5-2023

Need To Know Before Utopian Balloon Is Popped: Security Perspective Analysis of Nun-Fungible Tokens

Kenneth Amoah

Need To Know Before Utopian Balloon Is Popped: Security Perspective Analysis of Nun-Fungible Tokens

by

Kenneth Amoah Junior

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

May, 2023

Starred Paper Committee:
Lynn Collen, Chairperson
Jieyu Wang
Hazem Farra

Abstract

Non-Fungible Tokens (NFTs) have exploded into the technological and blockchain worlds with millions of dollars' worth of cryptocurrencies such as Ethereum and Bitcoin among others, being traded for with these NFTs by individuals. NFTs are utilized by most buyers and sellers to show authenticity and sole ownership of a rare piece of work which could be in the form of an art, a video, a game, an image, a collectible, or anything the individual deems to be of great value and of interest for other individuals to pay for and own. NFTs however are not immune to the security and privacy issues that are already affiliated with the blockchain. This research work therefore examines the existing vulnerabilities in the blockchain then specifically investigates vulnerabilities with NFTs. Not much of research effort has been put into this area but the ones that have been conducted centered on generic security issues related to Non-Fungible Tokens. Taxonomies are developed in this paper to classify the security threats and attacks as identified by investigating the vulnerabilities of NFTs. This work will be of great assistance to investors and developers who look to enter into the NFT market, as they will be provided with some adequate knowledge for them to be aware of the security issues related to the booming market of NFTs.

Keywords: Non-Fungible Token, Blockchain, Security and Privacy Issues, Threats, Vulnerabilities, Ethereum, Bitcoin, Cryptocurrencies

Table of Contents

Chapter Page

List of Tables

Table Page

List of Figures

Chapter I: Introduction

Introduction

Imagine auctioning a tweet you once made as a Non-Fungible Token (NFT) and getting the highest bid for that tweet around $2.9 million. YES! This actually happened when Jack Dorsey, the CEO of Twitter, sold his first tweet at an auction (NFT's and Their Legal Implications, 2021). Mike Winkelmann, a digital artist who goes by name Beeple, also made a sale of an NFT of his work at an auction raking up a whopping $69,000,000. Until October 2020, it was revealed that the most he had ever sold a single print for was $100 before he started selling his first series of NFTs in October (Kastrenakes, 2021). This mind-blowing sale made Beeple the third most valuable living artist (Kinsella, 2021).

This poses the question: what at all is an NFT? An NFT simply is a reference to a blockchain right of ownership to a digital asset such as videos, images, art among others (Dowling, 2021). When we say something is fungible it means that thing can be exchanged like for like (Ante, 2021). This is to say ten dollars could be exchanged for two 5-dollar bills. NFTs on the other hand are unique and cannot be exchanged for another NFT. One cannot exchange digital artwork which has been turned into an NFT for, say, a rare video of a kangaroo making a slam dunk which is turned into an NFT. Both NFTs in this instance are valued different based on the worth that people will place on it in an auction. NFTs therefore have brought about a modernized way of making the works of digital artists much lucrative as people now want to claim sole ownership of a piece of fine art. According to Ante (2021), "like cryptocurrency and other types of

tokens, NFTs rely on blockchain technology and smart contracts as their digital infrastructure".

Problem Statement

When the coronavirus pandemic hit, many jobs were closed, and countless people lost their jobs. Other businesses resorted to working remotely from home. Even though in this period the stock and cryptocurrency markets took a nose-dive for some time, there was a resurgence as 13% of Americans bought or traded cryptocurrency and 24% of Americans invested in stocks over the past 24 months (Iacurci, 2021; More Than One in Ten Americans Surveyed Invest in Cryptocurrencies | NORC.Org, 2021).

To many people, NFTs are the new type of digital assets on the blockchain which are raking in huge some of profits as individuals tend to flip – buy and later sell at a profit – these NFTs at outrageous amounts of profits. The problem however is: How secure is it to trade in NFTs from the angles of the buyers and sellers (the authenticity of both parties), the platform that these trade deals happen on, and the blockchain-encrypted web addresses (Bonderud, 2021)? People all over the world are paying millions of dollars in cryptocurrency for NFT art and collectibles (NFT Scams Part 1, 2021).

NFTs, because they are located on blockchains, are not immune to known blockchain privacy and security attacks out there, which are made daily on other digital assets such as cryptocurrencies. As mentioned earlier about the two parties involved in the transactions of NFTs – buyers and sellers – it is also important to take note of the authenticity and safe communication between these two parties during their

transactions as huge sums of money are involved in these trades. The field of NFTs is an emerging field that has gained so much momentum in a short period of time and because of this, new dimensions of risks and attacks are likely to surface with this new way of trading digital assets.

To the best of my knowledge, at the time of authoring this paper no educational paper has been written specifically analyzing the security perspective of dealing in NFTs with regards to the traders (Buyers and Sellers), the platforms that bring these parties together and the security of the blockchain-encrypted web addresses.

Nature and Significance of the Problem

The 24-hour trading volume on average of the NFT market currently hovers around $4, 592,146, 914. Whereas the entire cryptocurrency market is approximately $341,017,001,809 (Wang et al., 2021). The daily number of NFT sales is about 12,320 which at one point on September 27, 2021, recorded a peak daily number of sales at 33,939. The total amount spent on completed daily sales of NFTs is $50,880,630.94 (Market History | NFT Sales and Trends, 2021). This shows how many millions of dollars people put into NFTs every day. However, with this “lucrative investment” comes with the volatility of the market and a “red-hot” target for hackers. Over the weekend of March 15th, 2021, an NFT trading platform: Nifty Gateway, was hacked with several accounts of their users compromised. One person tweeted of their account being hacked and $10k worth of NFTs stolen. Another person also tweeted about their account hacked and the credit card attached to his account was used to purchase $20k worth of art (Peters, 2021). In addition to digital art and other NFT collectibles being

targeted and stolen, so is Personally Identifiable Information (PII) since credit cards of individuals are easily retrieved. At one point, a hacker was selling a zero-day vulnerability as an NFT which was later blocked by the trading platform: OpenSea (Powers, 2021). What would happen if these marketplaces were not aware of these kinds of NFTs traded on their platforms? Or when hackers use steganography to hide such cybersecurity exploits? These security and privacy issues among others made this a hot area for investigators who are concerned about a secure electronic space.

Objective of the Study

The objective of this study is in fourfold to provide a solution to the problem stated by:

- Studying and surveying this new area of Non-Fungible Token trading
- Identifying the security and privacy issues related to trading in NFTs, the known issues of blockchains in general and the emerging issues specific to NFTs and classifying them in a taxonomy.
- Identifying the gaps in the field with respect to what has been done and what needs to be done to educate anyone looking to trade in NFTs
- Recommending solutions to the identified security and privacy issues

Study Questions

1. What have other researchers done in this area?
2. What are the existing and known vulnerabilities in blockchains?

3. What are the new and emerging vulnerabilities that could be exploited as attacks on NFTs?
4. What are the security and privacy issues related to NFT trading?
5. How can an individual protect themselves from these security and privacy issues?

Definition of Terms

- *Non-Fungible Token (NFT):* “A non-fungible token (NFT) is a cryptographically unique, non-replicable token” (Bal & Ner, 2019).
- *Blockchain:* “A blockchain is defined as a distributed and attached-only database that maintains a list of data records linked and protected using cryptographic protocols” (Wang et al., 2021).
- *Smart contracts:* Smart contracts are programmable contractual clauses that automate and define rules for inter-party transactions without trusted intermediaries (Bal & Ner, 2019).
- *Cryptocurrency:* A cryptocurrency is a virtual coinage system that functions much like a standard currency, enabling users to provide virtual payment for goods and services free of a central trusted authority (Farell, 2015)
- *Vulnerability:* A weakness in a system, application, or network that is subject to exploitation or misuse (Cichonski et al., 2012).
- *Peer-to-Peer:* A P2P network is a group of computers on the internet that have agreed to share files with one another (*Peer-2-Peer Networking*, 2018).

- *Threat:* potential cause of an unwanted incident, which may result in harm to a system or organization (Garfinkel, 2015).
- *Auction:* an auction is a process of sale - either public or private depending on the restrictions regarding the auction, which brings together buyers and sellers, with buyers occupying the positions as bidders and the specific object up for sale, sold to the highest bidder.
- *Buyers:* these are individuals or groups who raise bids in hope of buying the NFT which has been placed for sale. The final sale transaction is paid for using cryptocurrencies such as Ethereum, Bitcoin and others.
- *Sellers:* these are individuals or groups who have the legitimate and sole ownership to the NFT and place it for sale on the auction platform to be sold to the highest bidder, for ownership to be transferred.
- *Steganography:* steganography is a technique which takes advantage of the content redundancy in digital media to conceal secret information, to achieve covert communication through the common channel (Liao et al., 2020).
- *Personally Identifiable Information (PII):* is typically used to indicate information that contains identifiers specific to individuals (Garfinkel, 2015).
- *Cyber-attack:* Cyber-attacks are actions that attempt to bypass security mechanisms of computer systems (Raiyn, 2014).

- *Exploit:* An exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability within an authorized service (Liu & Cheng, 2009).
- *Zero-Day Vulnerability:* **"**A zero-day attack is a cyber-attack exploiting a vulnerability that has not been disclosed publicly" (Bilge & Dumitras, 2012).
- *Blockchain-encrypted web address:* this is a web address hosted by a remote server and serves as a pointer to the NFTs on the blockchain. In effect, this is what is traded for when one buys an NFT.
- *Fungible:* anything fungible can be interchanged like for like. For instance, US$ 10 interchanged for 2 notes of US$5. Here these notes are of the same property and therefore are fungible.
- *Minting:* is how your digital art becomes a part of the Ethereum blockchain–a public ledger that is unchangeable and tamper-proof (Ayson, 2021)
- *Burning:* Burning your NFT simply means destroying it and removes it entirely from the Ethereum blockchain (AlexWGomezz, 2021).
- *Cryptographically unique:* this means that the pattern for securely obscuring the content of an object is specific to that object and cannot be duplicated
- *Digital asset:* refers to any content that is in a digital form and has the right to use. E.g., images, videos, and audio files
- *Collectable:* anything considered as valuable and worthy of use or ownership to a collector.

- *Node:* A node, in the world of digital currency, is a computer that connects to a cryptocurrency network (“Node (Cryptocurrency Network) - Definition and Examples,” 2021).
- *Authentication:* to authenticate is to verify the identity of an entity to determine whether they are who or what they say they are.
- *Non-repudiation:* this presents an instance where a sender cannot argue or deny that they did not send out a particular message to another party.
- *Digital signature:* Digital Signature is a mathematical scheme which ensures the privacy of conversation, integrity of data, authenticity of digital message/sender and non-repudiation of sender (Kaur & Kaur, 2012).
- *Ethereum:* Ethereum is a major blockchain-based platform for smart contracts – Turing complete programs that are executed in a decentralized network and usually manipulate digital units of value (Tikhomirov, 2018).
- *Bitcoin:* Bitcoin is a digital currency which relies on a distributed set of miners to mint coins and on a peer-to-peer network to broadcast transactions (Biryukov et al., 2014).
- *API:* API is the acronym for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other (MuleSoft, 2021).
- *Two (2) Factor Authentication:* **“**An account secured with 2FA typically requires an individual to authenticate using something they know— typically a password—

as well as something they have, such as a cell phone or hardware token" (Reese et al., 2019).

- *Denial of Service (DoS):* A DoS attack prevents users from accessing a service by overwhelming either its physical resources or network connections. The attack essentially floods the service with so much traffic or data that no-one else can use it until the malicious flow has been handled (F-Secure, 2021).
- *Malware:* Malware is intrusive software that is designed to damage and destroy computers and computer systems (Cisco, 2021).

Summary

In this chapter, Non-Fungible Tokens (NFT) have been introduced, with the problem at hand – security and privacy issues – identified under the problem statement. The significance of the problem has been briefly described leading into the identification of the objectives and research questions of this project. The next chapter will expand on what other researchers have done and reveal some known vulnerabilities in the blockchain that NFTs are not immune to.

Chapter II: Background and Review of Literature

Introduction

This chapter provides more insight into the framework behind the use of Non-Fungible Tokens (NFTs). How blockchains generally work is first examined as NFTs reside on the blockchain, then NFTs in particular are analyzed as to how they work, the history, the standards that underly the usage and minting of NFTs, purposes and various categories of NFTs out there, the key features of NFTs, and the platforms in which these tokens are traded for. Furthermore, research efforts made by other scholars in the area of security and privacy issues related to NFTs are examined and discussed.

Background Related to the Problem

Non-Fungible Tokens (NFTs) have gained so much of a momentum in the past few years but is not a new phenomenon in blockchain as it was first seen some years back. A non-fungible token is a token or digital asset that cannot be replicated and is cryptographically unique in terms of the digital signature assigned to it (Bal & Ner, 2019). The fungibility trait of an asset makes it easy and possible to be interchanged like for like. For instance, a quarter cent cannot be uniquely differentiated from another quarter cent. This exact logic can be seen in all cryptocurrencies on the blockchain. One Bitcoin for instance cannot be uniquely distinguished from another Bitcoin. If you offer items for sale in return for bitcoin as mode of payment, you do not care the exact bitcoin a buyer sends you as payment for your goods or services. The non-fungibility characteristic of an item, in this case a digital asset, therefore, is the direct opposite of

what has been stated about fungible tokens. These tokens are not similar in any way. They might be identical, but they are different. The Mona Lisa painting is one of a kind – only one original copy exists in the world and can be found in the Louvre Museum in France. This does not mean people have not tried to make replicas of the Mona Lisa which may look identical to it. These replicas, however, are not same as the original. Hence, the Mona Lisa is a great example of a non-fungible item.

