登録され，コントラクトアカウントのアドレスを決定する．ブロックチェーン上に存在するコントラクトアカウントの実行にはコントラクトアカウントを使用する権限とアドレスが必要となる．EOA はコントラクトアカウントのアドレスを指定し，ブロックチェーン上のコントラクトアカウントを実行する．

3.3　スマートコントラクトの利用例

スマートコントラクトは従来の契約，取引の自動化を可能とする．従来の契約とスマートコントラクトを用いる契約を，家をを借りる場合を例に Fig. 4 に示す．

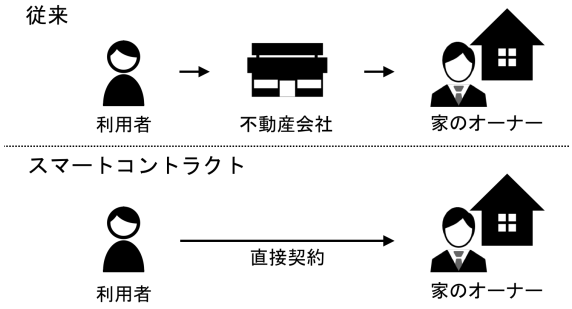

Fig.4　家を借りる場合の比較

従来，家を借りるためには不動産屋に出向き，賃貸契約を行う必要があった．不動産会社で賃貸契約が成立すると，利用者は家を借りることできる．一方，スマートコントラクトを利用すると，利用者は家のオーナーと直接契約を行うことが可能である．家のオーナーは，プログラムで契約内容を事前に定義する．利用者が家を借りる場合，プログラムによって契約条件の確認が行われる．家のオーナーと利用者で契約が成立すると，利用者は家を借りることができる．このようにスマートコントラクトは，第三者機関を通さずに，ユーザ同士で直接契約ができる．

4　今後の展望

ethereum にはビットコインにはないスマートコントラクトという特徴がある．スマートコントラクトは，ブロックチェーンを仮想通貨取引以外の分野に応用することを可能にする．

ethereum を様々な分野のビジネスに活用することを目標とした ethereum 企業連合が 2017 年 2 月に設立した．現在，ethereum 企業連合には Microsoft やトヨタ自動車など約 300 社が加盟している．ethereum 企業連合によって， 企業サービスやアプリケーション開発が行われることにより，金融以外の分野にも ethereum が応用されると考えられる．

参考文献

1) a-mitani，Ethereum　入 門 ，https://book.ethereum-jp.net/，参照 Apr.15，2018
2) 荒牧裕一，ブロックチェーンアルゴリズムの分類と問題点，京都聖母女学院短期大学研究紀要，Mar，2012
3) Blockchain Biz，スマートコントラクト，http://gaiax-blockchain.com/smart-contract，参照 Apr.17，2018