Sleepminting, the brand new frontier of Non Fungible Tokens fraud

Barbara Guidi
Department of Computer Science, University of Pisa
Pisa, Italy
guidi@di.unipi.it

Andrea Michienzi
Department of Computer Science, University of Pisa
Pisa, Italy
andrea.michienzi@unipi.it

ABSTRACT

Non Fungible Tokens (NFTs) are becoming a standard to represent unique and valuable items, such as a piece of art, a videogame item, or other digital or physical goods, and keep track of their provenance. Thanks to blockchain technology and the power of smart contracts, NFT holders have true ownership over them, because they are the only ones who can transfer them. However, through an attack called sleepminting, an attacker is able to impersonate another person, including an artist, and create NFTs on the artist's behalf, while still maintaining its possession, leveraging bugs in the code of the smart contract that manages the NFTs. Therefore, the attacker can cheat concerning the provenance of an NFT and then sell the fake NFTs to unaware buyers. In this paper, we propose a study that sheds light on this phenomenon. In particular, we collect over 1.3 million events that are connected to sleepminting and analyse the events under multiple aspects. The study uncovers that, by using the sleepminting attack, some users are able to create fake NFTs of popular brands, and are able to mint them to famous personalities in the NFT field, such as well known artists and collectors.

CCS CONCEPTS

• **Security and privacy** → Cryptanalysis and other attacks; **Social engineering attacks**.

KEYWORDS

Blockchain, Non fungible token, Smart contract

ACM Reference Format:
Barbara Guidi and Andrea Michienzi. 2022. Sleepminting, the brand new frontier of Non Fungible Tokens fraud. In *Conference on Information Technology for Social Good (GoodIT'22), September 7–9, 2022, Limassol, Cyprus.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3524458.3547239

1 INTRODUCTION

During the last years, several blockchain projects and technologies were proposed for social impact. With the advent of Non-fungible tokens (NFTs), the link between blockchain technology and the social good seems to be stronger than ever, because of their natural application to many important social causes. NFTs are digital assets that cannot be exchanged, altered or split, which are minted on a blockchain so that they can be proven to be unique. They are often utilised as collectables because they cannot be duplicated. Nowadays, NFTs are connected to the concept of the Metaverse [11], and they are used to represent digital art. Despite the excitement around NFTs, and their popularity among artists for their potential to revolutionise intellectual property ownership, they may also be utilised to incentivise and propose good behaviour in our society. The most obvious case is the fundraising for non-profit organisations and charities. Selling NFTs can give non-profits access to new sources of funding outside of established channels and help them diversify their revenue-raising efforts. Another use case is legacy non-profit organisations that can monetise their physical assets without losing access to them, providing a method for digital ownership.

Even if NFTs started to be disruptive in 2021, the first important application based on NFTs that reached a widespread adoption was CryptoKitties [18], which consists of collecting and breeding virtual cats that are modelled as NFTs.

From the technical point of view, an NFT contains two parts: the content represented by the NFT and its metadata [5]. The metadata serves as a description of the content, and contains the unique identifier of the NFT, the current owner, and so on. The content represented by the NFT can either be stored inside the NFT, or a logical link to the content is given, so that NFTs can represent any asset with specific characteristics [14]. When an NFT is created, through the minting process, a token ID is randomly generated which ensures that each NFT is unique. Then, it is stored on the blockchain, and no one can remove it because the blockchain is public. This guarantees not only the uniqueness of the NFT, but also the ownership of this NFT.

From the application point of view, it is clear that NFTs represent an opportunity in several scenarios, but unfortunately, they are affected by issues related to the underlying technologies that can have an impact on the diffusion of this technology. Indeed, NFTs are typically implemented on top of blockchains that support smart contracts [5], such as the Ethereum blockchain, which is also the most used. The smart contract is deployed on a blockchain, and contains the metadata of the NFTs of the collection managed by it, and a set of functions to manage the tokens. The smart contract can contain bugs or can be written with malicious intents, and in this case, it represents a vulnerability of NFTs, which can be exploited by impersonification attacks. An important attack which attracted a lot of attention is the sleepminting attack. Sleepminting is a form of fraud in the NFT scenario, where a hacker can exploit a vulnerability of an existing smart contract or deploy a custom-built NFT contract to mint NFTs in place of other users and claim them at a later stage. Sleepminting may ruin the credibility of NFTs, and can

GoodIT'22, September 7–9, 2022, Limassol, Cyprus
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9284-6/22/09…$15.00
https://doi.org/10.1145/3524458.3547239

severely limit the scenarios of application of this technology. Due to this attacks, the blockchain is not perceived anymore as secure, and people are losing trust in blockchain-powered technologies.