Buying a non-fungible token (NFT) in effect does not bring the exact digital asset in your possession. You are rather given the transferrable rights of ownership to that specific unique digital asset which could be an art or other collectables (Ante, 2021). This is a classic example of you not getting what you bought. NFTs reside on the blockchain, meaning it conforms first to how blockchain works and it has its own workflow tied into it.

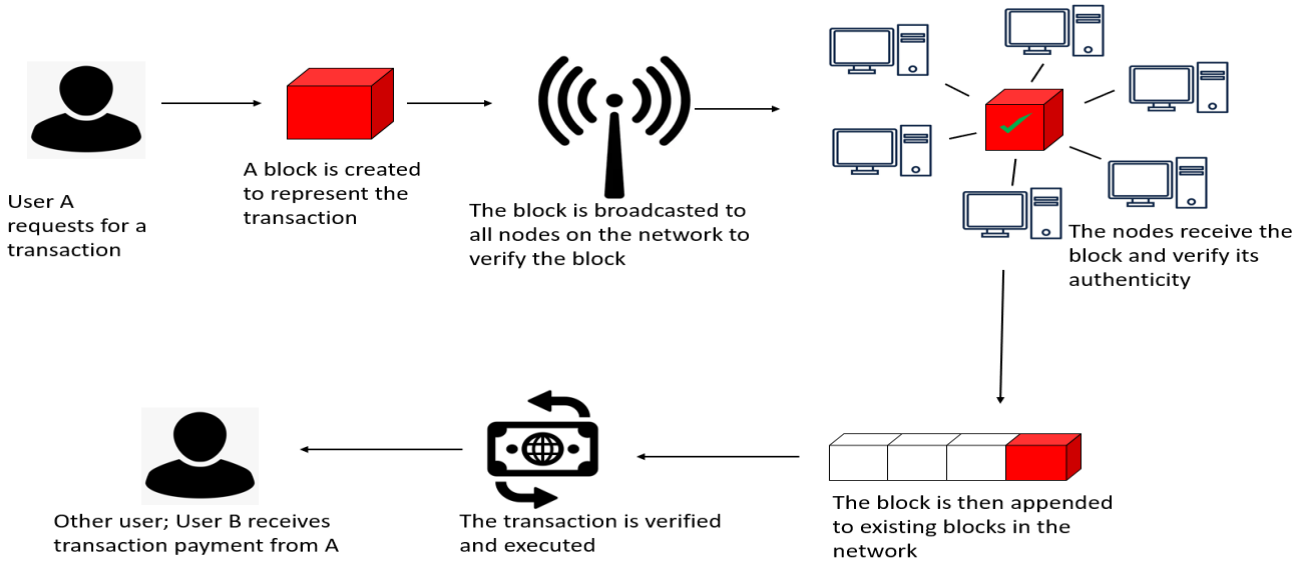
How blockchains work

According to Mosakheil (2018), a blockchain is “a database or a ledger that provides a way for information to be recorded and shared by a community. In this community, each member keeps his or her copy of the information, and all members must validate any updates collectively” (p. 25). In the blockchain ecosystem, when a user requests for a transaction, a block representing that transaction is created. This block is then propagated or broadcasted to every node on the network for these nodes to validate the authenticity of that block transmitted. Once the authenticity and verification checks are done, the block is appended to the chain on the network after

which the transaction gets verified, executed, and completed. These steps are graphically represented in Figure 1 below.

Figure 1

How Blockchains work



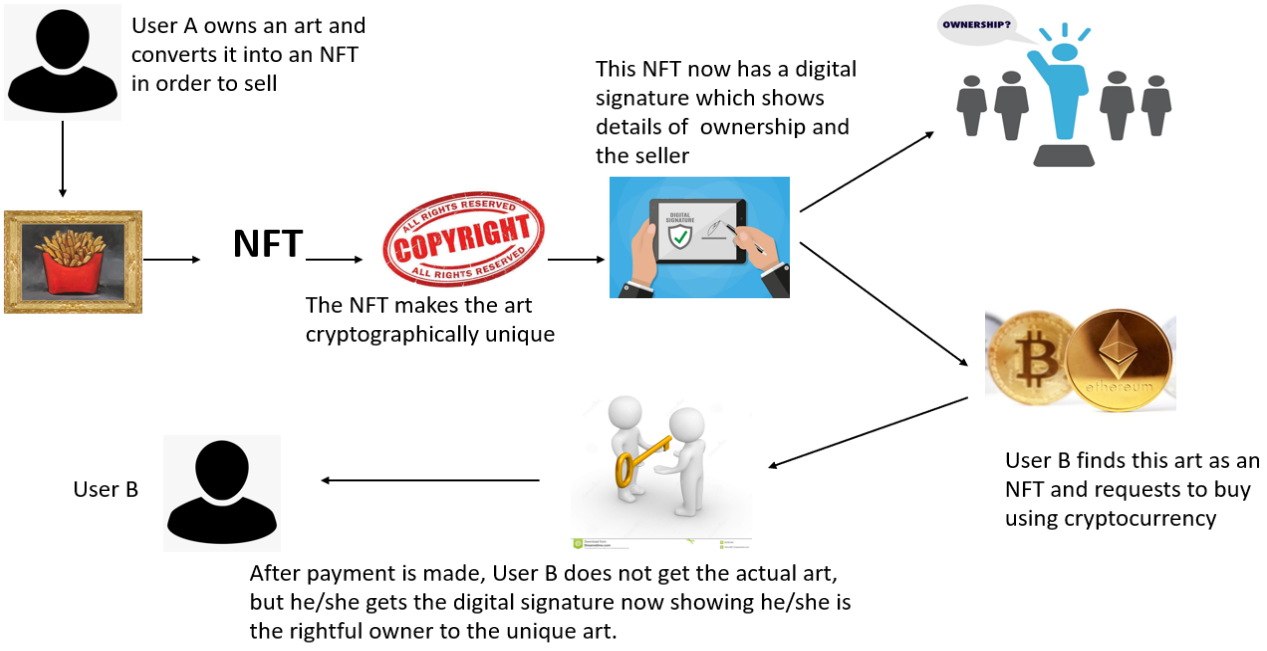
How NFTs work

As a resident on the blockchain, NFTs have their own workflow which is described in the following instance. Suppose User A is an artist who has been wondering how to commercialize their work and finally hears of NFTs. This user converts their art into an NFT, which goes through the processes of the blockchain ecosystem earlier described. This NFT makes the artwork of User A unique and one of a kind because it is attached to a digital signature which shows information of the owner and seller. The digital signature ensures authentication, non-repudiation and integrity of the NFT (Badev & Chen, 2014). With this cryptographically unique assignment, no other

copies could be made and be claimed to be the original. Even if User A had 2 copies of the same art and registers both as NFTs, they both are uniquely different as they have different digital signatures on the blockchain network. User B comes across this art which is now an NFT and requests to buy it using cryptocurrencies such as Ethereum or Bitcoin, among others. User B does not get the digital art in their possession, but rather gets the digital signature which now shows their ownership of the NFT. Figure 2 below gives a diagrammatic representation of the processes outlined above.

Figure 2

How NFTs work



History of Non-Fungible Tokens (NFTs)

In 2012, Colored Coins were introduced, which some people argue were first of NFTs to have been used (Bamakan et al., 2021). Colored Coins comprise of very small quantities of bitcoin which could be as small as a unit of Satoshi. A Satoshi refers to the smallest unit of a bitcoin (Ober et al., 2013). These Colored Coins were used to represent the various assets and they had varying uses. For instance, 3 people could come together and agree that 100 Colored coins represent 10,000 shares in a particular company. But these uses were purely based on agreements between the parties. In 2014, Robert Dermody, Adam Krellenstein and Evan Wagner founded the Counterparty which was a platform adopting the peer-to-peer decentralized operations that allowed trading of memes and card games. This platform came to being because the use of Colored Coins at the time was different from what Bitcoin was created for. Spells of Genesis was then deployed on the Counterparty platform in 2015 which allowed the issue of in-game assets onto the blockchain with the currency being traded for with something known as BitCrystals. Later in 2016, “Rare Pepes” was deployed on the counterparty platform which was the trading of memes of a frog character. Rare Pepes grew so massively that they had experts who certified the uniqueness and rareness of these memes. This brought up the signals of people liking unique digital assets. Rare Pepes later moved to the Ethereum platform early 2017 after Ethereum gained so much momentum in the crypto and blockchain world. In late 2017, John Watkinson and Matt Hall decided to create their own version of unique characters on the Ethereum blockchain. This was called Cryptopunks. In this project, they offered 10,000 unique

different characters, for free to anyone who had the Ethereum wallet. After these characters were claimed, they went into circulation as people started to trade for them. These Cryptopunks were a hybrid of the ERC20 and ERC721 standards. These standards will be explained and differentiated later. October 2017 saw the birth of the full-fledged NFT which was named CryptoKitties. This is a blockchain-based game which allows players to raise and trade digital cats. The difference between CryptoKitties and all earlier versions of games and transactions on the blockchain is that this is solely based on the ERC20 standard which is the standard used in creating NFTs. All earlier transactions created on the Ethereum platform was based on the ERC721 standard (Steinwold, 2019).

NFT Standards

The two major standards used in creating Non-Fungible Tokens are ERC-721 and ERC-1155 standards. But before we describe what both standards are and do, it is imperative for us to know what the ERC-20 is, before we differentiate between these three standards.

First off, ERC stands for Ethereum Request for Comments (Norvill et al., 2019), and these standards are sets of functions developed by individuals and are accepted as the yardstick for determining how these token types interact with other applications and smart contracts (Febrero, 2019). In 2015, the ERC-20 was proposed. This is a standard to set out the functionalities of fungible tokens on the Ethereum blockchain. These ERC-20 tokens are similar to other cryptocurrencies such as Bitcoin, Litecoin and the likes.

But they reside specifically on the Ethereum blockchain. These tokens, just like all other cryptocurrencies, are identical, interchangeable, and not unique.

Later in 2018, ERC-721 was proposed, which is a standard that provides the API for non-fungible tokens in Smart Contracts. This standard came as an extension of the ERC-20 as people delighted in having ownership in unique digital assets and the desire to develop such digital assets grew extensively. This has been the go-to standard in the creation of NFTs.

The ERC-1155 standard also was proposed to provide functionalities for typically semi-fungible tokens as well as provide the API for both fungible and non-fungible tokens to be in the same smart contract. With this standard, developers can define which fungible and non-fungible tokens to use and how many of each exist on the Ethereum blockchain. A sample code for both ERC-20 and ERC-721 has been provided below in Table 1 to provide differentiation from the function and event code perspective.

Table 1

Sample code for ERC-20 and ERC-721 standards

ERC-20	ERC-721

`function name() public view returns (string)`
`function symbol() public view returns (string)`
`function decimals() public view returns (uint8)`
	`function balanceOf(address _owner) external view returns (uint256);`
	`function ownerOf(uint256 _tokenId) external view returns (address);`

function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
 	
function transfer(address _to, uint256 _value) public returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
function approve(address _spender, uint256 _value) public returns (bool success)
function allowance(address _owner, address _spender) public view returns (uint256 remaining)
 	
event Transfer(address indexed _from, address indexed _to, uint256 _value)
event Approval(address indexed _owner, address indexed _spender, uint256 _value)
	function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data) external payable;
	function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
	function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
	function approve(address _approved, uint256 _tokenId) external payable;
	function setApprovalForAll(address _operator, bool _approved) external;
	function getApproved(uint256 _tokenId) external view returns (address);
	function isApprovedForAll(address _owner, address _operator) external view returns (bool);
	
	event Transfer(address indexed _from, address indexed _to, uint256 indexed _tokenId);
	event Approval(address indexed _owner, address indexed _approved, uint256 indexed _tokenId);
	event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);

ERC-20 Standard sample function available at: https://ethereum.org.en/developers/docs/standards/tokens/erc-20/	ERC-721 Standard sample function available at: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

Purpose and Types of NFTs

Non-Fungible Tokens (NFTs) have become a huge boost to the commercialization of products of artisans, musicians, and owners of other collectables. Artists, for instance, saw their patronage of art in general take a nosedive as compared to earlier sales as people now visit exhibitions just for the mere curiosity and not with the intention to really purchase. Arts in their physical nature are rare as most artists make just a single copy of their work. Since the introduction of NFTs, artists have gained a different way of looking at how to commercialize their work and how to reach greater market.

NFTs make rare items such as art more unique and scarcer. One of the basic laws of economics projects that high prices yield high profits for products which have high demand but are low in supply respectively. Artists can now create NFTs for their work, which can be verified on the blockchain with a specific digital signature. This makes it easy to be located, hence scarce, and this is then offered to highest bidder in an auction. This is a way for artists to rake in profits that previously were not incoming.

