おさえておきたい基本や、最新動向を解説するコーナーです。

Ethereumスマートコントラクト
―暗号通貨から拡がるプラットホーム―

1 はじめに

2008年にSatoshi NakamotoがBitcoin(ビットコイン)を公開したことで誕生したブロックチェーンは、昨今ではメディアで目にしない日がなくなった。ブロックチェーンと聞くと暗号通貨を思い浮かべる人も多いだろう。今、ブロックチェーンは、暗号通貨としてはもちろん、スマートコントラクトと呼ばれるアプリケーション開発におけるプラットホームとしても注目されている。特に、分散アプリケーション(DApps)の設計や、非代替性トークン(Non-Fungible Token, NFT)によるアート販売など、その展開は多岐にわたる。本稿ではブロックチェーンについて、スマートコントラクトおよびその関連技術を中心に解説する。

2 Ethereumスマートコントラクト

Ethereum(イーサリアム)は、Bitcoinに次ぐ市場規模を持つ暗号通貨である。このEthereumを基盤として動作する、ブロックチェーンを利用した非中央集権型アプリケーションのプラットホームが、Ethereumスマートコントラクトである。Ethereumスマートコントラクトは、昨今では後述する非代替性トークンを通じたアートの販売や、分散アプリケーションの構築や実行など、さまざまな利用がされている。

そもそも、スマートコントラクトとはどのような概念であるか。実は、スマートコントラクトの概念は、ブロックチェーンが登場するよりも以前、1996年にNick Szaboが執筆した「Smart Contracts:Building Blocks for Digital Markets」に登場している。1990年代は“契約をスムーズに行う技術”という定義であり、これは暗号技術としての電子取引が当時活発に研究されていた背景によるところも大きい。著者の感覚では、その当時の概念は、今の概念ほど詳細かつ複雑なものではなかった。

ブロックチェーンが広まった現在、スマートコントラクトは、Ethereumの開発者であるGavin Woodが提唱した概念が一般的なものとなっている。いわく、スマートコントラクトは「Ethereumネットワークプロトコルの一部として、EVM(Ethereum Virtual Machine)の文脈として確定的に実行される、変更不可能なコンピュータプログラム」とされており、世界状態機械(World-State Machine)とも評される。これは非常に興味深い概念である。SF映画では、世界中のコンピュータを繋いで、みんなの力を合わせて作中の難題を攻略する場面がしばしば見受けられる。著者の認識では、Ethereumスマートコントラクトは、

Ethereumのネットワーク内における計算機を相互に繋ぐことでネットワーク全体で一つの機械となり、誰でもその実行ができるという意味で、SF映画のコンピュータを体現するようなものである。そう思うと、なかなかに厨二心をくすぐられる技術である。

Ethereumスマートコントラクトの話に戻ると、上述した概念をより大雑把に解釈するならば、やはり一種のプログラミングプラットホームになる。ただし、C言語など従来のプログラミングプラットホームと比べて、Ethereumスマートコントラクトは独自の概念が多くある。本稿では紙面の都合上、特に重要な概念である「コントラクト」と「燃料(gas)」について述べる。

まず、Ethereumスマートコントラクトでは、一つのプログラムがコントラクトという単位で扱われる。C言語では関数が最小単位だが、Ethereumスマートコントラクトではコントラクトが最小単位となる。Ethereumにおけるコントラクトの記述にはSolidityやVyperといった高級言語が使用され、そのコードを記述することで暗号通貨の取り引きのみでなく、複雑な処理を必要とする取り引きなどを容易に実現できるようになる。このSolidityなどで記述されたコントラクトはEVMバイトコードへコンパイルされ、ブロックチェーン上で初期化・展開される。このブロックチェーン上に展開される動作まで含めてディプロイと言う。記述されたコントラクトの実際の処理は、専用の仮想マシンであるEVMで行われる。