In this paper, we propose a detailed description of the scenarios in which transactions can be attacked through a sleepminting attack, and we also propose an evaluation of the phenomena by collecting and analysing suspicious Ethereum transactions. To the best of our knowledge, this is the first paper where this kind of attack on NFTs is explained and studied. In particular, we identify three moments of an NFT lifecycle where a sleepminting attack can occur. The analyses show that sleepminting attacks occur more frequently during its creation and that specific contracts exists to perform these types of attacks. A more detailed analysis concerning the most recurring addresses involved in this attack, show that famous artists and collectors are usually targets of this attack, and that tokens associated with the attacks are commonly fake tokens.

The paper is structured as following. Section 2 presents the background concerning blockchain and NFTs. Section 3 describes in detail the sleepminting attack. The analyses presented in Section 4 describe the impact of sleepminting, and identify important properties concerning it. Section 5 concludes the paper, pointing out possible future works.

2 BACKGROUND

In this Section, we introduce an overview of the blockchain technology, which is used as the main characteristic of NFTs, and a detailed description of what NFTs are.

2.1 Blockchain

A blockchain is a digital ledger of transactions maintained by a distributed network that facilitates the process of recording information. The growing list of blocks is linked together using cryptography, and this enhances the security of a blockchain. Blockchain technology became famous thanks to Bitcoin [13]. Nowadays, the technology is evolved, principally after the introduction of smart contracts in Ethereum [4], which has simplified the application of the blockchain to not only financial applications [1, 7, 10].

Current literature categorises blockchain networks by using their permission model [12], which determines who can manage them. This classification divides current blockchains into two main categories: permissionless and permissioned. Permissionless blockchains allow anyone to read and write on the blockchain. Instead, permissioned blockchains require authorisation to interact with the blockchain.

Both categories have some drawbacks. Indeed, permissionless blockchains are considered more secure than permissioned blockchains, because there are many nodes that participate in the validation of transactions. However, they usually have long transaction processing times due to the large number of nodes and the large size of the transactions.

A key aspect of blockchain technology is the consensus algorithm used to determine who will be the producer of a new block. Several consensus algorithms have been proposed [17]. The most famous is the Proof of Work consensus model (PoW) [9] used both in Bitcoin and Ethereum. Another used algorithm is the Proof of Stake consensus model (PoS) [16], based on the amount of cryptocurrency a user has invested into the system.

2.2 Non Fungible Tokens

A non-Fungible Token (NFT) [20] is a digital asset that uniquely represents real-world objects. NFTs are generally built using the same kind of programming as cryptocurrencies, but they are different from bitcoin and ether.

Indeed, physical money and cryptocurrencies are called fungible tokens, which means that they can be traded or exchanged for one another (one bitcoin is always equal to another bitcoin). Instead, each NFT is unique and irreplaceable, and for this reason, it is called non-fungible. Each NFT has a digital signature that makes it impossible for NFTs to be exchanged for or equal to one another [15]. Thanks to their unique properties, NFTs can be used in several scenarios, such as virtual gaming, cultural heritage, digital identity, etc.

The history of NFTs began in 2013 with the so-called "coloured coin" [19], initially distributed on the Bitcoin network. NFTs are typically held on blockchains allowing smart contracts. Indeed, the Ethereum blockchain is currently the most used. From the technical point of view, an NFT contains two parts: the content represented by the NFT and its metadata [5]. The metadata serves as a description of the content, and contains the unique identifier of the NFT, the current owner, a logical link to the content or the content itself, and so on NFT can represent any asset with specific characteristics [14]. When an NFT is created, through the minting process, a token ID is randomly generated which ensures that each NFT is unique. Then, it is stored on the blockchain, and no one can remove it because the blockchain is public. This guarantees not only the uniqueness of the NFT, but also the ownership of this NFT.

Several NFT standards were proposed, but the most recurring ones are the Ethereum standards: the EIP-721 defines a standard, called ERC-721 [6], containing an interface that must be implemented by a smart contract to give the mint and trade actions; the ERC-1155, called the Multi Token Standard, which offers the possibility to define "semi-fungible" tokens; finally the ERC-998, which is the standard which provides composable tokens.