On the other hand, in the music industry, NFTs have gained much recognition as musicians and DJs now prefer to create NFTs for their music and offer them for sale in

order to get 100% or almost of all the profits on the sale of their music. Musicians may prefer this compared to uploading their music on streaming platforms and having record labels take out their cut in profits from sales.

NFTs have come as a revolution in creating autonomy for people in the creative industries, as they can now rely on the scarcity of their work to reach their target market of people who desire unique and one of a kind digital asset which they can claim to be sole owners of.

NFTs could be grouped into seven different categories as per the various use cases of NFTs on the blockchain currently in circulation. These categories are Art, Games, Music, Collectibles, Utility, Metaverse, and Other. Table 2 below, shows the descriptions of these categories of NFTs listed and these operative descriptions were inspired by Nadini et al., (2021) and Brown (2021).

Table 2

NFT categories and their descriptions

CATEGORY	**DESCRIPTION**
Art	NFTs of digital artworks, images such as memes, videos such as some big sports moments, or GIFs
Games	NFTs used in competitive games such as CryptoKitties

Music	NFTs created for musical tracks in the form of digital files
Collectibles	NFTs worth collecting and of interest to a collector
Utility	NFTs created for some specific purposes such as domain names and virtual fashion where people trade clothes not to wear themselves but to dress up their avatars
Metaverse	NFTs created for pieces of virtual worlds
Other	These are the other NFTs not captured under the descriptions of the above categories

Key features of NFTs

Non-Fungible Tokens have some characteristics which makes them different from other tokens on the blockchain. As the name non-fungible implies, most of these features breed from its name. Some key features of NFTs are that they are unique, provably scarce, indivisible, easily transferable and they guarantee ownership.

Unique: No two NFTs are the same even if the same person created both. This is because they have different digital signatures attached to it.

Provably scarce: Because NFTs are unique and cannot be replicated, they are scarce as there are only single versions available. These scarce versions, however, are always accounted for as the number of NFTs can always be determined at any point in time hence its characteristic, provably scarce.

Indivisible: NFTs cannot be divided into smaller units or denominations, as other tokens can be. This implies that one cannot buy or sell a proportion of the NFT. It is either all or nothing.

Guarantee Ownership: NFTs have digital signatures specific to them when created and these digital signatures serve as “copyright” that shows who owns that NFT. This is a way of verifying who has the right of ownership of that token on the blockchain.

Easily Transferrable: The characteristic of NFTs having digital signatures makes the transfer of these tokens easy and relatively safe as compared to other tokens such as cryptocurrencies. With NFTs one can verify whom the NFT was sold by, who owns it, as well as who bought it. This makes transfer of the rights to ownership easy as the actual NFT is not technically traded for, but the cryptographic web address that points to that NFT is rather bought and sold. This then tells who the rightful owner of that NFT at any point in time is.

Table 3 below gives a glance at what makes non-fungible tokens different from fungible tokens on the blockchain.

Table 3

Difference between fungible and non-fungible tokens

Fungible Tokens	Non-Fungible Tokens
Uniform All fungible tokens that are of the same type and design are indistinguishable and similar in specification. For instance, 1 Bitcoin is identical to another Bitcoin. No Bitcoin can be exclusively distinguished from another.	**Unique** Each non-fungible token is distinctive from others even though they may belong to the same category. For instance, taking the category of art, 2 paintings made by the same artist are distinctive and uniquely individually as they each have different digital signatures on the blockchain.
Interchangeable Fungible tokens can be exchanged for other fungible tokens of same type. For instance, 1 Ethereum can be exchanged with another Ethereum without any reservations to the exact Ethereum traded with.	**Not Interchangeable** Non-fungible tokens are not interchangeable for other non-fungible tokens. This is because NFTs are each valued differently so no two NFTs can be traded for with each other. Rather NFTs are traded for with fungible tokens after their values are determined.

Divisible Fungible tokens can be separated into smaller units and these units are identical and does not matter what units you get so far as the value is the same. For instance, a $10 bill can be divided into 2 $5 bills without any concerns to the holder.	**Indivisible** Non-fungible tokens are not divisible. They cannot be separated into smaller units. It is just a single token and one token only. For instance, a metaverse NFT cannot be divided into any known smaller units.
ERC-20 Standard The standard functions for creating fungible tokens are based on the ERC-20 standard	**ERC-721 Standard** The ERC-721 standard is the base standard for creating non-fungible tokens even though the ERC-1155 brings to the table an overarching standard encompassing both tokens.

Note. Source: (0xcert, 2018)

NFT Platforms

For every item of trade there is a platform that brings buyers and sellers together for the transactions to take place and non-fungible tokens are no different . Many

platforms out there have been created to hold the trade of NFTs. The most top ranked platforms across the web as rated by various publishers and bloggers are OpenSea, Rarible, Axie Marketplace, Larva labs, NBA Top Shot Marketplace, SuperRare, Foundation, Nifty Gateway, and Christie's among others (Bourcart, 2021; Lucker, 2021; Rossolillo, 2021). What these platforms have in common is that they all use the auctioning mode of trade in, making transactions for these NFTs. The highest bidder gets the NFT on auction.

Literature Related to the Problem

This section describes the work done by other researchers with respect to the nature of the problems stated about non-fungible tokens (NFTs).

Liscia (2021) provides an overview in their article about how Nifty Gateway, one of the most top ranked NFT platforms out there, was hacked with the accounts of several customers compromised. This is seen by many as the first heist in the NFT world, as this hack really exploded on the news. Most of these account holders took to Twitter to vent their rage for their loss of digital assets, and even their money sitting on their credit cards. Nifty Gateway appears to allow customers to trade NFTs with their credit cards as opposed to other platforms, so the security compromise of these accounts also meant some Personally Identifiable Information (PII) of these customers were also accessed. According to the author, Michael Miraflor – who is a renowned media strategist – was one of the victims of the compromised accounts and he tweeted that all his NFTs were transferred to a different account. He also tweeted that his credit card on file was used to purchase more than $10,000 worth of NFTs, which were

subsequently transferred to a different account. Nifty Gateway however released a statement that the small group of accounts compromised did not have 2 Factor Authentication enabled and this made it easier for the hackers to succeed in their heist.

According to Powers (2021), a hacker was selling a zero-day vulnerability as an NFT on OpenSea – the highest ranked NFT platform (Wang et al., 2021). It took the intervention of OpenSea to take down the auction of this NFT from their platform. The Hacker goes by name Matthew Hickey of Hacker House, and in his own words, according to the report he advertised, the token was a "…post-authentication memory corruption vulnerability in ioquake3 engine. The issue can be exploited to cause a denial-of-service condition, code execution has been deemed unlikely. This issue has been tested on OpenArena but should be present in all 28 games using the idTech3 (ioquake3) engine". Zero-day attacks are however still being sold on black markets by creating NFTs for it. The buzz around NFTs has been exploited as an avenue for legitimizing the sale of such. This NFT was the first to be blocked but will certainly not be the last.

An article by Cimpanu (2021) discusses how NFT creators were tricked into installing malware files. In this attack, the threat actor targeted several NFT creators on Twitter and dialogued with them privately, posing to be other prominent NFT platform officials. They then sent malicious files to these targeted creators disguised to be windows screensaver (.SCR) files. Once these were clicked on, the accounts of the targeted group on any non-fungible token platform gets compromised. One person revealed that they lost all their tokens in their account. According to this report, the

malicious file of the (.SCR) format contained Redline malware which can collect both browser credentials and cryptocurrency wallet configuration files. Several NFT creators were affected as one victim confirmed that the attacker managed to swipe more than 40,000 AXS tokens, which is worth around $176,000.

Literature Related to the Methodology

As this paper is focused on analyzing the threats, attacks, security, and privacy issues around non-fungible tokens (NFTs), works of other researchers in these areas are reviewed.

The paper by Wang et al. (2021) provides great insight into the overview, evaluation, opportunities and challenges of NFTs. The authors in this paper, however, evaluated the current NFT security system from a much generalized perspective as they adopted the STRIDE threat and risk evaluation in their analysis. STRIDE represents Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege. They further mentioned about some security and privacy issues which they foresee to be related to NFTs such as legal pitfalls, anonymity issues, data inaccessibility, NFT interoperability and updatable NFT issues. These yet again represent a generalized scope with respect to some specific threats, attacks, security, and privacy issues related to NFTs.

An article published by Bonderud (2021) – “Token Resistance: tackling the New NFT Threat Landscape” – points out an interesting twist to the security issues related to NFTs. The author mentions that in the early development of the NFT concept, one of the minds behind it, Anil Dash, said they ran into technological limitation. As a result,

they had to adopt a workaround which was encrypted web addresses that acted as links to these NFTs. These web addresses are still in operation which means that buyers are getting access to links to the specific digital assets they buy. The security issue with this is should the companies that host these web address links on the servers go out of business, NFTs of several individuals also go down the drain as no verifiable means of ownership can be traced to those digital assets on the blockchain.

Another article by Garimella (2021) – “NFT Scams Part 1:5 NFT Scams you need to know” – attempts to address the security issues of NFTs from the platform lens. According to the author, many scams are being recorded daily because the authentic platforms for trading NFTs have been cloned to trap certain individuals who fall to it. Aside from creating these replica stores in the form of clones, others have created fake NFT stores with domain registrations resembling authentic ones. These are other avenues for hackers to exploit the innocent NFT creator or buyer.

Summary

This chapter provides a brief summary of the concept of non-fungible tokens, the history, characteristics, standards, categories, and platforms on which they are traded. Included in this chapter was also a literature review conducted on works by other researchers with respect to the problem and methodology.

Chapter III: Methodology

Introduction

The qualitative research method was mainly used in this study to identify some already identified threats and vulnerabilities on the blockchain that Non-Fungible Tokens are not immune to. A survey into already published papers about the subject matter was explored comprehensively to categorize these threats. Using surveys and attack scenarios are key components of the qualitative form of research study as compared to the quantitative research method. This chapter summarizes the threats posed to the traders of NFTs, which have been categorized into four taxonomies.

Design of the Study

This study took the form of a qualitative approach by exploring research work conducted in the general field of blockchain security and classified them into a taxonomy, as Non-Fungible Tokens (NFTs) are not immune to the known security and privacy threats on the blockchain. Since this is a new field of research, the security threats specific to NFTs were investigated extensively and the identified threats specific to NFT security were also categorized into a taxonomy.

In this chapter, the goals to be achieved were the objectives of this study as stated earlier in the previous chapter.

- Studying and surveying this new area of Non-Fungible Token trading – this will be done by investigating this new phenomenon using google scholar in reviewing any already published works by other researchers (even though not much

research papers in this area have been published) and also utilizing the news outlets with regards to their information security posts in news articles.

- Identifying the security and privacy issues related to trading in NFTs, both the known issues of blockchains in general and the emerging ones specific to NFTs – this will be achieved by setting some time apart and surveying research carried out on blockchain security as NFTs are not immune to such known security issues, then classifying the identified security issues into a taxonomy.
- Identifying the gaps in the field with respect to what has been done and what needs to be done to educate anyone looking to trade in NFTs – this paper is intended to be a source of education and insight to all readers, as it is my aim to make people aware of the precise security issues to be anticipated for since currently, they have not been pinpointed.
- Recommending solutions to the identified security and privacy issues

This study does not lack a research design concept because since it takes the form of a qualitative approach, it has its own inherent design identified with the taxonomy tool (Maxwell, 2008).

The systematic survey used in this study places emphasis on the security threats identified by labelling them into three different taxonomies. The first taxonomy focuses on the known security threats on the blockchain which NFTs are a subset of. The second taxonomy encompasses the security threats as identified in the wallets of NFT

users and the trading platforms or markets for NFTs. The third taxonomy classifies the NFT specific threats outside the trading platforms.

Data Collection

This study required the use of both primary and secondary data. Primary data in the sense that they are originating directly from the source and secondary data in the sense that they are obtained from other published works by other researchers. For the primary data, these were obtained from individuals who have experienced any form of security issues or flaws while trading in Non-Fungible Tokens (NFTs). They have also either posted on any of their social media accounts, especially Twitter, or were reached for interviews through emails, which was one way I sought to employ in this study. For secondary data, I obtained these from published papers and articles on Google Scholar, the University repository for culminating projects, Microsoft Academic, blogs, and news articles by various news outlets among others.

Finding a vast pool of resources with respect to secondary data of the form was a major challenge during this research. Nonetheless, this research was not to be restricted to only information from published papers, so I sought to utilize blogs and news articles as well.

Tools and Techniques

The tools which were used in this study were Google scholar, the University repository for culminating projects, news articles, blogs, and social media platforms such as Twitter.

After the primary and secondary data were gathered using these tools, the security and privacy issues based on the findings were classified into taxonomies. A taxonomy is the practice and science of classification (Groenewald, 2010).

First Taxonomy: this presents the main framework on which the identified security threats in this study are categorized. The main vectors of security threats are the known security vulnerabilities identified on the Blockchain, vulnerabilities in the wallets and Trading platforms of NFTs, and the Smart contract-based vulnerabilities.

