

ブロックチェーン Ethereum とマーケットプレイス Magic Eden での NFT 取引の整合性の調査

遠藤 冴花 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1 はじめに

近年、暗号化した取引履歴を鎖のように繋いでいく技術であるブロックチェーン技術を利用した仮想通貨が注目を集めている。2008年に登場したビットコインをはじめとした様々な仮想通貨が用いられている中で2017年頃から特に注目されているものに NFTがある。NFT(Non-Fungible Token [非代替性トークン])は、デジタルアートをはじめとしたデジタル商品の唯一性とその所有者を保証することができるようになり、新しいマーケットプレイスとして浸透している。

NFTは公用分散型台帳ブロックチェーン技術を使用して取引の記録を確認することができる一方、その真正性は事業者にゆだねられている。そのため、取引を個人間で行うことから詐欺事件も発生している。2022年2月に最大手の NFT マーケットプレイス OpenSea はユーザーを狙ったフィッシング詐欺で300万ドルに相当する NFT の不正流出 [1] があったことを公表している。

そこで、本研究では、NFT 取引で主に使用されている通貨 ETH の取引をブロックチェーンのエクスプローラとマーケットプレイスの2つのデータソースから観測し、取引が整合しているか調査を行い、NFT 取引の信頼性を確認することを目的とする。

2 Etherscan と Magic Eden

2.1 システム構成

本研究ではブロックチェーンエクスプローラと NFT マーケットプレイスでの取引履歴をユーザごとに確認し、取引上の整合性を確認することを目的とする。システム構成図を図1に示す。

本研究ではブロックチェーンエクスプローラ Etherscan, NFT マーケットプレイス Magic Eden を調査する。

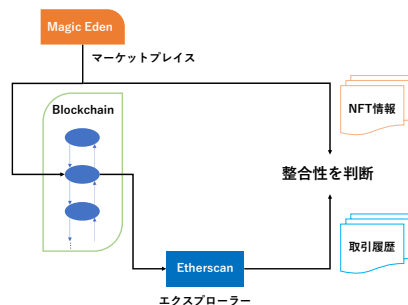


図1 システム構成図

2.2 Etherscan

Etherscanはブロックチェーン Ethereum 上の NFT 取引で主に用いられている通貨である ETH でのやりとりの履歴を閲覧するサービスプラットフォームである。

NFT 取引で扱われている暗号資産は ETH が主流である。

2.3 Magic Eden

Magic Eden は多くある NFT マーケットプレイスの中の1つである。NFT の売買をするために利用するサービスのひとつで、Magic Eden は特にアートに分類される NFT の取引が活発である。

3 実験

3.1 目的

本実験は Etherscan と Magic Eden のユーザごとの取引データを集めて比較し、同じ取引が両方のデータに存在しているかを判別し、不整合が発生していないかを明らかにする。調査対象の Ethereum アドレスを表1に示す。

すべての取引データは公開されているので、マーケットプレイスの NFT データを照合することで、NFT の所

†Kikuchi Laboratory, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

表 1 Ethereum アドレス一覧

	Ethereum アドレス
1	300d65b82c39ca315cbd8c26c9e20d2267f8edee
2	7dff47820fa7ef1c2eae54803b9c06a6fcace40d
3	4749e63a25c34501bc579edcdaa364d3b2206073
4	1f8b5b6220eee763c60ac064da06fcd63533fd00
5	f81e01761184dcfb5e7475ea51e1dc497fdb6ac
6	879f941bac811c379b2a0212f158d8ecbd741c91
7	40661c8a3c48f7f8ecac1f962a6ce8a1b7dc614c
8	d2c0c0cfbeb4a72042c53a31b863a29f9d7cdcd0
9	28f8969540165a0a0978d0ec62ae8c9dde843232
10	4c6686ed75d0c6685cc26fdab818cb975b5256e3

$$\text{不整合率} = \frac{\text{Etherscan} \times, \text{Magic Eden} \circ \text{の取引数}}{\text{Magic Eden での取引数}}$$

図 2 不整合率の定義

有権を判断することができる。

3.2 不整合の定義

Magic Eden の取引履歴にあるが、Etherscan で確認できない取引と、その逆、すなわち、Ethereum のみにある取引を不整合と定める。不整合の割合を調査する。不整合率を Magic Eden での取引数の内、Magic Eden で確認されて Etherscan で確認できなかつた取引数の割合とする。式を図 2 に示す。