この時、EVMでのコントラクトの実行において、重要な役割を果たす概念が燃料である。燃料はコントラクトの実行に必要となる手数料であり、そのコントラクトに与えられるトランザクションのサイズと、コントラクトの実行ステップ数によって決定される。手数料の支払先はEthereumネットワーク上に存在するマイナーと呼ばれるノードであり、このマイナーが自身の環境に構築されたEVMを通じてコントラクトを実行する。この時、燃料はコントラクトの実行に関するトランザクションのマイニング処理、すなわちプログラムの実行に対する成功報酬として、マイナーに与えられる。燃料の値はトランザクションの発行者が自由に設定できる。一般には燃料を高く設定するとマイナーへの報酬が増えることから、優先的にそのトランザクションを処理してもらえる可能性が高くなる。また、トランザクションを発行する際、そのトランザクションに使用できる燃料の上限値(gasLimit)を指定する必要がある。

このように燃料の概念を述べると「ブロックチェーンだからプログラムの実行もお金で解決」と安直に思う人もいるかもしれない。実は、この燃料は理論計算機科学の観点から、きわめて重要な意味を持っている。そもそも一般に、プログラムはいつ処理が終了するかわからない「停止性問題」が、有名な計算機科学の問題として知られている。大まかには、燃料はこの停止性問題をうまく扱っているのである。さきほど、Ethereumスマートコントラクトはいろいろな計算機を繋いで皆で利用するという旨を述べたが、これは裏を返せば誰かが無限ループを回すことで、不当に計算機資源を占有してしまう問題なども含んでいる。プログラムの停止性問題から、この資源がいつ解放されるかわからないため、ともすれば重大な欠陥ともなりかねない。これに対し、Ethereumスマートコントラクトでは燃料が尽きれば処理が止まり、計算機資源が解放される。つまり、燃料に応じてプログラムがいつ終了するかわかるのである。これはコード内に不具合があったとしても終了することが保証される。例えば、無限ループに陥ってしまうようなコードであっても、燃料の上限値に達した時点で必ずコントラクトの実行が終了する。

つまり、Ethereumスマートコントラクトとは、理論計算機科学の問題を暗号通貨というお金の問題で柔軟に解決している、非常に興味深い道具と言える。

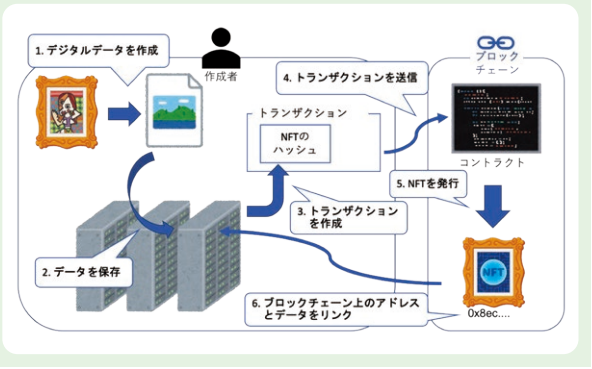
3 非代替性トークン(NFT)

Ethereumスマートコントラクトを語る上で近年最も注目を浴びているものが、トークンという概念である。ここで言うトークンとは、Ethereum上で作成、取り引きが可能なEtherとは異なる暗号資産と言える。特に、近年注目されているNFT(Non-Fungible Token)は、このトークンの一種で非代替性トークンと呼ばれる。Ethereumでは、ERC(Ethereum Request for Comments)-20という規格によってトークンの仕様が初めて標準化された。ERC-20は代替性トークンの規格であり、これに沿って作成されたトークンは、それぞれが等価であり代替可能な

トークンであるといった特徴がある。このERC-20から着想を得て提案されたのが非代替性トークンの規格EIP(Ethereum Improvement Proposals)-721であり、その後ERC-721によって標準化された※1。ここでNFTとは、非代替性、つまり代替品が存在しないトークンであり、デジタル資産などと紐づけられる。NFTはスマートコントラクトによって管理され、そのコントラクトのアドレスとトークンIDと呼ばれる識別子によって、唯一であることが保証される。このような仕組みから、NFTはその所有者がスマートコントラクトによって管理、保証される。NFTの例としては、デジタルアートやゲームのキャラクターなどがNFTとして作成されることがあり、さらにツイートなどがNFTとして売買されていると話題にもなっている※2。