Second Taxonomy: this comprises the known security threats and vulnerabilities identified on the blockchain. This taxonomy is expanded at a high level, into three layers or routes of attack which are Mining threats, Double-Spending threats and the Network threats. Each layer has specific attack routes and scenarios presented in the continuing chapter.

Third Taxonomy: this encompasses the security threats and vulnerabilities in the wallets and Trading platforms of NFTs. NFT users, just like any blockchain asset holder, uses wallets to facilitate trading, but NFTs have dedicated trading markets intended for only buyers and sellers of Non-Fungible Tokens.

Fourth Taxonomy: this incorporates smart contact-based security threats and vulnerabilities. NFTs are based on Smart Contract design and hence these vulnerabilities could be classified as NFT specific vulnerabilities.

Summary

In this chapter, the design of the study has been identified and presented. The paper took the form of a systematic survey of works by researchers in the field. The

tools which were used have also been highlighted with the main tool used in classifying the data being taxonomy.

Chapter IV: Data Presentation and Analysis

Introduction

This chapter places more emphasis on the security threats identified and categorized in the various taxonomies. The security threats are first categorized under three main headings: 1) The known and identified threats on the blockchain, 2) The security threats in wallets of users and trading platforms of NFTs and 3) The security threats associated with Smart contracts or the NFT specific security threats.

The distinction between these categorizations does not imply NFTs cannot suffer attacks from the first two categories identified since the third categorization has a more precise wording as “NFT-specific”.

Data Presentation

Figure 3

Taxonomy showing categorizations of Vulnerabilities in Non-Fungible Tokens

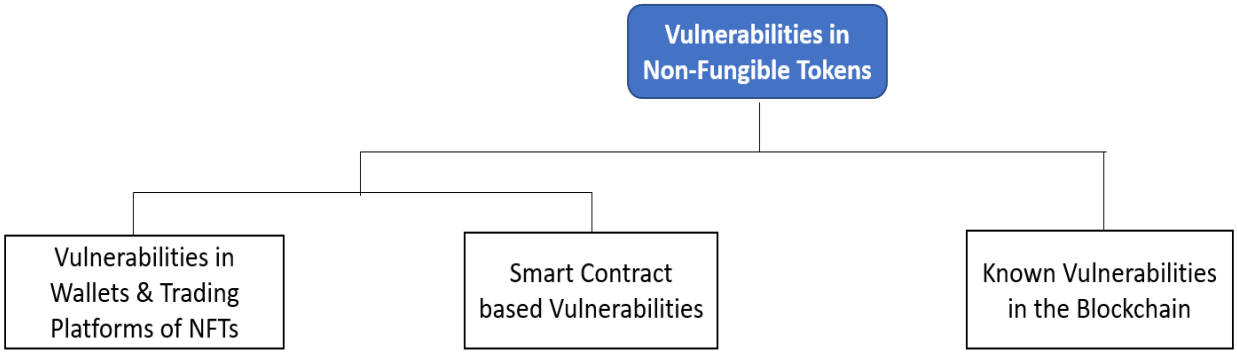
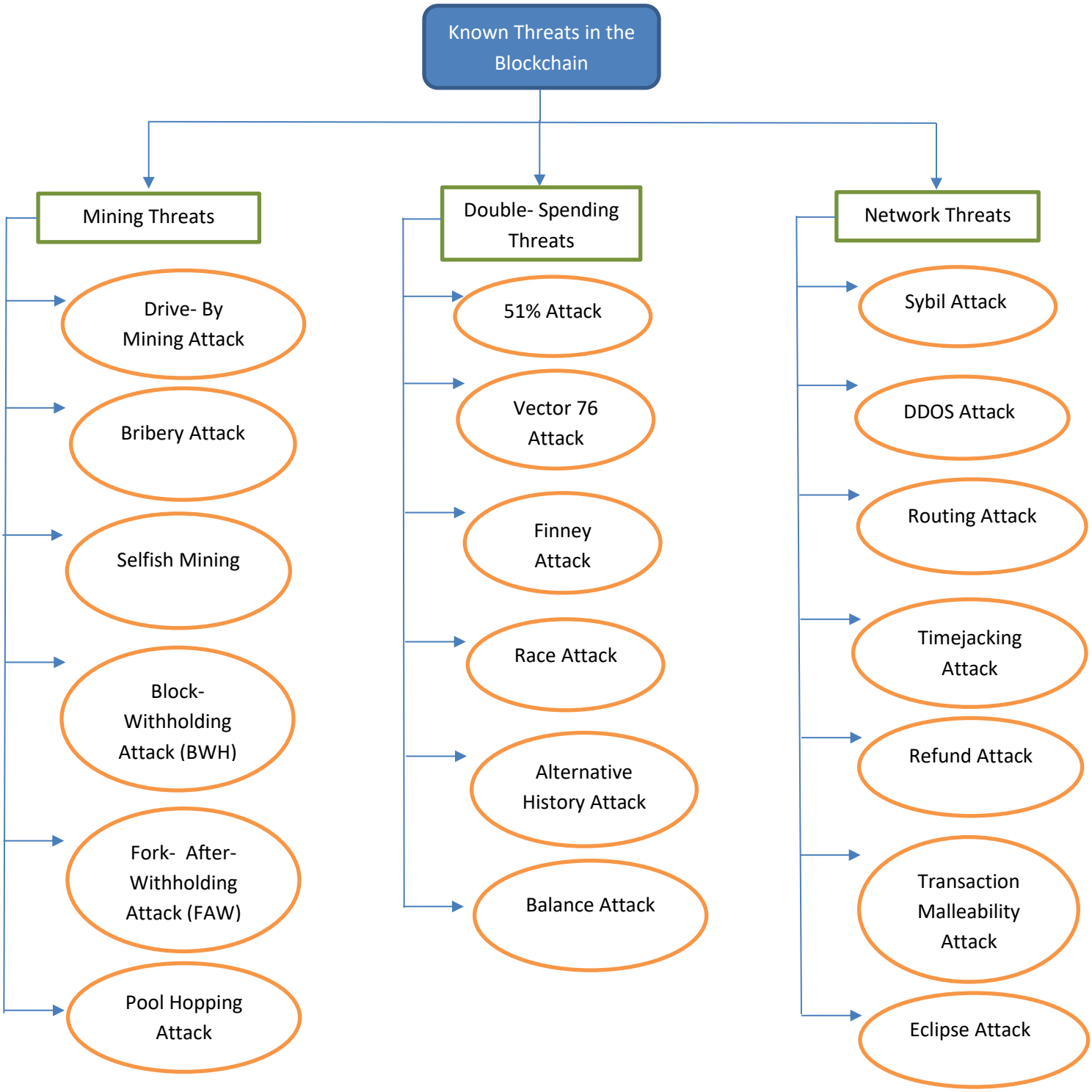


Figure 3 above shows the three main categorizations of the security vulnerabilities and threats that will be emphasized in this chapter and study.

Figure 4

Taxonomy of Known Vulnerabilities in the Blockchain



The relationship between NFTs and the blockchain as a result of NFTs being digital assets located on the blockchain makes NFTs inherit the positive and negative aspects of security on the blockchain. In essence, NFTs are not immune to the attacks on the blockchain.

Mining Threats

The mining pool plays a significant role in digital asset block generation on the blockchain. A mining pool is an organization of a group of miners who come together to share resources such as mining power and allow members to decentralize tasks amongst themselves and share the rewards or proceeds that result from their operations (Konoth et al., 2018). In order to create and maintain some form of order in blockchain mining activities, a mining pool manager or operator role is created. This manager oversees the amount of work by each mining pool member and enforcing that blocks/shares are ordered (Chang & Park, 2019). Regardless of the presence of the mining pool manager, there are still some attacks on the mining pool caused by either a cluster of the members themselves or individual members who have the ambition to hoard the blocks mined and keep all the rewards generated for themselves (Conti et al., 2018). The attacks on blockchain mining pools can be identified under two sets of influences: the internal influence and the external influence. The internal attacks are carried out by dishonest miners who for a period of time will propagate blocks on the network for validity checks by other members but later on begin to interrupt the activities of the honest miners by collecting more than what should be attributed to them in the collective share of rewards. The external attacks, on the other hand, are orchestrated by

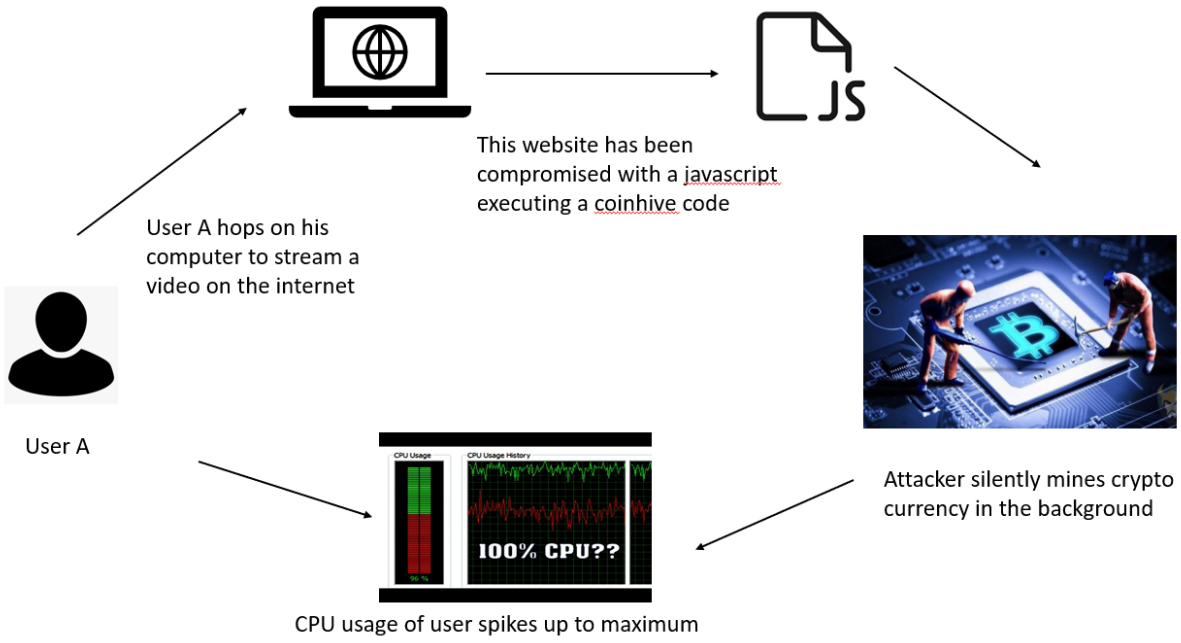
miners outside the specific blockchain mining pool who either disguise themselves as authenticated members of the pool or even disrupt the network latency of the pool using some Distributed Denial of Service mechanisms (Mosakheil, 2018).

Drive-by Mining Attack

Konoth et. al (2018) describes drive-by mining (also known as cryptojacking) “as a new web-based attack, in which an infected website secretly executes JavaScript code and/or a WebAssembly module in the user’s browser to mine cryptocurrencies without her consent” (p. 1714). This type of attack utilizes the concept of a drive-by download on user devices. This occurs when an individual visits a website and unintentionally downloads a malicious code or file embedded in that website. These malicious code or files can cause a lot of harm to this user without the user even recognizing the activities happening behind the scenes. In drive-by mining attacks, hackers and attackers add javascript code containing the coinhive lines behind some frequently visited websites which record constant traffic load. These websites are mostly pirated or offer to allow free streaming of movies or music videos. The drive-by mining happens silently in the background without the consent or even the recognition by the user. Once activated, the CPU resources of the device gets taken up to almost a 100% usage in mining these cryptocurrencies and the rewards goes to the attacker with the user unknowingly bearing costs of increased electricity and the processing power of their resources. The concept of drive-by mining may not be entirely criminal, but should the consent of the users involved not be sought, then it amounts to using someone else’s property to make income off of.

