An Analysis of Zero-knowledge Proof-based Privacy-preserving Techniques for Non-fungible Tokens in the Metaverse

Dorottya Zelenyanszki
School of Information and Communication Technology
Griffith University
dora.zelenyanszki@griffithuni.edu.au

Zhé Hóu
School of Information and Communication Technology
Griffith University
z.hou@griffith.edu.au

Kamanashis Biswas
Faculty of Law and Business
Australian Catholic University
kamanashis.biswas@acu.edu.au

Vallipuram Muthukkumarasamy
School of Information and Communication Technology
Griffith University
v.muthu@griffith.edu.au

***Abstract*—Non-fungible tokens (NFTs) have a huge potential to be included in metaverse-related applications such as digital ownership management and asset trading. However, existing research identified that appropriate privacy-preserving techniques and methods are essential for NFTs for large-scale adoption in the metaverse. This paper conducted an analysis of several existing research works that mainly use zero-knowledge proofs (ZKPs) and/or commitments to protect privacy for blockchain applications. Based on the results of this comparative analysis, we deducted several assumptions. This paper identifies the potential next steps to design new privacy-preserving techniques that will enable privacy-aware metaverse users to leverage the maximal benefits of the NFTs.**

***Index Terms*—blockchain, non-fungible tokens, metaverse, privacy, zero-knowledge proofs**

I. Introduction

Metaverse is a combination of virtual worlds where multiple technologies offer immersive experiences. NFTs are unique tokens that have been introduced on the Ethereum public blockchain [1]. They can represent various types of objects in different domains, including digital art, event tickets or collectables in Web3 games. They also show high potential in metaverse applications as they can represent elements such as avatars and other objects that the users behind these avatars can interact with. In order to provide these interactions, blockchain transactions have to be submitted, and although only the strictly necessary data of these NFTs is stored on-chain [2], the transactions themselves hold valuable information. This introduces a privacy issue because users may want to keep their NFT-related information privacy-protected.

In these transactions, information such as the owner's address is included, which enables other (potentially malicious) users to gain knowledge of the owner's other tokens, which privacy-aware users may not want to share [3]. In areas where the metaverse has high potential, such as real-estate or digital artwork trading, it's likely that the participants wish to stay anonymous because the collected information can lead to de-anonymisation attacks by malicious actors [4]. We refer to this as the lack of transactional privacy [9]. Recent research presented that the combined usage of ZKPs and commitments may provide a solution for this. This paper presents a survey of previous works using these techniques and provides an analysis that can be used later as a foundation to develop more efficient privacy-preserving techniques.

The paper is structured as follows: Section II introduces the underlying key technologies and methods. Following that, Section III describes the existing related research works. Section IV presents a comparative analysis of these solutions and our deducted assumptions. Finally, Section V concludes the paper.

II. Technical background

A. Blockchain

Blockchain is a decentralised, verifiable and immutable ledger that provides complete transparency. Therefore, its historical transaction data, which includes information such as account addresses and balances, can be publicly accessible [5]. This is considered a privacy risk, which makes it non-appealing to certain privacy-aware users and prevents its potential usage in several industrial areas such as supply-chain management, real estate and healthcare.

B. Commitments

Commitment is a cryptographic tool that takes a message and creates a commitment for it through a probabilistic algorithm that hides that message until it is revealed through a deterministic algorithm. It satisfies the binding and hiding properties [6]. It ensures that the commitment can be verified; therefore, it can be used the same way as the message. It can hide information such as blockchain addresses to protect privacy [4].

C. Zero-knowledge proofs

Zero-knowledge proofs are described as a system that has two parties: a prover and a verifier. In this system, the prover proves that he/ she has the knowledge of some private values, which are related to certain public values, that can be verified in a way that these said values are not going to be exposed. It is an interactive verification protocol which means repeated implementation is needed for different use cases. Subsequently, several ZKP models have been introduced. Zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) is a ZKP model where there is a one-time proving and verification key generation process, which removes the need for repeated setups. This setup process is conducted by a trusted third party. Following that, in the proof generation algorithm, the prover is able to generate a proof with the proving keys for a set of private values which also corresponds to the related public values. The verifier then verifies whether the proof is valid by the usage of the public values through the verification algorithm, which uses the generated verification key [4].

Ben Sasson et al. [11] proposed a zk-SNARK for arithmetic circuits that were designed to address the previous models' limitations, such as per-program key generation, lacking support for higher-level languages and non-optimised usage of various types of sub-algorithms (elliptic curves and pairings). They also introduced a new circuit generator that is universal. The zk-SNARK and the circuit generator can be used independently and by combining them. In the latter case, once-and-for-all key generation is provided to verify all types of programs with different sizes.