3 NFT SLEEPMINTING

NFTs are usually implemented through the usage of smart contracts, that record their metadata and keep track of their ownership through time. While using blockchain and smart contracts minimises the risks connected to having a single central managing authority, it is far from being completely secure. Indeed, there are already multiple known ways to exploit smart contracts [2, 3], in particular through bugs in their source code [8]. As concerns the NFT scenario, a recent issue is the so-called *Sleepminting*. Sleepminting is a form of fraud in the NFT scenario, where a hacker can exploit a vulnerability of an existing smart contract or deploy a custom-built NFT contract to mint NFTs in place of other users and claim them at a later stage.

One of the key aspects for collectors of digital and physical items is *provenance*, which consists of having a certain type of proof concerning the past ownership of the item. In the case of NFTs, since they are implemented on a blockchain, provenance is usually taken for granted, as it is usually unfeasible to make a successful attack on an existing blockchain. However, since NFTs are managed by smart contracts, by publishing the smart contract with quirky or faulty implementations, it is possible to manipulate the NFT provenance. This kind of attack is highly harmful to the future of NFTs as it can be a strong motivation against their widespread use.

More in detail, an attacker (scammer), can ask an NFT contract to mint a new NFT and assign it to the address of a famous artist. Once the mint is recorded in the blockchain, the attacker can force the contract to transfer the NFT so that the attacker can claim to own a real NFT for the targeted famous creator, and can even sell it to an unaware person for a high price. While provenance can be "guaranteed" by the blockchain, the faulty smart contract fakes it at an artist's and collector's loss.

In late March 2021, a person that goes under the pseudonym of *Monsieur Personne*, decided to expose the weaknesses of current blockchain-based NFT implementations through sleepminting. The primary aim of this person was to highlight a possible exploit that can be done on NFTs[1]. To support his claims, he developed a smart contract to manage an ERC721 token, called `NFTheft`[2], and, shortly after, he minted an NFT, assigning its ownership to *beeple*, a well-known artist, and attaching one of beeple's pieces of art as metadata.

The online NFT community was shocked by this fact, because another NFT by beeple, linked to the same picture, was sold for over 69 million dollars. While on one hand the NFT was not minted by the artist, the information returned by the smart contract pinpointed beeple as the rightful owner of the NFT. Since most of the platforms that manage NFTs are also based on the information returned by the smart contracts, also auction houses like OpenSea and Rarible showed that beeple was the minter and sole owner of the NFT.

However, after the minting, Monsieur Personne was able to issue another transaction that ultimately led to the NFT being transferred from beeple to another address, presumably controlled by Monsieur Personne, without beeple taking any action. After this first impersonation attack, other NFTs were minted to beeple's address by other contracts ascribable to Monsieur Personne.

3.1 Sleepminting: technical details

The difficulty to identify a solution to this attack is that there are multiple technical implementations of it, but all rely on bugs in the code of the smart contract or, in other words, behaviours that are allowed but really should not. On top of that, detection of sleepminting attacks can be extremely challenging. As shown in Figure 1 a user A can interact with a normal NFT contract and with a faulty one analogously. This means that a user can not understand in advance the nature of a contract, just by its interface.

Sleepminting may involve multiple aspects of a contract, however, the three sets of functions that are usually targeted by this attack are the ones related to minting (creating) an NFT, transferring it (changing ownership), or approving addresses (enabling non-owner addresses to manage an NFT). In particular, faulty smart contracts may decide to omit important checks regarding the address that calls the contract and the owner of an NFT, and therefore allow tokens to be transferred by addresses that do not own the NFT. An example of a faulty contract is shown in Figure 2, which manages the contract calls in a very superficial way, without making any checks. On the other hand, Figure 3 shows how a normal contract should behave to prevent faulty behaviour. A mint transaction should be accepted only when the address issuing the transaction is the same address to which the token should be assigned when minted. For transfer and approval operations, the contract should check whether the address issuing the transaction is either the owner of the NFT or an approved address for the NFT for which the operation is requested. Adding these checks would prevent operating on NFTs that are not owned by a potential attacker and would preserve true ownership and provenance.

An example of a sleepminting attack is presented in Figure 4. Initially, the attacker A requests an NFT mint to the contract, and the NFT (with unique number 42) is minted to another user D. When querying the NFT contract, the NFT is rightfully owned by D. However, at a later stage, the attacker A is able to send another transaction to the NFT contract, requesting that the token is transferred to another address, for instance, the attacker's address. Most importantly, we can see that, due to the faulty behaviour of the NFT contract, the attacker A is able to perform the attack single-handedly, without the help of third parties.