Figure 5

How Drive-by mining works



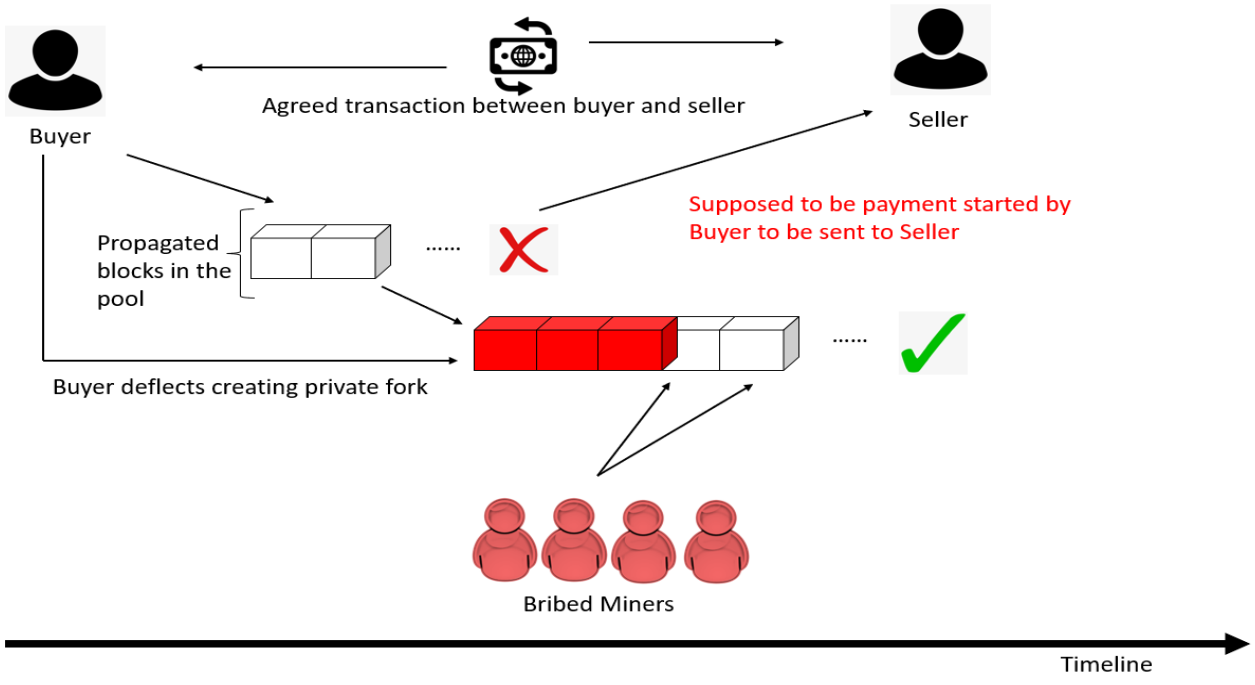
The figure above illustrates how a user surfs the internet to certain unprotected sites not knowing these websites have been compromised with some code injections in the background. Their presence on the website triggers the execution of the code and this allows the attacker to mine cryptocurrencies behind the scenes, causing the CPU usage of the user to spike. The end result is that the reward of the mining goes to the miner but the user bears all the expense that come along with it.

Bribery Attack

In the bribery attack, the attacker bribes other honest miners in a pool by purchasing their mining and computational power so they mine on a block propagated by the attacker. The fork to be mined contains the bribe money in the form of a cryptocurrency, for instance Bitcoin. The attacker could also outrightly rent the computational power of some miners or even form a pool promising higher return for participants in this type of attack (Conti et al., 2018).

Figure 6

How Bribery attack works



In Figure 6 above, a dishonest miner sends a transaction purported to be the valid payout transaction to a seller, who releases goods to buyer after confirming the

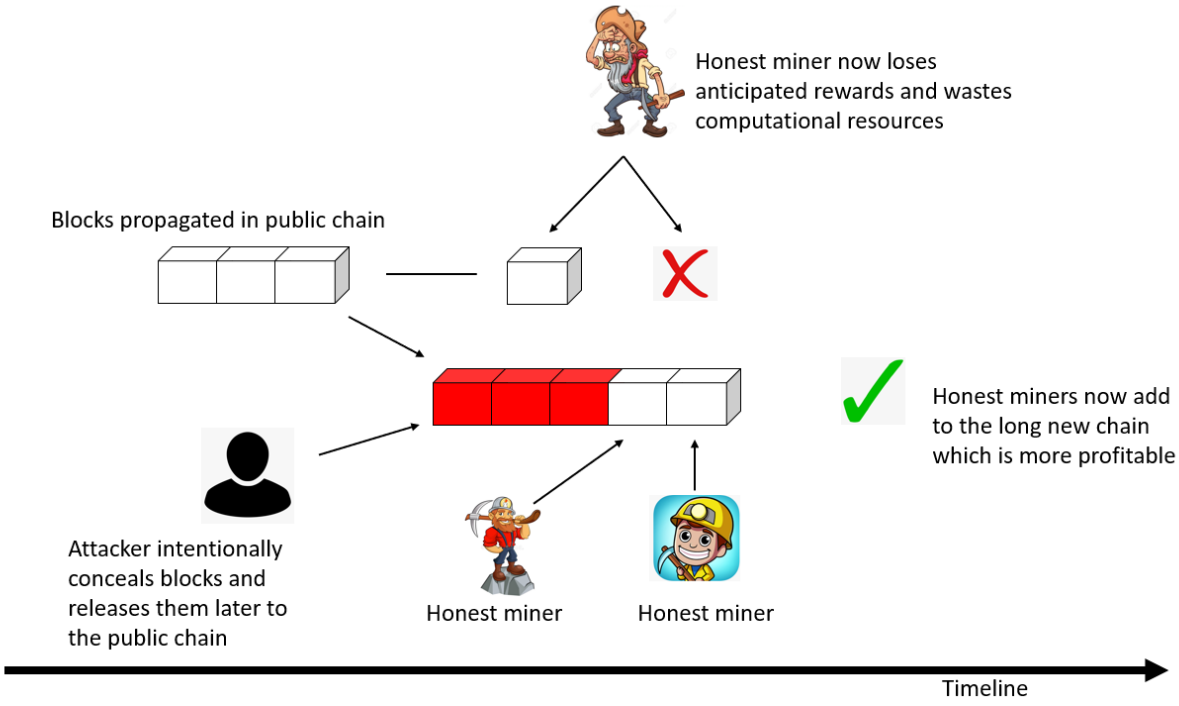
transaction. The attacker then creates a private fork by bribing other miners to mine on top of this private fork thereby discarding the original transaction. This second transaction is reengineered to pay out rewards back to attacker resulting in a double spend.

Selfish Mining Attack

A selfish mining attack is where dishonest miners in a pool try to maximize their rewards as much as possible by either confusing the honest miners in the pool into wasting their computational resources or by gaining an unfair share of the rewards due to them per the computational effort put in. In selfish mining, the dishonest miner hides information about the discovered block without propagating into the pool and selectively shares these blocks creating some chains per their discretion.

Figure 7

How selfish mining attack works.



In figure 7 above, there are blocks in the public domain which miners are supposed to add up blocks to for shared mining on these blocks, but the dishonest miner chooses to create his own private fork of blocks by deviating from the standard protocol. An honest miner finds one block and send it to the pool but later, this dishonest miner propagates all three blocks he kept secret, and the other miners are shifted to the long new chain which now becomes the main public chain. This implies

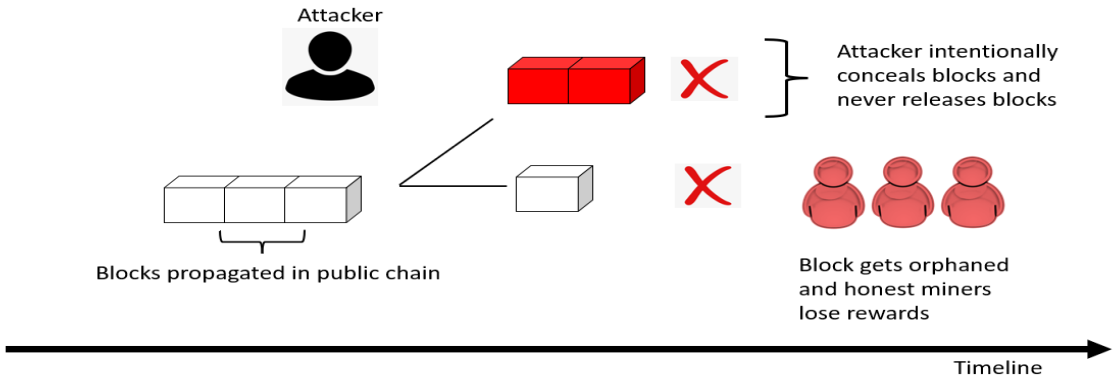
the block sent by the other honest miner to the previous fork gets discarded and he loses all the rewards and computational resources used in propagating that block.

Block-Withholding Attack (BWH)

This attack occurs when the attacker conceals the block by permanently delaying the submission of the block. This is a deliberate act to sabotage the protocols of the mining pool. The attacker pretends to be contributing to the pool and gets the rewards accrued from participating in the pool but never propagates the blocks they find. The BWH is mostly carried out by attackers in infiltrated pools who have the motive to cause most of the honest and legitimate miners to lose their fair share of rewards by hoarding and discarding blocks. This reduces revenue generated in the victim mining pool.

Figure 8

How Block- Withholding (BWH) attack works



In figure 8 above, an attacker infiltrates the victim pool purporting to be an honest miner who is significantly contributing his hash power or computational power to the pool. This dishonest miner / attacker conceals all the blocks he finds permanently

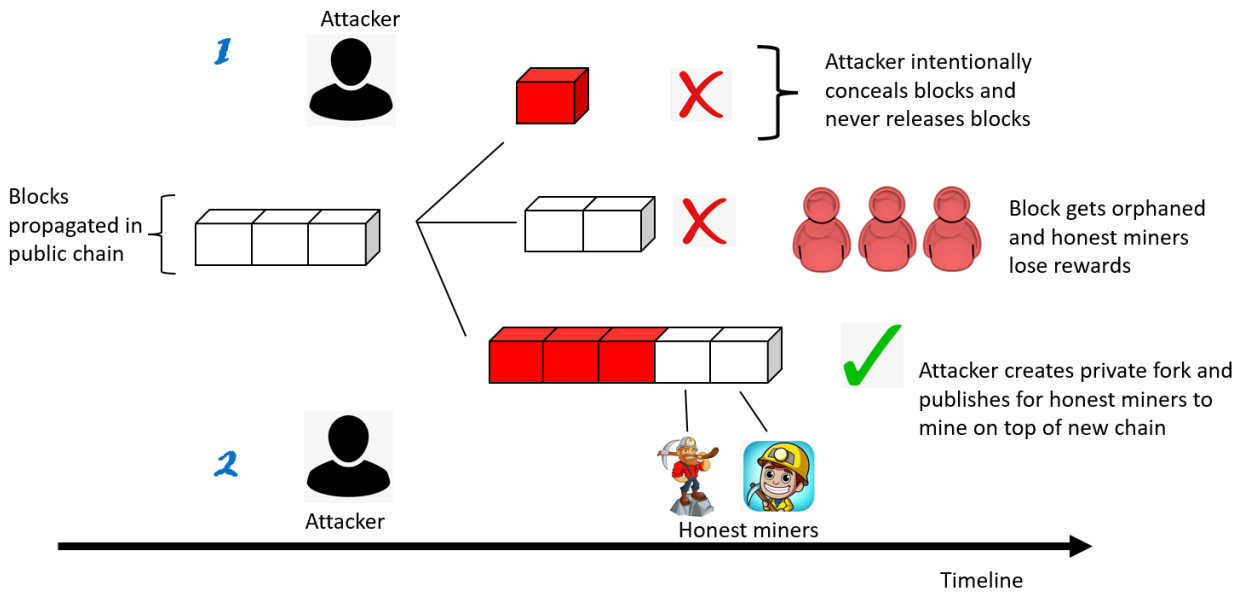
without propagating these. He creates a private fork but later discards it just to cause the honest miners in the pool to lose their rewards and waste computational resources.

Fork-After-Withholding Attack (FAW)

The Fork-After-Withholding attack is a variation of selfish mining and the block-withholding attack, where the attacker intentionally refuses to submit the blocks they find and starts to create a private fork in a private chain. In this scenario, the attacker later either releases the privately held blocks as in selfish mining attacks or discards them as in the block- withholding attack. The FAW attacker releases the private fork to the public domain if that generates more revenue or the attacker decides to never publish the fork if an honest miner found a block that is much profitable in rewards than the withheld block held by the attacker. Yet again, the attacker may also drop the withheld blocks if they find the blocks in the second or alternate mining pool in which they are honest miners, having more rewarding compensation than the infiltrated pool. This means attackers would also want to maximize their rewards by comparing which option will give high returns at any given time.

Figure 9

How Fork- After- Withholding (FAW) attack works



In figure 9 above, the FAW attacker has two scenarios which they tend to pick whatever instance benefits their motive the most after splitting computational power into 2 pools: the honest mining pool and the target pool to be infiltrated. In both instances, the attacker conceals blocks he finds and creates a private fork from that. Depending how beneficial an instance will be to the cause of the attacker, he either discards the concealed block(s) or publishes the private chain to the public pool. An attacker discards the privately held blocks if he realizes that the rewards generated in finding and publishing blocks in the honest mining pool are much greater than the rewards that he can accrue in the target pool. The attacker will have no reason to continue holding onto these blocks and wasting computational resources. On the other hand, an attacker

will publish the private chain of blocks withheld if he realizes the rewards in the infiltrated pool outweigh the rewards in the honest mining pool.

Pool Hopping Attack

The pool hopping attack happens when miners decide not to stay loyal to a specific mining pool for a long period. Mostly miners are looking to maximize rewards, hence with any given chance or favorable circumstance these miners will hop off from one mining pool to another with the latter being more lucrative in terms of rewards generated compared to the former. This attack is based mainly on the attractiveness of the pool in terms of rewards offered to miners (Rosenfeld, 2011).

Double-Spending Threats

To double-spend simply means to use the same currency, which is a mode of transaction, on multiple occasions as against the required one-time use. Double-spend attacks on the blockchain presents scenarios where the attacker uses means to outwit sellers by never really transferring the required funds for goods or services purchased. This is done by re-engineering the process where the attacker intentionally creates a private fork aside from what was originally propagated in the public domain, meant to be transaction tagged to be sent as mode of payment to seller. The attacker later publishes the blocks held up privately into the public mining pool. As rational as miners on the blockchain are, they will move to mine on top of the long new chain in the public stream. By doing so, the original transaction which the seller saw coming through gets dropped and the funds go back to the buyer effectively double-spending same cryptocurrency promised to be paid to seller (Frankenfield, 2022).