III. Related works

To provide a foundation for designing new privacy-preserving methods for the NFTs in the metaverse, a literature review of the related research work has been conducted and is presented in this section.

Zerocoin [12] is an e-cash system that uses cryptographic techniques to achieve stronger user anonymity. However, Zerocoin lacks several features for actually offering full-fledged anonymous payments, such as no support for payments with exact values, no functionality to enable users to pay to someone in "zerocoins" and it does not hide the amount and other metadata in transactions. Ben-Sasson et al. [7] offered an enhancement by the introduction of the usage of decentralised anonymous payment schemes (DAP), which leverages zk-SNARKS that is based on the work of Ben-Sasson et al. [11]. It achieves several benefits such as reduced transaction size and verification time, the ability of anonymous transactions of variable amounts, the ability to hide amounts/values of coins and the enablement of payments directly to fixed addresses.

Li et al. [8] described blockchain as a technology that offers a completely distributed way of bookkeeping. It enables parties that do not trust each other to communicate in various types of areas. However, as it was mentioned in Section I, blockchain does not protect transactional privacy, which can expose information such as marketing plans. Although there are existing privacy-preserving methods, Li et al. questioned their level of privacy protection and their ability to not break the verification protocol. They specifically mentioned solutions like Zerocash [7] and their limitations, such as reduced transaction speed and increased storage overhead. To provide an improved solution, they proposed a new method called RZKPB (Ring Zero-knowledge Proof based on the Blockchain) which uses ring zero-knowledge proofs and Pedersen commitments and thereby satisfying the following features: privacy, fairness, no trusted party and efficiency.

Kosba et al. [9] proposed a framework called Hawk to enable users to build privacy-preserving smart contracts. It offers on-chain security by sending cryptographically hidden data to the blockchain and by using ZKPs to ensure the correctness of contract execution and money conservation. It also introduces a minimally trusted manager that handles the execution of the contracts, which, although it gets the user's input, is not able to negatively affect the execution. This is achieved because Hawk provides contractual security, meaning that financial fairness and security against dishonest managers are ensured. For example, if the manager aborts without valid reasoning, it is penalised. The major contributions are as follows: an introduction of formal models for decentralised smart contracts, a presentation of a new cryptography suite that involves the generalisation of Zerocash [7] and finally, implementation and evaluation.

Song et al. [6] proposed ZKDET which is a data exchange scheme that uses NFTs and ZKPs for free on-chain exchanges and traceability. NFTs are applied for providing on-chain credentials for the off-chain data which means that the ownership of that particular data is identified and can be easily tracked. ZKDET also supports dataset transformations such as aggregation, partition, duplication and processing which makes data mining possible and which allows users to sell their computed results. For protection, datasets are encrypted, and their metadata is stored in NFTs, whereas, they integrated a commit-and-prove non-interactive zero-knowledge (CP-NIZK) scheme based on the Plonk construct for verification. In addition, the usage of a circuit-friendly block cipher and commitment primitives were also introduced to reduce the proving/verification overhead.

Xiao et al. [4] deduced that a new protocol is needed for the NFTs that enables privacy-preserving but also makes it possible to publicly verify the transactions that are related to these said digital objects. They considered the usage of previously implemented methods for transaction information obfuscation. However, they stated that these solutions are built on monetary invariants, meaning whether the blockchain nodes will verify if the particular transaction preserves them or not (for example, in the case of Zerocash [7], in a transfer, the user has to destroy and also create some new coins to send a particular amount), and since NFTs are indivisible they do not have these monetary constraints for their transactions. Therefore, these techniques cannot be applied to the stated problem. Instead, they proposed a new protocol called NFTPrivate which enables users to create NFTs for a digital object anonymously and

TABLE I
A COMPARATIVE ANALYSIS OF EXISTING SOLUTIONS

Name	Applications	Characteristics				
		Overhead	**Proof Size**	**Gas Cost**	**Privacy Risk**	**NFT Applicable**
Zerocash [7]	Apply DAPs and zkSNARKs to offer an enhancement for the privacy-preserved payment on the blockchain	●	○	-	-	No
RZKPB [8]	Enhancement of previous solutions like Zerocash [7] with the usage of ring zero-knowledge proofs	●	-	●	-	-
Hawk [9]	Privacy-preserving smart contracts	●	○	-	Yes	-
ZKDET [6]	Off-chain data exchange through NFTs, privacy protected by CP-NIZK	●	●	●	-	Yes
NFTPrivate [4]	Use NFTs to represent digital objects and provide a privacy-preserving method to trade them	●	-	●	-	Yes
Aegis [3]	Privacy-preserving market for NFTs	●	○	●	Yes	Yes

