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 流通における深層学習を用いた分散型真正性検証プロトコルの提案
A Proposal for a Distributed Authenticity Verification Protocol Using Deep Learning for NFT market

木村 圭吾 * 今村 光良 † 面 和成 *
Keigo KIMURA Mitsuyoshi IMAMURA Kazumasa OMOTE

キーワード NFT, 不正取引, 贋作, 深層学習, 異常検知

あらまし

近年，ブロックチェーンの普及が広まっており，ブロックチェーンのセキュリティリスクを明らかにすることは早急の課題である．ブロックチェーンに対するサイバー攻撃の一例として，ブロックチェーンに対するポイズニング攻撃が挙げられる．ポイズニング攻撃とは，ブロックチェーンに対して悪性データを格納することにより，ブロックチェーンを汚染する攻撃を指し，これは汚染を通じて二次的な攻撃へと発展する危険な攻撃である．

このポイズニング攻撃は目的によっていくつかに分類することができ，その分類の一つとして，ブロックチェーン上で NFT(Non-Fungible Token) を用いて管理される，デジタルアート作品の贋作を流通させるイミテーション攻撃が挙げられる [1]．本攻撃が実現されると，正規のアート作品に似せた贋作を用いた不正取引や，一つのコンテンツを多重に流通させ利益を得ることが可能となる．[1] では，このイミテーション攻撃についてのリスク分析を行なっており，イミテーション攻撃を攻撃者と攻撃環境の違いからフェイク攻撃と二重流通攻撃に分類した．そして，それぞれの攻撃を防ぐために，NFT に紐づくコンテンツの真正性の検証，及び NFT のマーケット上での唯一性の検証が必要であることを結論づけた．

[1] では作品の真正性と唯一性ついて，それぞれの検証フローを提案しているが，ここで提案した検証方法には課題が残る．例えば真正性の検証においては，信頼できる第三者鑑定機関の設置を前提としているが，ブロックチェーンの分散性を考えれば，集権的な機関の設置は望ましくなく，分散型オラクルによる検証が理想である．しかし，分散型の検証を行うには作品の共有が必要であり，検証の中で作品が盗用される危険性が生じる．そこで，作品を盗用から保護しつつ共有する必要がある．

また，どのようにコンテンツの真正性を判断するのかも課題となる．アート作品などにおいて贋作を判定する場合，その判断は専門家の人間が定性的に行うことが多く，真正性の判断を行う上での境界，基準を明確に定義することは困難である．しかし前述の分散型の検証手法を考えるに際には，統一化された判断基準が必要となる．

そこで本研究では，深層学習を用いることで，分散型オラクルにおいてコンテンツを保護しつつ作品を共有しながら，真正性の検証を行えるような分散型真正性検証プロトコルを提案する．具体的には，深層学習の一手法である生成モデルを利用することで，オリジナルコンテンツの潜在分布を学習し，検証対象のコンテンツが統計的に有意水準を満たすか検定することで真正性の判断基準を得る．これにより統一化された判断基準を得ることができるため，分散型オラクルにおける検証が可能となる．さらに，生成モデルをもとに特徴量を引き継いだコンテンツを生成し，それを元に検証を行うことでオリジナルのコンテンツの保護を行いつつ共有を可能とする．本提案手法を用いることで，[1] における真正性の検証における課題を解決し，セキュアな NFT 取引アーキテクチャのより現実的な実装を目指す．

参考文献

[1] 木村圭吾, 今村光良, and 面和成． ”NFT の信頼性にみるセキュリティリスクの考察．” 研究報告コンピュータセキュリティ (CSEC) 2021．28 (2021): 1-8.

* 筑波大学, 〒 305–8577 茨城県つくば市天王台 1–1–1, University of Tsukuba, 1–1–1, Tennoudai, Tsukuba, Ibaragi 305–8577, Japan,
† 野村アセットマネジメント株式会社, 〒 103–0027 東京都中央区日本橋 1–11–1, Nomura Asset Management Ltd. , 1–11–1, Nihonbashi, Chuo-ku, Tokyo 103–8260, Japan,