51% Attack

The blockchain mining network comprises of a group of miners who come together in unity to follow some protocols and agreed upon processes overseen by a pool manager. As a result, the influence of a single miner, even though harmful and can disrupt the mining operations is well kept in check. However, miners coming together to form a coalition becomes dangerous for the network as they can control the entire network's mining hash rate. This hash rate refers to the computing power needed by the cryptographic algorithms of these blocks. The alteration power to blocks becomes the privilege of this majority in any mining pool. In the event of a 51% attack, the attackers are "able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control" (Frankenfield, 2022).

Race Attack

In a race attack, the attacker, after entering into a transaction in the capacity of a buyer with a seller, sends two conflicting transactions in a swift sequence into the cryptocurrency network. Here, the notion is to facilitate double spending by deceiving the seller into believing a transaction has been started hence they will release goods bargained for to buyer, but the cryptocurrency transaction never happens. The attacker hopes for honest miners to mine on top of the duplicate block/ transaction created so the original gets discarded. These two transactions therefore enter a race as to which

has the shortest latency to be mined on by the rational miners. The duplicate transaction is reengineered to pay the rewards back to the buyer/attacker.

Finney Attack

A Finney attack happens when a vendor accepts an unverified cryptocurrency transaction from a buyer/attacker. In a Finney attack, the attacker discovers a block in the mining pool but conceals the block from the mining pool and sends this unconfirmed block to the seller. Because the seller sees this transaction, he releases the goods to the buyer. Meanwhile the buyer/attacker, after getting the goods, now propagates this same block to the network which gets mined on but the reward of this block goes directly to the buyer instead of the legitimate seller of the goods. The seller ends up receiving no payment for goods sold and attacker escapes double spending the same cryptocurrency.

Vector76 Attack

The vector76 attack is a combination of both the race and Finney attack described earlier. In a vector76 attack, the dishonest miner will mine a block privately without propagating to the mining pool. Immediately after this, the dishonest miner will send a block to the seller in the form of payment and release the privately mined block right afterwards. Because the privately mined block has already been verified, this gets accepted in the network and the previous block sent to the seller is discarded. This is also called a one-confirmation attack (Rathod & Motwani, 2018).

Alternative History Attack

In the alternative history attack, the dishonest miner requires a high degree of hash-rate or computational capacity and the readiness to absorb a high risk of experiencing a high risk of expenses in wasted resources. The attacker/dishonest miner starts a transaction to pay a seller in the form of cryptocurrency, so this is propagated in the public mining pool, and the seller releases the goods to the buyer. Here, sellers require multiple numbers of confirmation of the valid blocks of cryptocurrency hence attackers tend to conceal a good number of blocks in their private fork. The target is to privately mine as many blocks as possible that can either match or exceed the blocks currently in the mining pool. Should the private fork match the public pool, the attacker publishes this private fork and hopes that the private fork shows quick latency for the honest miners to mine on top of the attacker's fork which is engineered to pay the reward back to the attacker. If the private fork, now published, exceeds the originally propagated fork, the honest miners shift their attention to the long new fork and the original gets discarded, meaning the seller would not get the reward of payment, but the attacker retains his coins. However, in the event the private fork concealed by the attacker does not match up or exceed the public fork, the attacker would have to discard the private cost and bear the cost of wasting resources in mining the blocks with no end reward.

Balance Attack

The balance attack in blockchains occurs when there are multiple mining subgroups with same hash power or computational power in question (Conti et al.,

2018). In this attack, the dishonest miner / attacker first issues a transaction into one of the subgroups in the mining pool but does not contribute any mining power in there. This transaction could be a form of payment to a seller for goods. When the seller sees and verifies the transaction, the seller releases the goods to the buyer who is the attacker. The attacker then adds his hash power by mining in a second subgroup propagating the same block which he sent in a different mining subgroup having the same hash power as the current subgroup. There are no communications between the two subgroups so honest miners cannot identify this as an attempt to double spend because the dishonest miner adds his computational power to this new and second subgroup. The hash power of the group now exceeds that of the first subgroup. In this second subgroup, the attacker sends the block to be mined and rewards routed to himself. Because of the high hash power in this instance, the block gets mined faster, and rewards get sent to the attacker whereas this second action nullifies the first action carried out as transaction.

Network Threats

The nodes and individual miners collectively operate in an environment suitable for mining cryptocurrency blocks, called the blockchain network. This network has been identified to be vulnerable to some attacks which are explored subsequently.

Sybil Attack

The name Sybil was derived from a case of a woman called Sybil Dorsett who was treated for dissociative identity disorder or multiple identity disorder (Kaplan, 2021). A sybil attack is a security threat where a user/attacker creates multiple accounts or

nodes in the network of an online system. On the blockchain network, an attacker can create multiple nodes in the mining pool with the intention of capturing the majority of the hash rate or power of that pool. The attacker or dishonest miner then becomes extremely powerful to be able to control what blocks gets accepted or what fork gets mined on. Sybil attacks can also result in 51% attacks when the attacker becomes so powerful without any competition regarding the hash rate or computational power in that mining pool.

Distributed Denial of Service Attack (DDOS)

DDoS attacks comprise burdening a target system or server by sending multiple streams of data packets with the intention of reducing the efficiency of that network. Even though the blockchain network is decentralized in nature, making it difficult to some extent for attackers to carry out the DDoS attack, the handful of such scenarios that occur hits heavily on the target network. These attacks most often are triggered from disparate sources making it difficult to put out a specific measure to counter such attacks. The data packets sent in these attacks mix up with authentic ones which makes it hard to properly segregate what is an attack and what is not (Douligeris & Mitrokotsa, 2004). The DDoS attack could be carried out by Sybil attackers after cloning and creating multiple nodes on the network. Attackers outside of the target pool could also have some interest in this attack to waste the resources of the honest miners in the target pool.

Routing Attacks

In a research study conducted by Apostolaki et.al (2017), the routing attack was identified to be a security threat on the blockchain network. This involves dishonest Internet Service Providers (ISPs), who are third parties on the forwarding path of the blockchain process. These ISPs have the ability to snoop, decline, change, accept or even delay the timing of blocks on the network. A dishonest ISP can easily partition the entire network by separating the nodes to prevent communication between the groups and creating parallel mining pools which can in effect lead to Double Spending attacks. Miners or nodes in these parallel pools have no way of communicating and verifying transactions and blocks propagated in these respective pools. An ISP can send the same transaction to these multiple pools to retrieve the rewards using the double spending attack. Again, ISPs could also use the delay attack, also a subset of the routing attack, by doing away with the shorter and most efficient hops to get to the destination of blocks and transactions, meaning the target packets will have to travel longer paths to reach the destination. The goal of this attack on the blockchain is to slow the transmission of the blocks on the network.

Transaction Malleability Attack

In this attack on the blockchain, an attacker who poses as a party to whom cryptocurrency must be paid to, requests for a second transfer in lieu of he not receiving the original transaction. Here, the attacker changes the signature string, and this triggers the change in hash value that identifies with the transaction after the paying party sends the transaction. The recipient who is the attacker will then notify the payer

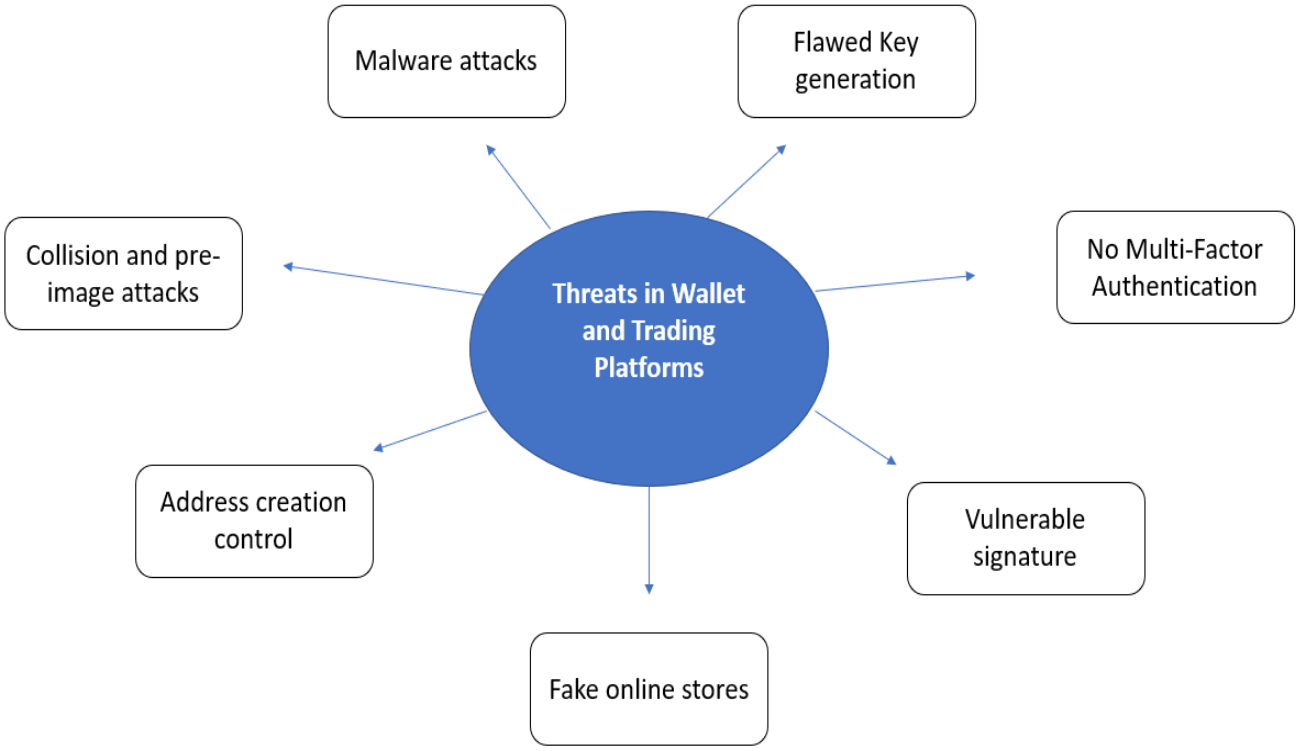
that the transaction failed so they should resend the transaction. This then leads to a double spend attack. The transaction malleability attacks happens when the attacker changes the transaction ID or hash value before the said transaction is confirmed.

Eclipse Attack

In an eclipse attack, a targeted node on the network is isolated and the attacker obscures its view to the other nodes on the network (Deshpande, 2022). After secluding this node, the attacker creates and populates the network with imposter nodes which communicate with this targeted and infected node. If this is a success, the attacker can now exploit the infected node for attacks on the network it was a part of. Another scheme employed by attackers in relation to the eclipse attack is to use a botnet which infuses into the target pool several attacker infected Internet Protocol (IP) addresses. These IP addresses are mapped to a target node which when restarted loses its authentic inbound and outbound connections and these connections are replaced by the attacker's IP addresses. Now the attacker will have the opportunity to falsely validate illegitimate transactions in the mining pool.

Figure 10

Taxonomy of vulnerabilities in wallet and trading platforms



Before Non-Fungible Tokens can be traded for, buyers and sellers ought to have some compatible cryptocurrencies wallets which hold their coins. Examples of cryptocurrency wallets out there include Coinbase, MetaMask, Binance, Robinhood among others. Trading Platforms also play integral roles in the NFT ecosystem. These platforms bring buyers and sellers of these cryptographically unique digital assets together. Examples of these trading platforms include OpenSea, Marketplace, Nifty Gateway, Rarible among others.

Flawed Key Generation

Users of cryptocurrencies use two sets of keys – public and private – to gain access to their coins and make successful transactions (Mosakheil, 2018). The public keys are of public knowledge, and these are accessed by other parties with whom the transaction will be made. The private keys are what need much protection as only the owner of the cryptocurrency has access to these. The private keys are usually stored by the wallets for transactions. The flawed key generation vulnerability identified on the blockchain is a result of faulty implementation of the associated hash function which encrypts the private keys. The flaw in the process exposes the private keys to attackers, and if these vulnerabilities are acted upon, a user could lose of their coins without any means of retrieving them.

Multi-Factor Authentication (MFA)

NFT trading platforms currently do not default to using any high level of authentication in their operations. In a quest to create a much user-friendly interface, most platforms compromise on the security aspect of the interface by using the single level of authentication which comprises the username/ID and password for authentication. As basic as this is, attackers can easily gain access if they chance on the password or even use some attacks such as dictionary attacks or brute force attacks in guessing the password. Nifty Gateway (a popular NFT trading platform) suffered an attack compromising the accounts of some users and selling the NFT they had in their accounts (Peters, 2021). Nifty Gateway later came out with a communique as to how and which accounts were compromised where they identified that these users did not have the 2

factor authentication enabled (Nifty Gateway, 2021). This platform among others do not provide several authentication layers as default unless enabled and this is a vulnerability. The best and most secure level of authentication, which is the MFA, is not employed by these platforms. The MFA adds a third and/or extra layers of authentication such as biometrics (Bhargav-Spantzel et al., 2006) making it extremely hard for attackers to identify and exploit any vulnerabilities.