From the perspective of the NFT ownership and its provenance, it is indistinguishable whether the NFT was rightfully sold by the owner D to another user or whether an attacker performed an attack and transferred it without the owner knowing. The only trace left by this attack is the fact that transactions are stored in the blockchain and therefore it is possible to check whether the contract is faulty, as in Figure 2, or not, as in Figure 3. However, currently, it is not possible to prevent this attack. Additionally, while one can think that this problem is related only to a specific NFT smart contract standard, like the ERC-721 standard, all NFTs can be affected by this problem as the problem is connected to the way a smart contract code is written, rather than the interface exposed to interact with the assets it represents.

In this paper, we describe and analyse the sleepminting attacks concerning the ERC-721 standard, which is the standard interface which defines a set of API methods that a token contract needs to implement. We focus our attention on this standard because it is the standard which is currently more affected by this attack due to the sheer amount of dApp implemented by using the Ethereum blockchain.

4 EVALUATION OF THE SLEEP MINTING PHENOMENON

The sleepminting attack is an important issue concerning the NFT world, and there is a need to understand the current sleepminting attacks in order to provide, in the future, a way to avoid this attack. It is an important attack which can affect the evolution of the NFTs, and to provide a solution, it is important to understand the characteristics of current attacks. For this reason, we collect information about the sleepminting attacks by using the Forta protocol[3],

[1] https://news.artnet.com/opinion/sleepminting-nftheft-monsieur-personne-1960744

[2] https://etherscan.io/address/0x5FBbACf00ef20193a301a5BA20acf04765fb6DaC

[3] https://docs.forta.network/en/latest/

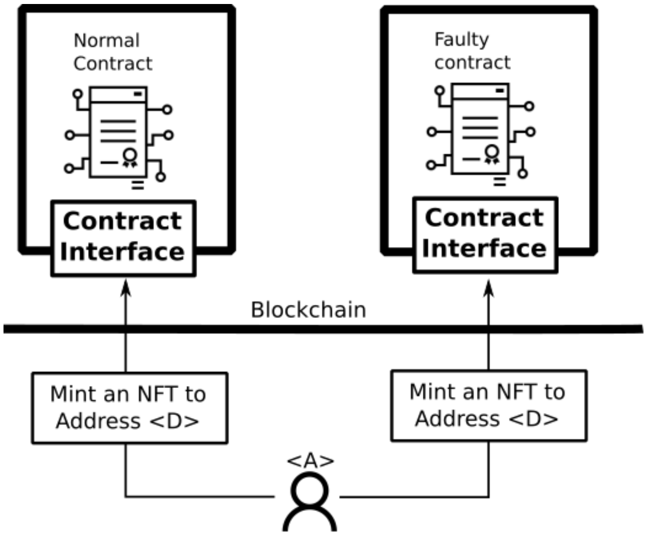


Figure 1: An Ethereum user A interacts with two NFT contracts in a very similar way.

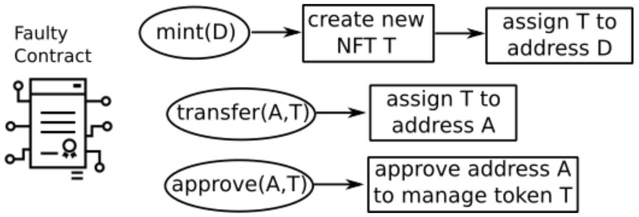


Figure 2: The faulty contract implementation omits important security checks, letting the attacker A perform illegal actions.

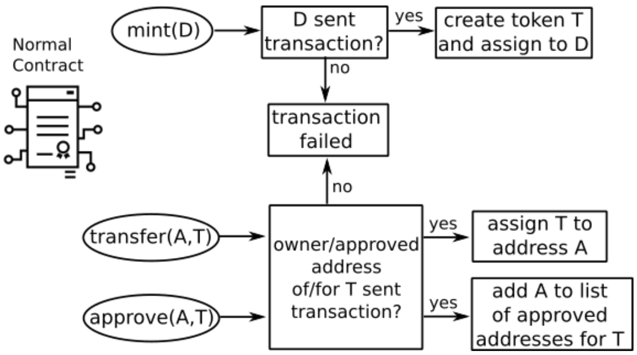
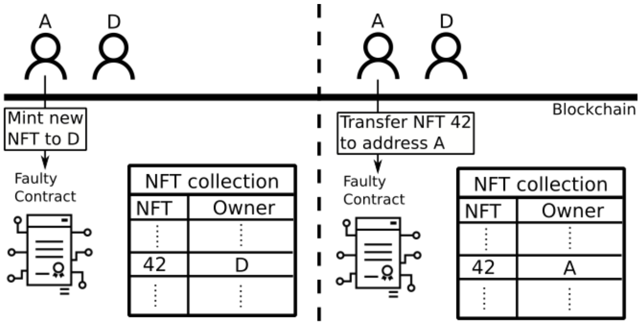


Figure 3: How a normal NFT contract is supposed to be handling requests.