NFTの作成は2種類のパターンが存在するが、今回はデジタルアートやツイートなどを作成する際の、トップボトム型と呼ばれる作成方法について図1で紹介する※3。

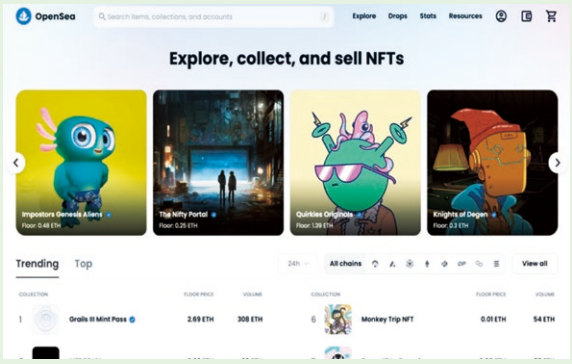
図1 NFTの作成方法(トップボトム型)



この方法では、まずNFTとなる資産が作成される。そして、それをNFTとするためのトランザクションが作成され、スマートコントラクトによってその資産とNFTが紐づけられる。

デジタルアートから作成されたNFTはその後売り買いされるが、それらの取り引きの多くはマーケットプレイスで行われる。メジャーなものとしては、図2のOpenSeaなどが挙げられる。NFTの普及に伴い、それを扱うマーケットプレイスも海外だけでなく、国内でもさまざま登場している。マーケットプレイスによって、取り扱う仮想通貨やNFTの種類が異なってくるため、興味がある読者は、ぜひ調べてみてほしい。

図2 OpenSea (https://opensea.io)



※1 https://eips.ethereum.org/EIPS/eip-721
※2 https://nonfungible.com/reports
※3 Qin Wang, Rujia Li, Qi Wang, Shiping Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," arXiV, abs/2105.07447, 2021.

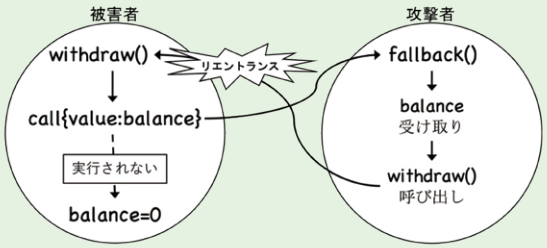
セキュリティに関する問題

Ethereumスマートコントラクトは、ブロックチェーンの性質を持つ一方、その性質に起因し、セキュリティに関するさまざまな問題も存在する。プログラムのバイトコードがブロックチェーン上に保存・公開される、透明性がその一例である。これにより、ブロックチェーン上でプログラムが実行可能となる一方で、誰でも情報を閲覧できるため、攻撃者がその解析をすることも容易となってしまう。また、ブロックチェーン上に上げられたプログラムは変更不可能であり、攻撃者によって脆弱性が発見されてしまった場合は、それを踏み台として長期的に攻撃されてしまう可能性があるため、コントラクトの作成には注意が必要である。また、スマートコントラクトではプログラムの実行に手数料が必要であり、金銭的な価値のあるものを取り扱うことが多いといった特徴から、攻撃が金銭的な被害に直結する。実際に発生した事件として、Ethereumスマートコントラクトにおいて悪名高い事件であるThe DAO事件について紹介する。

2016年に発生したThe DAO事件は、スマートコントラクトの脆弱性の一つであるリエントランシーが踏み台にされた。リエントランシーの概要を図3に示す。リエントランシーでは、fallback関数と呼ばれるEthereumの記述言