○ denotes low, ● denotes high, – denotes non-deducible

transfer that token to another user. Nodes in the blockchain can also verify whether the user owns the token. Based on previous studies, they apply a cryptographic commitment to represent the owner of the token instead of just simply using a blockchain address. For the transfer, the owner generates a unique serial number from this commitment and then he/she also generates a new commitment from the receiver's address which results in the old commitment's nullification. Besides this, the owner also has to construct a ZKP in order to prove that the NFT is minted in the correct way and that this owner legitimately has ownership over the said token.

Galal et al. [3] deduced that the NFT marketplaces also lack privacy because trade through public auctions and swaps allows adversaries to gain knowledge of bids in advance by observing the mempool. To solve this, a privacy-preserving protocol called Aegis was proposed by them, which allows users to maintain private balances of funds and the automatic swap of NFTs for payment amounts without exploiting sensitive information. Aegis uses zkSNARK proofs to present the correctness of state updates without exploiting unnecessary information. In the case of successful verification, a smart contract accepts the updated state. It also uses Merkle trees for the accumulation of the commitments and serial numbers for the nullification of consumed UTXOs.

IV. ANALYSIS OF THE SURVEY

Cho et al. [10] conducted a summary of the challenges of NFTs based on the transaction history of several well-known collections using the Gallop[1] data service. They looked into how the traits and rarity affect the price of the token. They also discovered that it is more difficult to get the actual price of trading an NFT if the process involves multiple smart contracts, including smart contract executions with zero value. Besides these, they also looked into potentially malicious activity when users trade the same NFT several times to set its price to their liking. Finally, they also presented how volatile NFT collections can behave.

[1]https://www.higallop.com

This shows that transactional information is considered highly important in NFT-related matters, and it has to be in the focus when designing and implementing new privacy-preserving solutions. The information that is shared via emitted events in smart contract executions also has to be part of future research on privacy-preserving since additional, not default transaction data, can be revealed there.

An analysis of the existing solutions (included in section III) is presented in Table I. Besides a short description of their use cases, these privacy-preserving solutions are compared based on five characteristics: computational overhead, zero-knowledge proof size, gas cost, the potential of privacy risk and whether they can be applied for NFTs. The first three evaluation metrics are selected from the existing works, whereas the latter two are related to our major focus, the privacy-preserving of the NFTs. The first three characteristics are represented by circles where the empty circle denotes low and the full circle presents high values. On the other hand, we have used 'Yes/No' to denote the presence/absence of privacy risks and NFT applicability/non-applicability for the last two characteristics. When it was non-deducible, a hyphen was used for the corresponding characteristic. The following paragraph presents the results of this comparison.

With the first characteristic, we measured whether these works successfully avoided having additional computational overhead. We observed that all mechanisms incur a significant overhead because of the various types of operations that were necessary to offer privacy-preserving. For example, ZKDET does not scale well with larger datasets because its setup time grows with the size of the dataset. The NFTPrivate protocol has higher computational and storage overhead, and it was stated to be overall less efficient than ERC-721 (although Xiao et al. mentioned that this is a workable disadvantage compared to the need for privacy-preserving [4]). For Zerocash, storage overhead was already mentioned in Section III and it was generally described as slow which can negatively affect the network.

The second characteristic examined the size of the zero-knowledge proofs produced by the particular privacy-

preserving solution. For this characteristic, there was a higher variance in the results. For example, Aegis uses the Groth protocol which results in a very small proof size. For RZKPB and the NFTPrivate protocol, there were no results regarding this, therefore, they were added as non-deducible. The other solutions included actual proof sizes in their results which show generally smaller-sized proofs. Among those, ZKDET had the largest size, although their aimed security levels (80, 112, 128, 129 bits) have not been the same.

The third characteristic was the gas cost. For which the majority of them presented evidence of an increase. For example, in RZKPB the on-chain time cost is growing if more ring members are added; in ZKDET there is an increased setup time and also larger proof generation time if the data transformation is more complex and in the NFTPrivate protocol there are higher gas costs because of the maintenance of the Merkle tree and as a result of the additional computations related to verifying the zero-knowledge proofs. For some solutions, the evaluation of this property was not evident such as Hawk but generally, it can be stated that higher gas cost is expected for transactions involved in these solutions, simply because the usage of the ZKPs and commitments adds additional computations.