NFT collection

NFT	Owner
⋮	⋮
42	D
⋮	⋮

NFT collection

NFT	Owner
⋮	⋮
42	A
⋮	⋮

Figure 4: An example of a sleepminting attack.

and in particular, a Forta agent[4]. We analyse the behaviour of user addresses and contracts involved in this activity. The motivation behind using the Forta agent lies in the fact that it is a tool publicly available that is already able to detect suspicious activity, and offers API to retrieve its data and alerts produced.

4.1 Dataset

We collected the malicious activities identified by the Forta agent about the sleepminting attack, detected on the Ethereum blockchain. The dataset considered in this study covers a two months time frame, from the 1st of March 2022 to the 30th of April 2022, and consists of 1,339,593 alerts. Since the Forta agent was deployed on the 1st of March 2022, we were not able, at this stage, to easily gather data before that date.

The Forta agent is able to highlight suspicious activity concerning the Ethereum blockchain, and in particular sleepminting attacks. It identifies 3 categories of alerts:

(1) **sleepmints**, have alertId=`"SLEEPMINT-3"`. These alerts are the most common and indicate a minting of an NFT that may have been sleepminted.
(2) **approvals**, have alertId=`"SLEEPMINT-2"` These alerts are used to signal when an address is approved to transfer one or more NFTs owned by another address. In these cases, the address requesting the approval is not the owner or an approved address of the NFT.
(3) **transfers**, have alertId=`"SLEEPMINT-1"`. These alerts are used to signal when an NFT is transferred by an address that is not the owner of the NFT or an approved address.

In Listing 1, we show an example of the data contained in a Forta alert. The fields which are worth to be mentioned are:

[4] https://explorer.forta.network/agent/0x20d0cd9432c7e15cb625097a718c15cc07f463b5252e3c36ae23acb7ef98d54e

- **createdAt**, which shows the time and date at which the alert was created;
- **protocol**, which shows the blockchain for which the alert was emitted;
- **transactionHash**, which identifies the hash of the transaction to which this alert is referring;
- **severity**, which indicates the impact of the alert risen. It can assume one of 5 values[5], but in the case of the sleepminting agent, it is either set to "INFO" or "MEDIUM";
- **alertId**, used to indicate a group of similar alerts;
- **description**, a textual description of the event reported in the alert;
- **hash**, a unique identifier for this alert, not to be confused with "transactionHash".

Listing 1: An example of the agent's alerts

```
{
  "createdAt":"2022-03-06T20:34:01.295653315
      Z",
  "name":"Sleep Minted an NFT",
  "protocol":"ethereum",
  "findingType":"SUSPICIOUS",
  "source":{
    "transactionHash":"0x8def1cc4d37b75c1ffa
        43a832f6038937134af8e5ecdfa5dd99a788
        a69614e37",
    "block":{
      "number":14335470,
      "chainId":1
    }
  },
  "severity":"INFO",
  "metadata":"None",
  "scanNodeCount":1,
  "alertId":"SLEEPMINT-1",
  "description":"An NFT Transfer was
      initiated by 0x90834b7997f857b1a4ba066
      45fb81e598a4dfef9 to transfer an NFT
      owned by 0xe479dfd9664c693b2e299230093
      0b00bfde08233. The NFT contract
      address is 0x959e104e1a4db6317fa58f829
      5f586e1a978c297",
  "hash":"0xe429afcfffab9ca40a129efd82374737
      2408243cb46f5fc3cde50846a2561e39"
}
```

The peculiarity of each category we defined is that their description follows a similar schema:

(1) **sleepmints**: An NFT was sleep minted by A_a to A_d. The NFT contract address is A_c
(2) **approvals**: An NFT was approved for A_a, by A_a, but owned by A_d. The NFT contract address is A_c
(3) **transfers**: An NFT Transfer was initiated by A_a to transfer an NFT owned by A_d. The NFT contract address is A_c