語特有の関数が、通貨の受取時に実行されるという性質が悪用され、送金を行う関数を不正に再度呼び出している。この呼び出しが「リエントランス」と呼ばれる。この時、送金による残高の更新が呼び出し前に行われていない場合は、被害者コントラクトが持つすべての通貨が送金されるか、実行に使用できる手数料の上限に到達するまでリエントランスが繰り返される。リエントランシーを踏み台にされた結果、ホワイトハッカーによる通貨の救出が行われるまでに、事件当時の価格で約52億円相当の通貨が攻撃者によって抜き出された。

図3 リエントランシーの概要



このような脆弱性を除外するために、Ethereumで最も一般的な記述言語であるSolidityでは頻繁にアップデートが行われており、2023年1月現在ではv0.8.17までがリリースされている。実際の対策の例としては、Integer Overflow／Underflowや、Default Visibilityと呼ばれる脆弱性に対する機能などが追加されている。実際に、Unchecked CallやLocked Moneyと呼ばれる脆弱性に対して、その効果があることも確認されている※4。

また、スマートコントラクトのセキュリティについての研究もさまざまに行われており、脆弱性の解析ツールなども静的解析ツールのOyente※5を筆頭にMythril※6やSmartCheck※7などが開発されている。動的解析ツールはスマートコントラクトの特性から数が少ないものの、単一の脆弱性に特化し、さらにコントラクト間などでの脆弱性も解析可能なSereum※8なども開発されている。これらのツールを評価した研究※9 ※10なども行われているため、開発者の方にはぜひ、これらを参考にしたセキュアなスマートコントラクト開発を期待している。

※4 Chihiro Kado, Naoto Yanai, Jason Paul Cruz, Shingo Okamura, "An Empirical Study of Impact of Solidity Compiler Updates on Vulnerabilities," In Proc. of BRAIN 2023.
※5 Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor, “Making smart contracts smarter,” In Proc. of CCS 2016.
※6 Bernhard Mueller, “Smashing ethereum smart contracts for fun and real profit” In Proc. of HITB Security Conference 2018.
※7 Sergei Tikhomirov, Ekaterina Voskresenskaya, Ivan Ivanitskiy, Ramil Takhaviev, Evgeny Marchenko, and Yaroslav Alexandrov, “SmartCheck: Static analysis of ethereum smart contracts,” In Proc. of WETSEB 2018.
※8 Michael Rodler, Wenting Li, Ghassan O Karame, and Lucas Davi, “Sereum: Protecting existing smart contracts against re-entrancy attacks,” In Proc. of NDSS 2019.
※9 Thomas Durieux., João F. Ferreira, Rui Abreu. and Pedro Cruz, “Empirical review of automated analysis tools on 47,587 Ethereum smart contracts,” In Proc. of ICSE 2020.
※10 Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur and Heung-No Lee, “Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract,” IEEE Access, Vol. 10, 2022.

5 終わりに

本稿ではブロックチェーンの解説として、Ethereumスマートコントラクトについて、その仕組みと、昨今の主要なアプリケーションであるNFT、近年のセキュリティ研究の動向について紹介した。本稿では書ききれなかったブロックチェーンの応用技術の設計や、また、脆弱性の諸問題などもあるが、これはまたどこかの機会があれば紹介したい。

最後に著者が思うこととして、ブロックチェーンは進化が早すぎる技術であるということを述べたい。ブロックチェーンはさまざまなメディアで取り上げられ、今では電車の中など街中でもSatoshi Nakamotoの名前やNFTという単語を目にするようになっている。一方で、これらの技術に問題はないのかという専門家による詳細な分析が、大衆への急速な普及に追い付いていないと著者は感じている。本稿を読むことで、わずかにでもブロックチェーンに興味を持ってもらい、この専門家による分析と大衆への普及の溝を埋めたいと思える人が出てくれることを願っている。

（加道ちひろ　大阪大学　大学院情報科学研究科）
（矢内直人　大阪大学　大学院情報科学研究科）