These works have been examined for possible privacy risks as well. Only two of them presented evidence for potential privacy issues: Hawk by the inclusion of the minimally trusted manager (it introduces centralisation which can lead to a single point of failure related problems) and Aegis by adding a lot of responsibility to the included Main smart contract.

Finally, since this research focuses on NFTs, we also evaluated whether these works are NFT-applicable. As a result of the solutions included in the last three rows being designed for NFTs themselves, they were evaluated positively regarding this property. In Section III, we already presented evidence that Zerocash is not a potential solution for privacy-preserving for NFTs. The other two work is currently non-deducible. However, Hawk being an updated version of Zerocash potentially means that it cannot be used for NFT-related purposes.

Based on this survey, the following assumptions were made: In order to introduce a new privacy-preserving solution for the NFTs that achieves better transactional privacy, first, a common metrics system has to be formed. The evaluation of the previous solutions was based on various types of characteristics. Some added a comparison to the ERC-721, others compared their work to previous zk-SNARKs or Zerocash and they also based the experiments on different metrics such as proof size or transaction size. Additional related works have to be examined and analysed to address what are the most important properties that have to be satisfied. If a universal metrics system is created for the NFTs, new privacy-preserving techniques can be evaluated based on it. That makes it easier to conduct a comparison of them for various types of use cases which can be used to provide evidence regarding which cryptographic techniques are suitable for which NFT-related purpose. Besides this, a deeper examination of the NFT-related transactions and their potential emitted events is also necessary because they can reveal additional information on the potential use cases and the current state of the NFTs. This is important because it can show us when is privcay-preserving needed. There may be some transactions or operations where the information is allowed to be exposed.

V. Conclusion

NFTs are unique tokens that can contribute to various types of use cases in the metaverse. However, as a result of the underlying blockchain technology, the interactions that the NFTs are part of, expose information that introduces a privacy risk for certain users. This paper provides a survey on how zero-knowledge proofs and commitments have been used for providing privacy-preserving in this area and presents potential directions that are necessary for designing a new privacy-preserving solution for NFTs which can make the usage of NFTs in the metaverse more appealing for privacy-aware users. In the future, we plan to add additional related works for the analysis and also conduct an examination of the transactions and their events for further enhancement.

References

[1] https://eips.ethereum.org/EIPS/eip-721

[2] Yulong Chen, Ziwei Wang, Xiangyu Liu, and Xuetao Wei. A new NFT model to enhance copyright traceability of the off-chain data. In 2022 International Conference on Culture-Oriented Science and Technology (CoST), pages 157–162, 2022.

[3] Hisham S. Galal and Amr M. Youssef. Aegis: Privacy-preserving market for non-fungible tokens. IEEE Transactions on Network Science and Engineering, 10(1):92–102, 2023.

[4] Yao Xiao, Lei Xu, Can Zhang, Liehuang Zhu, and Yan Zhang. Blockchain empowered privacy-preserving digital objects trading in the metaverse. IEEE MultiMedia, pages 1–11, 2023.

[5] Xiaoqiang Sun, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. A survey on zero-knowledge proof in the blockchain. IEEE Network, 35(4):198–205, 2021.

[6] Rui Song, Shang Gao, Yubo Song, and Bin Xiao. ZKDET: A traceable and privacy-preserving data exchange scheme based on non-fungible tokens and zero-knowledge. In 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), pages 224–234, 2022.

[7] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from Bitcoin. In 2014 IEEE Symposium on Security and Privacy, pages 459–474, 2014.

[8] Bin Li and Yijie Wang. Rzkpb: A privacy-preserving blockchain-based fair transaction method for sharing economy. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 1164–1169, 2018.

[9] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Cryptology ePrint Archive, Paper 2015/675, 2015. https://eprint.iacr.org/2015/675.

[10] Jason B. Cho, Sven Serneels & David S. Matteson (2023) Non-Fungible Token Transactions: Data and Challenges, Data Science in Science, 2:1, DOI: 10.1080/26941899.2022.2151950.

[11] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct Non-Interactive zero knowledge for a Von Neumann architecture, 23rd USENIX Security Symposium (USENIX Security 14), pages 781–796, San Diego, CA, August 2014. USENIX Association.

[12] I. Miers, C. Garman, M. Green and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2013, pp. 397-411, doi: 10.1109/SP.2013.34.