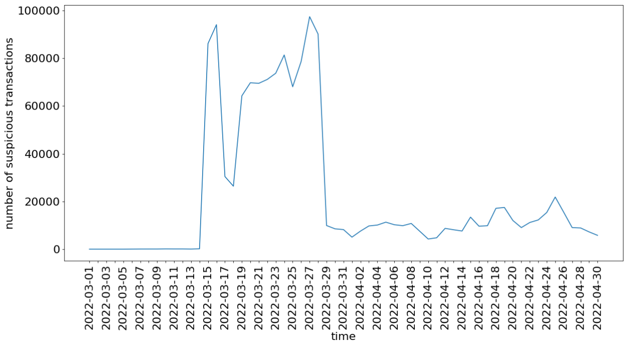


Figure 5: Number of alerts raised by the FORTA agent

where each A is a placeholder that represents Ethereum addresses of users and contracts. After checking the consistency between the alerts emitted by the Forta agent and the data stored in the blockchain, we decided to extract the suspicious activity using the description contained in each alert. In particular, for each alert, we identify three roles:

- the *attacker* (A_a), that is the address of user who initiated the suspicious activity,
- the *defender* (A_d), that is the address of the user who suffered the malicious activity,
- the *contract* (A_c), that is the address of the contract that manages the NFT collection on which the attack was performed.

4.2 Analyses

We start our analysis by investigating the number of alerts emitted by the Forta agent during the considered time frame in order to understand the frequency of this issue. Figure 5 shows the number of alerts between the 1st of March 2022 and the 30th of April 2022. The plot shows that the number of alerts during the first 14 days was very low, and then raised steeply, exceeding 80,000 alerts on multiple days. The motivation behind the fact that within the first 14 days we have very few alerts, lies in the fact that initially, the agent did not consider the sleepminting events (the ones that have alertId="SLEEPMINT-3"). The code of the agent was updated on the 15th of March, enabling it to detect much more suspicious activity. Although the agent was developed to inspect all activity on the Ethereum blockchain, there is an impressive amount of suspicious activity which involves more than 1 million NFT mints.

sleepmint	approvals	transfers
1,334,091	48	5,345

Table 1: Number of the alerts divided in the 3 categories of attacks

As reported in Table 1, sleepmint alerts are the vast majority of alerts raised by the Forta agent, which is a clear sign of the magnitude of this attack on the Ethereum blockchain, and how is hard to prevent this attack.

[5] https://docs.forta.network/en/latest/python/#finding

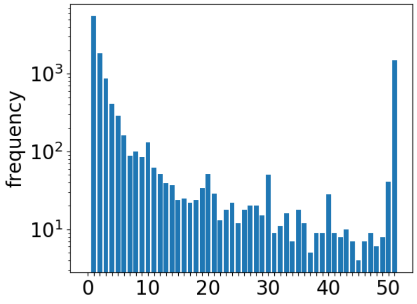


Figure 6: Number of times addresses are reported as attackers.

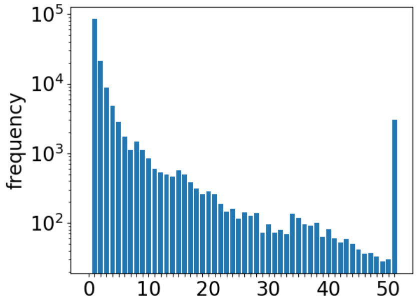


Figure 7: Number of times addressed are reported as defenders.

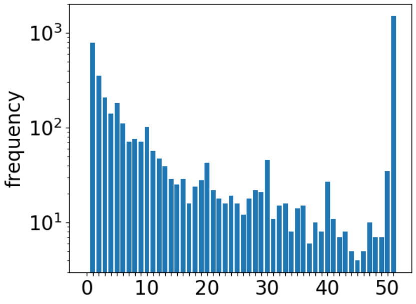


Figure 8: Number of times contracts are reported in an attack.

Figures 6 and 7 report the distribution of the number of times addresses are reported as attackers and defenders respectively. For readability reasons, we grouped all the addresses that appear more than 50 times in the respective role in a single bar. The Figures show that in both cases most of the addresses appear in the respective role just a few times. However, due to the different scales on the y-axis, we can notice that there are far fewer attackers that attacked just one time, with respect to the number of defenders that were attacked one time. This translates in having some attackers that performed a tremendous number of attacks. Among the addresses that appear most frequently as attackers, we find minters of fake and spam coins, and in few cases, some legit video games. Among the most targeted defenders, we find mostly NFT collectors and NFT artists, that confirms the main reason behind sleepminting, that is impersonification attacks.

