暗号資産Moneroの匿名性を支える技術

花村 直親[1]

,

概要：匿名性を主たる特徴とした暗号資産である Monero について、匿名性を実現する手法と解決するプライバシー課題に基づいた分類と調査を行った。まず暗号資産におけるプライバシー課題を分類し、次に各プライバシー課題に Monero が対応する匿名性機能の分析を行うことで Monero の解決する課題を定義した。最後に匿名性の実現手法について、組み合わされた技術要素を分解することで Monero が匿名性を実現している方法を検討した。

キーワード：Monero, 暗号資産、匿名性、リング署名

Privacy Enhancing Technology in Monero

Naochika Hanamura[1]

,

Abstract: This work examines privacy method and privacy issues Monero, which is crypto asset whose main feature is anonymity. First, we classify privacy issues in crypto assets. Second, we defined privacy issues which Monero would solve by analyzing the anomynity function that Monero corresponds to each privacy issue. Finally, we considered the method which Monero realizes anonymity, by decomposing the combined technical elements.

Keywords: Monero, Cryptoassets, Privacy, Ring Signature

1. はじめに

ブロックチェーン技術は暗号資産を支えるテクノロジーとして広く注目を集めている。ブロックチェーンは不特定多数の参加者がいる状態においても動作するシステムとして、Bitcoin[1] のアイデアと共に発表された。

Bitcoin は 2009 年に稼働してから年々多くの人がネットワークに参加して価値を増やし、暗号資産の時価総額を掲載しているサイトである CoinMarketCap[*1]によると 2.2 兆ドル以上の時価総額を持つようになった。Bitcoin 以外にも Litecoin[*2]、Ethereum[*3]など多くのブロックチェーンが存在しており、決済に使いやすくすることを目的にしたものや、チューリング完全性のあるプログラムをブロックチェーン上で動かすスマートコントラクト機能を用いているものなど、Bitcoin とは異なる課題に対応している。Bitcoin の持つ課題の 1 つにプライバシーの問題がある。Bitcoin はアドレスやトランザクションが透過的であり、取引の履歴が参加者から見えているため、アドレス間の関係性が判明する手がかりとなる。例えば、1 つのアドレスの所持者が判明した場合、そのアドレスと取引のあるアドレスについて、その所持者と関係や取引関係のある人間であることが推測できてしまう。このようなプライバシーの課題を解決するためにトランザクションが匿名性を持つ

[1] naomasabit@gmail.com

[*1] https://coinmarketcap.com/ 2022 年 1 月閲覧

[*2] https://litecoin.org/

[*3] https://ethereum.org/en/