Vulnerable Signature

Public and private keys play an integral role in cryptocurrency transactions to verify the authenticity of parties involved and do away with any third parties. Popular digital assets on the blockchain such as Bitcoin heavily rely on the Elliptical Curve Digital Signature Algorithm (ECDSA) which authenticates signatures and validates transactions (Sahoo et al., 2019). Per a study conducted by Bos et al., 2013), the ECDSA has a vulnerable property of poor randomness used in the signature generation process. The ECDSA, like DSA, all use random numbers in signature generation to make it nearly impossible for attackers to guess the correct number combinations of the signature. The study showed that the random numbers used in ECDSA are not consistently random and thereby could compromise the long-term key allowing attackers to steal coins of clients if the random numbers are repeated.

Fake Online Stores

As basic as this may appear, there are a lot of NFT owners who have fallen prey to attacks on fake online stores. Various NFT trading platforms have been cloned by attackers to lure potential traders on there just to extort their digital assets. These fake

online stores mimic the authentic ones but if closely investigated, users can identify the flaws and avoid such scam. A typical red flag users can always look out for will be the URL of the online store. NFT trading platforms all use the secured hypertext Transfer Protocol connection, but most of these fake ones just use the HTTP. Nonetheless, some infected or fake stores may still have the secured connection, but treaders need to be extra vigilant when signing up on any platform. If in doubt, always research into the history of the store to avoid being scammed.

Address Creation Control

Blockchain addresses are the hash values of the cryptographically encoded pair of private and public keys. These addresses dictate the source and destination of a blockchain transaction involving buyers and sellers. This public-private key pair helps in authenticating the linked accounts and ensuring one's funds are not falsefully spent by another (Astropay, 2022). The decentralized nature of the blockchain ecosystem however makes it nearly impossible to control the creation of addresses on the blockchain network. There is no central entity that regulates and guides the creation of these addresses. Despite the use of these addresses in transactions, users behind such addresses or the actual owners of the public-private key combination remains anonymous. The uncontrolled creation of addresses could be problematic as there is no regulatory body overseeing transactions in the network.

Collision and Preimage Attacks

Hash functions, which help in obscuring the actual contents of the blockchain addresses and play other imperative roles in the blockchain operations, have some

security conditions that they need to satisfy. These are the collision resistance and the pre-image resistance. Security Resistance as defined by (Knellwolf & Khovratovich, 2012) refers to " …*the of any specific technique that allows to find collisions, preimages, or second preimages faster than a generic algorithm."* The collision resistance property requires that it should be near to impossible or extremely difficult to find any two input variables that can be processed through hash functions to result in the same hash value. A collision attack therefore is a situation where the attacker tries all means to generate or find two inputs that can produce the same hash value through collision to bypass the authentication mechanism in the blockchain network. The preimage resistance property on the other hand requires that, given a target hash value, the input used to generate this hash value should not be able to be reverse engineered. Preimage attacks are instances where the adversary tries to reengineer the hashing process after figuring out the target hash value to generate the input used. The motive of that attacker here is also to compromise the security authentication system of the blockchain network.

Malware attacks

As security experts work round the clock finding solutions and ways of preventing attacks by hackers and other adversaries, so are these entities bent on finding and exploiting zero-day vulnerabilities in the software of cryptocurrency wallets. A malware as described by (Vasudevan & Yerraballi, 2006) is "…a generic term that encompasses viruses, trojans, spywares and other intrusive code." Attackers inject malware in the various stages of the run and build of cryptocurrency wallets. The motive of these

attackers is to retrieve the private keys through these malware injections. In 2018, Nano S Ledger, which is a cryptocurrency wallet, was identified to be attacked by malware (Rashid, 2018). This could potentially cost users to lose whopping sums of money in digital assets.

Table 4

Taxonomy of Vulnerabilities in Smart Contracts

#	**Vulnerability**	**Cause**
1	Gasless Send	Expensive fallback function of recipient
2	Exception Disorder	Inconsistencies in handling exceptions
3	Reentrancy	Reentrant function invoked at runtime
4	Timestamp Dependency	Liberty of miners in modifying timestamp
5	Block Number Dependency	Freedom of miners in manipulating block numbers
6	Dangerous Delegate Call	Dynamic code loaded from different address
7	Freezing Ether	Orphaned call function in contract

Smart Contracts in simple terms refers to legal contracts that have the capability of being translated into computer software code (Zou et al., 2021). NFTs are smart contracts based on the blockchain network. Smart contracts have some inherent and distinct vulnerabilities which could be exploited by attackers to nullify authenticity of transactions and retrieve the coins of legitimate owners. These vulnerabilities can be

said to be distinct to NFTs as well as compared to other cryptocurrencies on the blockchain. The vulnerabilities identified in Table 4 are discussed below.

Gasless Send

Smart contracts such as NFTs are created to run and be executed on an Ethereum based platform known as the Ethereum Virtual Machine (EVM). This environment for the runtime compilation of smart contract code has some resource limitations to keep in check the amount of load of work put on the environment. This is measured in gas as a unit measure for pricing transaction using Ether as mode of payment (Mosakheil, 2018). The gasless send vulnerability is the situation where an exception error is thrown because the transaction run out of gas. The limit of gas for a fallback function which has an amount sent greater than zero is 2300 (Jiang et al., 2018). In executing transactions in the EVM, the '*Send'* function is called which invokes the fallback function of the recipient of the transaction. Having the gas limit in the EVM in mind, if the fallback function of the recipient is very expensive exceeding the limit, the sender will get an exception error thrown that it run into an out of gas instance. Dishonest traders can take undue advantage of this exception if not checked as they will end up keeping ether supposed to be transferred.

Exception Disorders

During compilation of the smart contract code behind the transactions in the EVM, there are several occurrences of exception errors thrown. The problem of different ways of handling exceptions thrown becomes a vulnerability as the environment is not consistent in handling these exceptions (Bartoletti et al., 2016). In the case of a series of

calls nested together all calling directly to the function of the contract, if some calls are a success and others trigger exceptions, these irregularities may be skipped and not checked, and this vulnerability can be exploited by malicious users as some errors will go unnoticed. Other instances will also cause the entire nested call to be reverted, including the properly compiled calls rendering all gas lost.

Reentrancy

Most programmers of these smart contracts avoid including any recursive or looping actions in the code so they tend to believe the function invoked in run-time cannot be reentered. The reentrancy vulnerability in smart contracts occur because some malicious transactions can invoke their own fallback function in a reentrant manner without the consent and notice of the other party. This action burns gas and causes a lot of ether to be lost. An instance where this vulnerability was exploited was in “the DAO” attack in June 2016, resulting in about $US 60 million loss in Ether (Jiang et al., 2018).

Dependency on Timestamp

This vulnerability happens when the smart contract heavily depends on or uses the timestamp of the block in validating some conditions before functions such as the ‘Send’ function is called. On the blockchain, because of its trait as a distributed and decentralized system, miners have the liberty of setting the timestamp of the block. This implies that a dishonest miner equally has the freedom to manipulate the timestamp on the block which in effect alters the logic behind the smart contact operation leading to loss in Ether.

Dependency on Block Number

Just as the vulnerability identified in depending on the timestamp for validation for some critical conditions for the call of functions like the ‘Send’ function, depending on the block number also poses as a vulnerability because there are no restrictions on a miner’s ability to make modifications on the block number. Similarly, dishonest miners have the liberty to make such illegal manipulations to their benefit to cause huge sums of Ether to be lost in a transaction.

Dangerous Delegate Call

The dangerous delegate call is when a malicious contract contains a code that calls a function to a target address other than the authenticated address. This implies that during runtime a contract can load code dynamically from a different address while the storage points to the contract being called. An attacker can use this technique to cause a double-spend or reengineer Ether funds to their address without any proper checks in the code.

Freezing Ether

Another vulnerability in smart contracts is the freezing ether vulnerability which is a result of some smart contracts not having independent functions to send or receive ether on their own. These kinds of contracts depend on the code of other contracts using the delegate call to receive or send ether. There is a line of code in these contracts that when run, invokes the delegate call function triggering the action from another contract. This vulnerability comes to play when the second or referencing

contract performs a self-destruct operation on itself. It results in the ether sent by the other contract to be frozen or lost in transit.

What happens when the company / server hosting the blockchain encrypted web address that serves as a pointer to the NFT goes out of service? This presents another vulnerability associated with NFTs. In trading NFTs, buyers pay for a pointer to the digital asset and not necessarily the physical or actual asset itself. This implies that any compromise to the hosting agency's servers of that blockchain web address means the buyers or owners of the NFTs lose all their digital assets, potentially worth hundreds and millions of dollars.

Summary

This chapter outlined the data collected from the systematic survey and review of vulnerabilities identified on the blockchain and vulnerabilities that could be exploited as attacks in Non-Fungible Tokens. These vulnerabilities and attacks identified were explained and categorized in three taxonomies based on which digital asset and how they affect the related digital assets in this study. The next chapter presents the conclusions drawn from these identified and highlighted vulnerabilities and how attackers could potentially be restricted if not entirely prevented from exploiting these to become threats to the trading of Non-Fungible Tokens.

Chapter V: Results, Conclusion, and Recommendations

Introduction

This chapter concludes the survey study into the vulnerabilities associated with trading in Non-Fungible Tokens. In this chapter, some recommendations as to how users can further protect themselves from being vulnerable to the threats identified earlier are suggested. Some recommendations are also made for future researchers to explore in this field as a whole dimension of NFT security is yet to be deeply explored.

Results

This study highlighted the vulnerabilities that NFTs inherit from the blockchain as a result of being a digital asset that resides on the blockchain. NFTs simply are not immune to the vulnerabilities, threats and attacks that are known on the blockchain. NFTs again are traded for on some specific trading platforms who also have various associated vulnerabilities. The threats that result from exploiting vulnerabilities in the platforms for trading NFTs were identified and explained. Smart contract vulnerabilities were also examined in this study as these can be classified as NFT specific vulnerabilities in contrast to the other two categorizations identified earlier which can affect any digital asset on the blockchain. NFTs are smart contracts, implying they are vulnerable to all smart contract threats.

Conducting a systematic survey and review of literature and scholarly works were the backbone of the methodology employed in this study. Three taxonomies were developed providing a visual presentation of the vulnerabilities identified in the blockchain, vulnerabilities with trading platforms and vulnerabilities associated with

smart contracts. The paper answered the research study questions listed in the objectives of the study section as follows:

1. What have other researchers done in this area?
    - The works of other researchers were surveyed, and information was gathered giving in depth knowledge of the vulnerabilities known on the blockchain. Research on the security analysis of Non-Fungible Tokens however has not been heavily explored by the research society.
2. What are the existing and known vulnerabilities in blockchains?
    - This was answered using the second taxonomy which shows such vulnerabilities. These vulnerabilities were later explained in the Data collected section.
3. What are the new and emerging vulnerabilities that could be exploited as attacks on NFTs?
    - Taxonomy #4 answers this study question. The vulnerabilities identified were also later explained to provide more clarity.
4. What are the security and privacy issues related to NFT trading?
    - Threats and attacks on NFT trading platforms and wallets were also identified using Taxonomy #3. These were later explained in the Data Collection section of the study.
5. How can an individual protect themselves from these security and privacy issues?

- Some techniques to be used by users to protect themselves at a high level have been recommended in this results section of the study.

Users and traders of NFTs can better protect themselves if they are security and privacy conscious in all their online and sometimes offline engagements. As trivial as it may seem to this discussion, traders need to have as part of their security priorities, malware scanners on their host devices and any device on the network of their systems used in trading these NFTs. Malware can be a deadly tool for attack if not resisted. Traders are encouraged to first scan all devices for any possible malware application and install the current and original versions of the best anti-malware software available on the market.

Another recommendation for traders will be to use a Virtual Private Network (VPN) whenever connected to the internet and carrying out any NFT transactions. The anonymity of blockchain users, even though remains intact, does not guarantee that the packets of the trading activities over the network is not seen by anyone eavesdropping on the network. It is therefore very important to block any intruder or attacker from listening on any transactions that go on. VPNs form a sort of private tunnel for your personal use on the internet protecting your traffic and ensuring privacy on the internet.

Another recommended technique that could be used by traders is to switch from using hot wallets to using cold wallets. Hot wallets are the most common type of cryptocurrency wallets out there which can be used when only connected to the internet. This implies that hot wallets create private keys online and are stored on the

host computer. Should the host computer get compromised, the private keys become vulnerable to be retrieved by attackers to have access to all the digital assets associated with the account (Guri, 2018). On the other hand, cold wallets are offline based cryptocurrency wallets which come in the form of a USB device. The private keys are created and stored offline on this wallet. The cold wallets have extra embedded layers of security protocols to better protect the private key as compared to a trader who may not even have a malware detection or anti-malware software on their device.

Conclusion

This study was carried out to investigate security and privacy issues with trading and dealing with Non-Fungible Tokens (NFTs). These security issues were identified in three different categorizations which are the known vulnerabilities on the blockchain which NFTs are not immune to, the vulnerabilities and threats on the NFT trading platforms and in cryptocurrency wallets, and finally the vulnerabilities that are associated with smart contracts which NFTs are. The study has revealed a significant number of instances of vulnerabilities that could be exploited by attackers to gain undue advantage by flushing out the NFTs of target traders at given instances. Some high-level recommendations were also made for traders to protect themselves at the user endpoint.