Figure 8 shows the distribution of the number of times an NFT collection was involved in an attack. Similarly to what we observed in Figures 6 and 7, also in this case most collections were targeted only a few times, but the most targeted collection was targeted almost 30,000 times. Among the most frequent collections on which sleepminting happens, we find three contracts whose name refers to a very popular fashion firm (Louis Vuitton), a contract whose name is "Steam", one of the largest videogame distribution platform, and a contract whose name is "Apple", the well known tech company. Despite their names, which can be simply set by the contract deployer, these are all fake tokens, created only to trick people into believing that the tokens are official. We also find numerous tokens that have been tagged as spam tokens by the community or tokens with names that suggest their connection to other important projects or people, such as the pricey Cryptopunks NFTs or the famous NFT creator Azuki. Lastly, some addresses refer to trading card games, such as Syltare.

Figures 9, 10, and 11 show respectively the distribution of the number of attacker-defender, attacker-contract, and defender-contract pairs that was detected in the raised alerts. While in all three plots each pair appears up to 10 times, the distribution shown in Figure 10 has some peculiarities. The plot has a smaller scale, indeed there are only a few thousand of occurrences of attackers attacking the same collections, while the corresponding values on the other two plots are two orders of magnitude higher. On the other hand, some attackers operate on the same contract more than $10,000$ times, which indicates some sort of dedication or the existence of attack patterns by specific addresses. It is worthy to notice that this kind of scenario can happen also when NFT are created by a dApp, and this analysis shows that it is hard to identify an attack only by considering the nature of a contract, which can be faulty or not (e.g. dApp concerning the metaverse).

Figure 12 shows the bivariate distribution of the number of the attacker and defender addresses for each NFT collection. The Figure shows that usually NFT collections have very few attackers (1 or 2) but can have up to 10,000 defender addresses. There are also some cases in which the number of attackers and the number of defenders are roughly matched, and some other NFT contracts in which there are multiple attackers, up to few thousand, but only a single defender.

5 CONCLUSIONS

NFTs are digital tokens that we can use to represent unique items and to keep track of the ownership of these thanks to blockchain technology and smart contract. Nowadays, NFTs are tightly connected to the concept of Metaverse, and they are most commonly used to represent digital art. Despite being backed by the blockchain, they are not entirely safe from attackers that may try to cheat concerning the provenance of an NFT, and scam other users by selling fake NFTs through impersonation attacks. One such attack, called *sleepminting*, consists of leveraging some bugs in the code of an NFT contract to perform some transactions that should not, in principle, be allowed. In this paper, we identified three types of sleepminting attacks, which can occur at different stages of the life of an NFT: during minting, approving another address, or when transferring the NFT. Thanks to an agent deployed on the Forta protocol, we were able to detect over 1 million alerts in a time span of 2 months (March-April 2022). For each alert raised we were able to identify 3 roles: the attacker, the address starting the attack, the defender, the address suffering the attack, and the contract, the address of the contract that manages the NFT collection. Analyses show that minting is one of the most popular stages at which the attack takes place and that each attacker tends to favour sleepmiting on the same contracts. Among the most recurring defenders, we find numerous NFT collectors, while the most targeted contracts

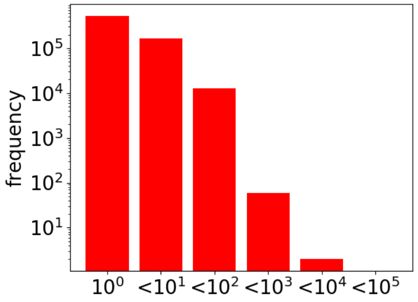


Figure 9: Distribution of the number of times a pair attacker-defender was reported.

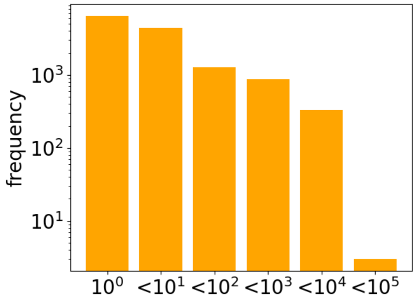


Figure 10: Distribution of the number of times a pair attacker-collection was reported.

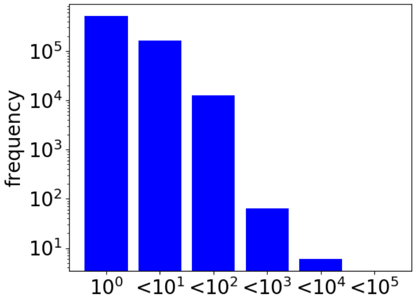


Figure 11: Distribution of the number of times a pair defender-collection was reported.

