SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

NFT 流通プロセスにおける不正検知のための監査システム
An Audit System for Fraud Detection in NFT Exchanges

東　知哉 *　　白石　善明 *　　今村　光良 †
Tomoya Azuma　　Yoshiaki Shiraishi　　Mitsuyoshi Imamura

掛井　将平 **　　廣友　雅徳 ††　　森井　昌克 *
Shohei Kakei　　Masanori Hirotomo　　Masakatu Morii

キーワード Non Fungible Token, 双線形写像, ブロックチェーン, Ethereum

あらまし

Non Fungible Token（NFT）において，その売買の取引は耐改ざん性を持つブロックチェーン上で行われる．その一方で，発行・取引や購入者への販売情報の提供を行う発行・取引機関の内部の処理についてはその透明性は保証されているわけではない．手続き通りに行われた NFT の発行の記録をブロックチェーン上に記録したとしても，その後の発行・取引機関の内部における不正によって，NFT 発行情報の独占・改ざん等により不当な利益を得ることが懸念される．ユーザの保護という観点からは，発行・取引機関が手続きに従った処理を行っていることを第三者が確認できることが求められる．

本論文では双線形写像とブロックチェーンを利用した発行・取引機関の監査システムを提案する．図 1 は提案するシステムの概要を示している．各エンティティが行う暗号処理は双線形写像を利用しており，共通するパラメータ，取引や監査のログはブロックチェーンを介して共有される．NFT を登録する “Upload フェーズ” と発行・取引機関の手続きを監査する “Audit フェーズ” のプロトコルは，クラウドストレージの監査を行う Provable Data Possession（PDP）システムの一つ [1]を基にしている．ブロックチェーンにログを残す PDP システムを踏まえることで，監査機関は発行・取引機関が所持するデータである NFT の取引記録について，ブロックチェーンに記録した取引ログとの整合性を検証することができる．そして，提案システムを Ethereum を用いて実装し，その安全性について議論している．

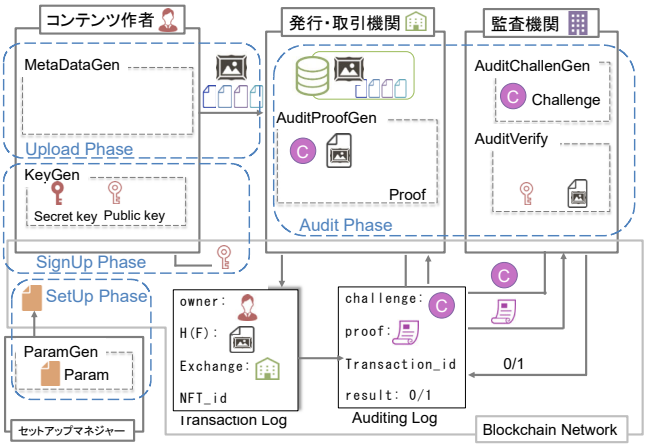

図 1 ブロックチェーンと双線形写像を用いた
発行・取引機関監査システムの概要

参考文献

[1] Y. Xu, C. Zhang, G. Wang, Z. Qin and Q. Zeng, "A Blockchain-Enabled Deduplicatable Data Auditing Mechanism for Network Storage Services," in *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp.1421-1432, 1 July-Sept. 2021, doi: 10.1109/TETC.2020.3005610.

* 神戸大学大学院工学研究科
Kobe University
† 野村アセットマネジメント（株）
Nomura Asset Management Co., Ltd
** 名古屋工業大学サイバーセキュリティセンター
Nagoya Institute of Technology
†† 佐賀大学理工学部
Saga University