3.3 使用プログラムと実験の流れ

本研究では、同様の実験を Opensea で行っている Yang Liyi のプログラム [2] を使用し行う。このプログラムは Magic Eden の NFT 取引情報を収集するために selenium webdriver を使用して、NFT 取引に使用されている Ethereum スマートコントラクトと Etherscan で確認できる NFTID の取得を行う。プログラムから得られたデータを csv に出力し、それらを比較し 3.2 で述べた不整合にあたる取引数を調査する。実験の流れを図 3 に示す。

3.4 実験結果

実験結果を表 2 に、本研究で不整合と判断したものの割合(不整合率)を表 3 に示す。アドレスごとにトラザクション数に偏りはある。Etherscan で確認できたトラ

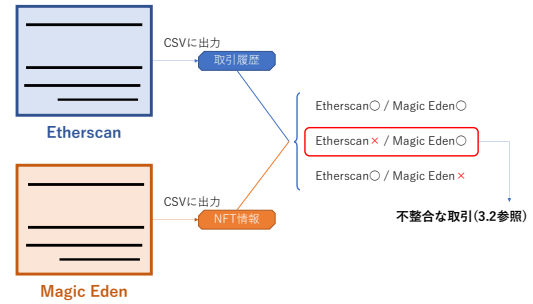


図 3 実験の流れ

表 2 観測された取引数

	Etherscan	Magic Eden	Eth ○ ME ×	Eth × ME ○
1	186	173	17	21
2	147	140	21	15
3	119	132	8	11
4	158	151	12	0
5	171	156	38	7
6	17	72	0	6
7	166	179	3	2
8	31	22	0	0
9	13	15	2	0
10	20	10	1	0
total	1028	1059	102	62

ザクション数は 1028, Magic Eden で確認できたトラザクション数は 1059 である。不整合と定義される Magic Eden で確認でき、Etherscan で確認できなかつたトラザクション数の合計は 62 である。結果から求められる不整合率は 5.85% となり、Open Sea と Etherscan で調査した [2] 不整合率は 4.42% となった。

3.5 考察

このように NFT マーケットプレイスで行われた取引の履歴がブロックチェーンエクスプローラーのほうで確認されない不整合率は Magic Eden と Open Sea での結果に大きな差がみられなかつたことからほかのマーケットプレイスで同じ手法で調査した場合も同じような結果になるのではないかと予想する。マーケットプレイスが Etherscan 側に取引情報を送信したときに何かしらの原因、例えばトラザクション情報の送信のラグ等が考えられる。

表3 不整合率

	不整合率	Eth 未確認	ME・OS 取得数
Magic Eden	5.85%	62	1059
Open Sea	4.42%	32	724

4 おわりに

実験結果から Magic Eden で購入した NFT の取引が Etherscan で確認ができないものは約 5.85% あることが分かった。Opensea での不整合率は約 4.42% となり、ほぼ同量である。実際に不整合があるものを観測し、原因を直接確認する等でより高い精度を目指すことを今後の課題とする。

参考文献

- [1] THE BLOCK - Supposed 17-year-old artist sells \$138,000 worth of fake NFTs and disappears (<https://www.theblock.co/post/119150/supposed-17-year-old-artist-sells-138000-worth-of-fake-nfts-and-disappears>)
- [2] Yang Liyi, “ブロックチェーン Ethereum とマーケットプレイス OpenSea における NFT 取引の整合性の調査”, 2022 年度明治大学卒業論文, 2022
- [3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system” (<https://bitcoin.org/bitcoin.pdf>), 2008.
- [4] G. Wood, “Ethereum: A secure, decentralised generalised transaction ledger” (<https://gavwood.com/paper.pdf>)
- [5] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, “A survey on the security of blockchain systems” Future Gener. Comput. Syst. 2017. (<http://dx.doi.org/10.1016/j.future.2017.08.020>.)
- [6] R. Matzutt, M. Henze, J. H. Ziegeldorf, J. Hiller, F. K. Wehrle, “Thwarting Unwanted Blockchain Content Insertion”, 2018 IEEE International Conference on Cloud Engineering (IC2E), pp.364–370,2018.
- [7] T. Sato, M. Imamura, K. Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain,” Proc. WISTP2019, pp.139–154, Dec. 2019.
- [8] 陳 浩太, 江村 恵太, 面 和成 “入札額の上限漏洩を防止した 資金拘束型の封印入札オークション”, コ