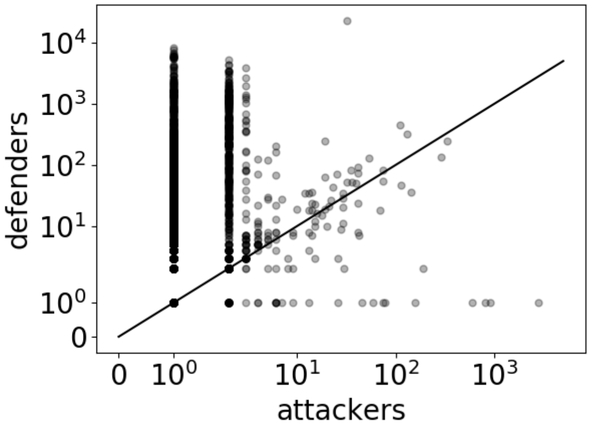


Figure 12: Bivariate distribution of the number of addresses that appear as attackers and defenders for each NFT collection.

are the ones related to important NFT projects or companies known worldwide, like Apple or Louis Vuitton.

This study represents only the first step towards understanding and fighting the phenomenon of sleepminting and paves the way for multiple future works. To begin with, while sleepminting can be seen as a malicious activity, in some cases it is actually the expected behaviour. For instance, in some games where NFTs represent important resources, only the game manager should be able to create NFTs, otherwise, users could create new NFTs at will without any control. This fact should be taken into account to improve a sleepminting detection technique. Moreover, sleepminting can assume convoluted forms that include multiple transactions in order to trick users concerning the provenance of an NFT, therefore, we plan to study NFT trading strategies by applying graph analysis techniques. Lastly, NFT sleepmitning does not have a clear solution, therefore we plan to investigate strategies to prevent such attacks, for instance by rejecting suspicious transactions or by supplying better NFT contract standards that are resistant by design.

REFERENCES

[1] Joe Abou Jaoude and Raafat George Saade. 2019. Blockchain applications–usage in different domains. *IEEE Access* 7 (2019), 45360–45381.

[2] Alessandro Brighente, Mauro Conti, and Sathish Kumar. 2022. Extorsionware: Exploiting Smart Contract Vulnerabilities for Fun and Profit. (2022).

[3] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. *arXiv preprint arXiv:1904.05234* (2019).

[4] Chris Dannen. 2017. *Introducing Ethereum and solidity.* Vol. 1.

[5] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. 2021. Understanding Security Issues in the NFT Ecosystem. *arXiv preprint arXiv:2111.08893* (2021).

[6] Monika Di Angelo and Gernot Salzer. 2020. Tokens, types, and standards: identification and utilization in Ethereum. In *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS).* 1–10.

[7] Dimiter V Dimitrov. 2019. Blockchain applications for healthcare data management. *Healthcare informatics research* 25, 1 (2019), 51–56.

[8] Wesley Dingman, Aviel Cohen, Nick Ferrara, Adam Lynch, Patrick Jasinski, Paul E Black, and Lin Deng. 2019. Classification of smart contract bugs using the nist bugs framework. In *2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA).* 116–123.

[9] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security.* 3–16.

[10] Barbara Guidi. 2020. When Blockchain meets Online Social Networks. *Pervasive and Mobile Computing* 62 (2020), 101131.

[11] Barbara Guidi and Andrea Michienzi. (in press) 2022. Social games and Blockchain: exploring the Metaverse of Decentraland. In *42nd IEEE International Conference on Distributed Computing Systems.*

[12] Christine V. Helliar, Louise Crawford, Laura Rocca, Claudio Teodori, and Monica Veneziani. 2020. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management* 54 (2020), 102136.

[13] Satoshi Nakamoto and A Bitcoin. 2008. A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4 (2008).

[14] A Popescu. 2021. Non-Fungible Tokens (NFT)-Innovation Beyond the Craze. In *5th International Conference on Innovation in Business, Economics and Marketing Research.*

[15] Ferdinand Regner, Nils Urbach, and André Schweizer. 2019. NFTs in practice–non-fungible tokens as core component of a blockchain-based event ticketing application. (2019).

[16] Fahad Saleh. 2021. Blockchain without waste: Proof-of-stake. *The Review of financial studies* 34, 3 (2021), 1156–1190.

[17] Mehrdad Salimitari and Mainak Chatterjee. 2018. A Survey on Consensus Protocols in Blockchain for IoT Networks. (2018).

[18] Alesja Serada, Tanja Sihvonen, and J Tuomas Harviainen. 2021. CryptoKitties and the new ludic economy: how blockchain introduces value, ownership, and scarcity in digital gaming. *Games and Culture* 16, 4 (2021), 457–480.

[19] Andrew Steinwold. 2019. The History of Non-Fungible Tokens (NFTs). (2019).

[20] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. 2021. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447* (2021).