In conclusion, this study was to help NFT traders and potential traders of this digital asset have an idea of what to protect themselves from and how to protect themselves. The content of the study was presented in its entirety.

Future Work

The security of Non-Fungible Tokens still remains a field yet to be fully explored. Future work and research should be targeted at such threats and potential attacks on smart contracts and how users / traders can better protect their valuable digital assets.

The security of encrypted web addresses, which serve as pointers to the NFTs on the blockchain, is a potential area of exploring in the NFT space. As companies who host these encrypted web addresses on their servers go out of business, what impact does this have on the NFTs of users and traders?

References

0xcert. (2018, July 2). Fungible vs non-fungible tokens on the blockchain. *0xcert*. https://medium.com/0xcert/fungible-vs-non-fungible-tokens-on-the-blockchain-ab4b12e0181a

Gomez, A. (2021). *Burning Your NFT: How to, Cost and Purpose*. Cyber Scrilla. https://cyberscrilla.com/burning-your-nft-how-to-cost-and-purpose/

Ante, L. (2021). The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3861106

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies (arXiv:1605.07524). *arXiv*. http://arxiv.org/abs/1605.07524

Astropay. (2022, March 8). *What is an address on a blockchain? What is a bitcoin address like?* https://www.astropay.com/what-is-an-address-on-a-blockchain-what-is-a-bitcoin-address-like/?lang=en

Ayson, S. (2021). *A complete guide to minting an NFT*. https://help.foundation.app/en/articles/4742869-a-complete-guide-to-minting-an-nft

Badev, A., & Chen, M. (2014). *Bitcoin: Technical Background and Data Analysis*. 39.

Bal, M., & Ner, C. (2019). NFTracer: A Non-Fungible Token Tracking Proof-of-Concept Using Hyperledger Fabric. *ArXiv:1905.04795 [Cs]*. http://arxiv.org/abs/1905.04795

Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2021). *A Decentralized Framework for Patents and Intellectual Property as NFT in Blockchain Networks* [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-951089/v1

Bartoletti, N. A., Massimo, & Cimoli, T. (2016). *A survey of attacks on Ethereum smart contracts*. https://eprint.iacr.org/undefined/undefined

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2006). *Privacy Preserving Multi-Factor Authentication with Biometrics*. Center for Education and Research in Information Assurance and Security Tech Report, 29.

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12*, 833. https://doi.org/10.1145/2382196.2382284

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. *ArXiv:1405.7418 [Cs]*. http://arxiv.org/abs/1405.7418

Bonderud, D. (2021, May 26). *Token Resistance: Tackling the New NFT Threat Landscape*. Security Intelligence. https://securityintelligence.com/articles/new-threat-landscape-nfts/

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2013). *Elliptic Curve Cryptography in Practice*. https://eprint.iacr.org/undefined/undefined

Bourcart, C. (2021, October 20). *Top 5 NFT Marketplaces for Creators to Sell Non-fungible Tokens in 2021*. Medium. https://medium.datadriveninvestor.com/top-5-nft-marketplaces-for-creators-to-sell-non-fungible-tokens-in-2021-73ee30b5bcd3

Brown, A. (2021, September 20). *The 9 Different Types of NFTs*. MUO. https://www.makeuseof.com/different-types-of-nfts/

Chang, S.-Y., & Park, Y. (2019). Silent Timestamping for Blockchain Mining Pool Security. *2019 International Conference on Computing, Networking and Communications (ICNC)*, 1–5. https://doi.org/10.1109/ICCNC.2019.8685563

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Cimpanu, C. (2021, June 16). *NFT creators tricked into installing malware in highly targeted attack.* The Record by Recorded Future. https://therecord.media/nft-creators-tricked-into-installing-malware-in-highly-targeted-attack/

Cisco. (2021). *What is Malware? - Definition and Examples*. Cisco. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

Conti, M., E, S. K., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Deshpande, P. (2022, April 1). *Explained: Eclipse attacks on blockchains and how to stop them*. Cnbctv18.Com. https://www.cnbctv18.com/cryptocurrency/explained-eclipse-attacks-on-blockchains-and-how-to-stop-them-13020692.htm

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666. https://doi.org/10.1016/j.comnet.2003.10.003

Dowling, M. (2021). Fertile LAND: Pricing non-fungible tokens*. Finance Research Letters, volume 44*(102096). https://doi.org/10.1016/j.frl.2021.102096

Farell, R. (2015). *An Analysis of the Cryptocurrency Industry* (Publication No.130) [Undergraduate thesis, University of Pennsylvania]. Wharton Research Scholars.

Febrero, P. (2019, May 17). *A guide to Ethereum's ERC standards*. https://www.yahoo.com/now/guide-ethereum-erc-standards-150024381.html

Frankenfield, J. (2022, January 7). *Understanding Double-Spending and How to Prevent Attacks*. Investopedia. https://www.investopedia.com/terms/d/doublespending.asp

F-Secure. (2021). *Article: What is... Denial-of-Service (DoS).* F-Secure. https://www.f-secure.com/v-descs/articles/denial-of-service.shtml

Garfinkel, S. L. (2015). *De-identification of personal information* (NIST IR 8053; p. NIST IR 8053). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8053

Garimella, A. (2021, March 31). *NFT Scams Part 1: 5 NFT Scams you need to know*. Bolster Blog. https://bolster.ai/blog/5-nft-scams-you-need-to-know/

Groenewald, T. (2010, April 4). *Taxonomy of research*. Qualitative Inquiry Growth. https://www.psychsoma.co.za/qualitative_inquiry_growt/2010/04/taxonomy-of-research.html

Guri, M. (2018). BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1308–1316. https://doi.org/10.1109/Cybermatics_2018.2018.00227

Iacurci, G. (2021, July 23). *13% of Americans traded crypto in the past year, survey finds*. CNBC. https://www.cnbc.com/2021/07/23/13percent-of-americans-traded-crypto-in-the-past-year-survey-finds.html

Jiang, B., Liu, Y., & Chan, W. K. (2018). ContractFuzzer: Fuzzing smart contracts for vulnerability detection. *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, 259–269. https://doi.org/10.1145/3238147.3238177

Kaplan, R. M. (2021). Rowing back into the past—A review of Sybil Exposed by Debbie Nathan. *Academia Letters*. https://doi.org/10.20935/AL2842

Kastrenakes, J. (2021, March 11). *Beeple sold an NFT for $69 million*. The Verge. https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million

Kaur, R., & Kaur, A. (2012). Digital Signature. *2012 International Conference on Computing Sciences*, 295–301. https://doi.org/10.1109/ICCS.2012.25

Kinsella, E. (2021, March 11). *An NFT Artwork by Beeple Just Sold for $69 Million at Christie's—Making Him the Third Most Expensive Living Artist at Auction*. Artnet News. https://news.artnet.com/market/christies-nft-beeple-69-million-1951036

Knellwolf, S., & Khovratovich, D. (2012). New Preimage Attacks against Reduced SHA-1. In R. Safavi-Naini & R. Canetti (Eds.), *Advances in Cryptology – CRYPTO 2012* (Vol. 7417, pp. 367–383). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32009-5_22

Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018). MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1714–1730. https://doi.org/10.1145/3243734.3243858

Liao, X., Yin, J., Chen, M., & Qin, Z. (2020). Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/TDSC.2020.3004708

Liscia, V. D. (2021, March 16). *Reports of Stolen Art on NFT Marketplace Raise Issues for Crypto Collectors*. Hyperallergic. http://hyperallergic.com/629328/reports-of-stolen-art-on-nft-marketplace-raise-issues-for-crypto-collectors/

Liu, S., & Cheng, B. (2009). Cyberattacks: Why, What, Who, and How. *IT Professional*, *11*(3), 14–21. https://doi.org/10.1109/MITP.2009.46

Lucker, N. (2021, October 19). *What is the biggest NFT marketplace? A top 10 comparison*. Blockdata. https://www.blockdata.tech/blog/general/what-is-the-biggest-nft-marketplace-a-top-10-comparison

Market History: NFT sales and trends. (2021). NonFungible. https://nonfungible.com/market/history

Maxwell, J. A. (2008). *Qualitative Research Design*. Sage Publications, 40.

More Than One in Ten Americans Surveyed Invest in Cryptocurrencies. NORC.org. (2021, July 22). Norc. https://www.norc.org/NewsEventsPublications/PressReleases/Pages/more-than-one-in-ten-americans-surveyed-invest-in-cryptocurrencies.aspx

Mosakheil, J. H. (2018). *Security Threats Classification in Blockchains* (Publication No.142) [Master's thesis, St. Cloud State University]. The Repository at St. Cloud State.

MuleSoft. (2021). *What is an API? (Application Programming Interface)*. MuleSoft. https://www.mulesoft.com/resources/api/what-is-an-api

Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the NFT revolution: Market trends, trade networks, and visual features. *Scientific Reports*, *11*(1), 20902. https://doi.org/10.1038/s41598-021-00053-8

NFT Scams Part 1: 5 NFT Scams you need to know. (2021, March 31). Bolster Blog. https://bolster.ai/blog/5-nft-scams-you-need-to-know/

NFT's and their legal implications. (2021, May 31). LawMiracle. https://www.thelawmiracle.com/commercial-awareness-articles/coporate-lawyer/nfts-and-their-legal-implications

Nifty Gateway. (2021, March 15). *Please see our statement below on reports circulating around security concerns on Nifty Gateway* [Tweet]. Twitter. https://twitter.com/niftygateway/status/1371479363036778503

Node (cryptocurrency network)—Definition and examples. (2021). *Market Business News*. https://marketbusinessnews.com/financial-glossary/node-cryptocurrency-network/

Norvill, R., Fiz, B., State, R., & Cullen, A. (2019). Standardising smart contracts: Automatically inferring ERC standards. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 192–195. https://doi.org/10.1109/BLOC.2019.8751350

Ober, M., Katzenbeisser, S., & Hamacher, K. (2013). Structure and Anonymity of the Bitcoin Transaction Graph. *Future Internet*, *5*(2), Article 2. https://doi.org/10.3390/fi5020237

Peer-2-Peer Networking. (2018, July 25). Cybersecurity. https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/peer-2-peer-networking

Peters, J. (2021, March 15). *Hackers stole NFTs from Nifty Gateway users*. The Verge. https://www.theverge.com/2021/3/15/22331818/nifty-gateway-hack-steal-nfts-credit-card

Powers, B. (2021, March 9). *A Hacker Was Selling a Zero-Day Exploit As an NFT.* CoinDesk. https://www.coindesk.com

Raiyn, J. (2014). A survey of Cyber Attack Detection Strategies. *International Journal of Security and Its Applications*, *8*, 247–256. https://doi.org/10.14257/ijsia.2014.8.1.23

Rashid, S. (2018, March 20). *Breaking the Ledger Security Model*. Saleem Rashid. https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/

Rathod, N., & Motwani, D. (2018). Security threats on Blockchain and its countermeasures, *International Research Journal of Engineering and Technology*, *5*(11), 8.

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). *A Usability Study of Five Two-Factor Authentication Methods*, 15.

Rosenfeld, M. (2011). Analysis of Bitcoin Pooled Mining Reward Systems (arXiv:1112.4980). *arXiv*. http://arxiv.org/abs/1112.4980

Rossolillo, N. (2021, November 2). *10 Top NFT Marketplaces*. The Motley Fool. https://www.fool.com/investing/stock-market/market-sectors/financials/non-fungible-tokens/nft-marketplaces/

Sahoo, M., Samanta Singhar, S., Nayak, B., & Mohanta, B. (2019). A Blockchain Based Framework Secured by ECDSA to Curb Drug Counterfeiting. *2019 10th International Conference on Computing, Communication and Networking Technologies*, 6. https://doi.org/10.1109/ICCCNT45670.2019.8944772

Steinwold, A. (2019, October 7). The History of Non-Fungible Tokens (NFTs). *Medium*. https://medium.com/@Andrew.Steinwold/the-history-of-non-fungible-tokens-nfts-f362ca57ae10

Tikhomirov, S. (2018). Ethereum: State of Knowledge and Research Perspectives. In A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, & J. Garcia-Alfaro (Eds.), *Foundations and Practice of Security* (Vol. 10723, pp. 206–221). Springer International Publishing. https://doi.org/10.1007/978-3-319-75650-9_14

Vasudevan, A., & Yerraballi, R. (2006). SPiKE: Engineering Malware Analysis Tools using Unobtrusive Binary-Instrumentation, *ACSC '06: Proceedings of the 29th Australasian Computer Science Conference*, *48*, 10.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. *ArXiv:2105.07447 [Cs]*. http://arxiv.org/abs/2105.07447

Zou, W., Lo, D., Kochhar, P. S., Le, X.-B. D., Xia, X., Feng, Y., Chen, Z., & Xu, B. (2021). Smart Contract Development: Challenges and Opportunities. *IEEE Transactions on Software Engineering*, *47*(10), 2084–2106. https://doi.org/10.1109/TSE.2019.2942301