暗号資産台帳の匿名性と特定・追跡性についての考察

A Note on Anonymity and Specifibility/Traceability of CryptoAsset Ledger

才所　敏明[*1]
Toshiaki Saisho
[*1] (株)IT 企画
Advanced IT Corporation

辻井　重男[*2]
Shigeo Tsujii
[*2] 中央大学研究開発機構
R&D Initiative, Chuo University

櫻井　幸一[*3]
Kouichi Sakurai
[*3] 九州大学大学院システム情報科学研究院
（株）国際電気通信基盤技術研究所

1. はじめに

一般に暗号資産台帳には、資産移転記録を構成する提供情報・受取情報が登録されている。最初の暗号資産 Bitcoin の移転記録 Transaction には以下の情報が登録されている。

提供情報：提供に使用する原資、原資の所有権情報
受取情報：受取者情報、受取額（送金額）

Bitcoin では移転記録の長期保存・管理により、新たな資産移転要求の処理を可能としている。

一方、受取資産の移転が完了した移転記録は以降の資産移転には使用され無いため、不必要な移転記録の台帳からの削除等により、管理する台帳の軽量化、資産移転処理の効率化を目指す暗号資産も存在する。

本稿では、11 の暗号資産 Bitcoin、Monero、Zcash、Grin、IOTA、Obyte、Aidos Kuneen、Dero、Nano、Hedera Hashgraph、Tangram の調査結果をもとに、暗号資産によって異なる台帳登録・管理情報から暗号資産の分類を実施、台帳登録・管理情報の違いが暗号資産の匿名性および特定・追跡性の実現へ与える影響・課題等について考察する。

2. 台帳登録・管理情報による暗号資産の分類

暗号資産の移転要求の妥当性検証には、提供者の保有資産の確認が不可欠である。保有資産確認方法として、個々の資産移転記録から確認する方法と、資産管理単位ごとに集計された資産残高から確認する方法、の 2 種に分類できる。

(1) 資産移転情報を台帳に登録・管理する暗号資産

Bitcoin で採用されている方法であり、多くの暗号資産 Monero、Zcash、Grin、IOTA、Obyte、Aidos Kuneen、Dero が採用している。

この方法の課題は、台帳の容量増加問題である。台帳容量増加が暗号資産システムの性能に影響を与えないよう、工夫が必要となる。

その一つの方法として、IOTA では不定期に snapshot と呼ばれる不要な資産移転記録の剪定が行われている。移転要求処理に不要な古い移転記録は台帳から抹消されることになる。また、Grin では cut-through という仕組みにより、ブロック内で提供・受取が完結する移転情報はそもそも台帳に登録されない。台帳に登録されない資産移転情報が存在することになる。

(2) 資産残高情報を台帳に登録・管理する暗号資産

Nano、Hedera Hashgraph、Tangram が本手法を採用している。

Nano、Hedera Hashgraph は、利用者識別情報ごとの資産残高で表現される暗号資産分布を定期的に台帳に登録・管理し、資産残高をベースに新たな資産移転要求を処理する。資産移転要求はラティス状の別の台帳に記録され、承認された移転要求により定期的に暗号資産分布が更新され、台帳に登録される。暗号資産分布に反映された移転記録、および過去の案資産分布は、以降の資産移転要求の処理には不要であり、削除可能である。

Tangram は、利用者識別情報ごとではなく暗号資産識別情報ごとの残高を管理する。資産移転要求は、検証者（ノード）で妥当性を確認された後に、暗号資産識別情報ごとの残高に反映される。反映された資産移転要求情報は台帳には一時的にも記録されない。

3. 匿名性及び特定・追跡性に関する考察

台帳情報による暗号資産分類ごとに、以下、匿名性及び特定・追跡性に関する現状・課題を整理している。

(1) 資産移転情報を台帳に登録・管理する暗号資産

匿名性の観点からは、登録情報は少ない方が好ましく、提供情報、受取情報から構成される資産移転情報が登録・管理される本分類の暗号資産は、台帳登録情報から利用者の情報が漏れないよう、匿名化の仕組みが課題となろう。

特定・追跡性の観点からは、強い匿名化の工夫がなされているにせよ、過去から現在までの提供情報・受取情報が台帳上に存在するため、匿名化を実施した提供者の協力を得て、あるいは協力無しで、匿名化の仕組みの解除等の工夫により、特定・追跡は可能であろう。但し、IOTA や Grin のように、台帳から資産移転記録が削除される、あるいはそもそも一部の移転情報が登録されない場合、利用者・資産の確実な特定・追跡性は保証できない。削除された資産移転記録、登録されない移転情報の記録・管理の仕組みが課題となろう。

(2) 資産残高情報を台帳に登録・管理する暗号資産

匿名性の観点からは、台帳に登録される利用者識別情報、暗号資産識別情報、資産残高情報の匿名化が課題となる。

特定・追跡性の観点からは、登録されている利用者識別情報、暗号資産識別情報、資産残高情報から、資産移転情報を特定するのは困難であり、資産移転情報の記録・管理の仕組みが課題となろう。

4. おわりに

主要な 11 の暗号資産を対象とした調査・分析から、暗号資産台帳に登録・管理される情報に基づき暗号資産の分類を実施、その分類ごとに匿名性および特定・追跡性との関係についての考察を実施した。

謝辞　本研究の一部は，JSPS 科研費 基盤(B) JP18H03240 の支援を受けている．