Risk assessment of digital assets – insurance applications in crypto and NFTs

Roberto Delgado Ferrezuelo
`ro3187de-s@student.lu.se`

Trygg-Hansa
Lund University

Academic supervisor: Paul Stankovski Wagner

Industry supervisors: Fredrik Thuring and Erik Rasmusson

Examiner: Erik Larsson

May 17, 2023

Printed in Sweden
Tryckeriet i E-huset, Lund

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Acknowledgements

Popular Science Summary

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed

vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Table of Contents

List of Figures

List of Tables

Chapter 1
Introduction

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1.1 Background and motivation

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

$$A = \sum_{i=0}^{\infty} \beta\alpha^i = \frac{\beta}{1-\alpha}, \quad |\alpha| < 1$$

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

1.2 Aim and scope

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

1.3 Methodology

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Chapter 2

Web3

The World Wide Web has evolved since its inception, going through different stages. The first iteration, coined as the "Web 1.0" by Tim Berners-Lee in 1989, consisted of static websites owned by companies that provided a better access to information for users, but it lacked of interactivity.

In the second iteration or, "Web 2.0", there is a shift towards a more participatory network in which bidirectional communication flows are established, leaving behind the "push model" used in the Web 1.0. One of the main features of the Web 2.0 is the social networking, which allowed people from different parts of the world to be connected. The main problem of this iteration is the dependency generated in users that rely in centralized entities to act honestly as they have control over most of the internet infrastructure and users data.

The third iteration of the Web, coined as "Web 3.0" or "Web3" by the Ethereum co-founder Gavin Wood put a solution to this problem by using technologies such as the blockchain, distributing access to the network in a more equitable manner. According to the Ethereum description [1], the core principles that characterize this Web are decentralization, permissionless, native payments and trustless. This iteration is still being defined and it can also be explained from the machine-readability perspective where data is represented in a way such that it can be processed by machines.

As the twitter post in [2] says, the three stages are generally described as: "Web 1: Read, Web 2: Read-Write, Web 3: Read-Write-Own". Figure 2.1 provides a visual representation of the different iterations.

2.1 Blockchain

Blockchain is one of the underlying technologies that powers Web3, eliminating users' dependence on large corporations acting as intermediaries. The speaker in [3] describes it as the technology that enables a shift from the "Internet of information" to an "Internet of value", a democratized version where the asymmetry derived from the majority control of the global infrastructure by these authorities is reduced.

This concept was first implemented in 2008, when the whitepaper in [4] was published by an anonymous person or group of persons under the pseudonym Satoshi Nakamoto, which introduced to a new peer to peer electronic cash system

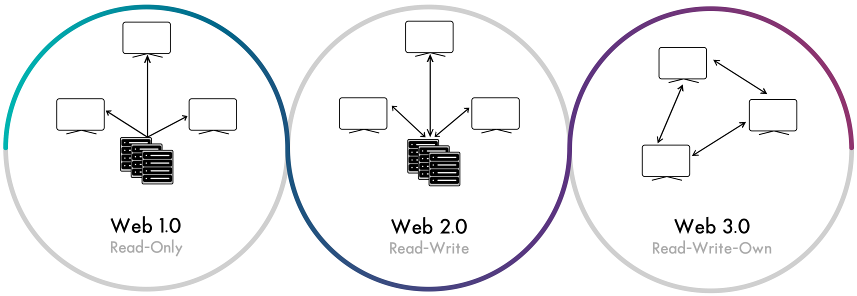


Figure 2.1: World Wide Web iterations

called Bitcoin. Blockchain is the technology behind Bitcoin and it can be described as an immutable distributed ledger where transactions are anonymously recorded. The anonymity is achieved by using public-key cryptography to generate a key pair that identifies the participants. The keys are stored in wallets and they can be non-deterministic, when private keys are generated randomly, or deterministic, which are commonly generated using the standards introduced in Bitcoin Improvement Proposals (BIPs) 39, 32 and 44 [6, 7, 8]. Public keys are derived from the private key using a cryptographic hash function such as the Elliptic Curve Digital Signature Algorithm. The public key is later hashed to create the public address. The private key is used to sign transactions, proving ownership of the assets being transferred, therefore it is kept in a secure location, while the public address is shared with the rest of the participants in the network so that they can send transactions to the wallet associated with the private key.

There are different blockchains and each of them is run by computers provided by volunteers around the world which are called nodes, each of these nodes has a copy of the ledger and for a transaction to be validated they have to agree based on a set of rules. A combination of cryptography and game theory is applied to avoid what is called the Byzantine Generals Problem [5], a dilemma in which isolated participants have to agree in a common decision but there is no guarantee that they will act on the group's best interest. Using consensus algorithms it is possible to create a Byzantine fault-tolerant system, a system in which trust among participants is not necessary, since it is in their own interest to act for the benefit of the group. There are different algorithms, but the most widely used are Proof of Work (PoW) and Proof of Stake (PoS). Typically, blockchains have a native currency that is used by these algorithms to incentivize participants to maintain the security and integrity of the network.

To send a transaction, users need to sign a digital message using their private key with the recipient's public address as the payee. The transaction is then broadcasted to the network of nodes who verify its validity and bundle it with other transactions into a block. Each block includes a header with information such as the timestamp, a reference to the previous block (thus forming a chain), the Merkle root, which is a hash of all transaction's hashes included in the block, and other parameters that can vary in the different blockchains.

2.1.1 Consensus algorithms

PoW concept was first implemented in Bitcoin, it consists on a competition among a group of nodes, that are called miners, in finding a solution to a complex mathematical problem where the first in solving it is financially incentivized, reaching in this way a consensus on the state of the network and preventing what is called the double-spending, when a user tries to spend the same asset twice.

To find a solution to the problem, miners need to find a value, the nonce, that when hashed together with the rest of the components of the block's header, the resulting hash is below a certain target value that is dynamically set based on the total computational power of the network, whoever finds this value has to broadcast it to the rest of the nodes and, if accepted, he receives newly generated coins, also called minted coins. This hash serves as a unique identifier of the block and this value will be used as input in the next block to find the new solution, thus linking the blocks with each other and making it very difficult to manipulate a block as it would imply redoing all the subsequent work. Users willing to participate in the competition need to provide vast amounts of electricity and computational resources, also called the "stake" according to [9]. The stake discourages miners to act dishonestly as they would need to control the majority of the network, what is called the 51% attack, something that is highly expensive as the size of the networks continue to increase, making it the most cost-effective option to act according to the established rules. One of the main problems of the PoW mechanism is the high energy consumption, with most of the energy sourced from fossil fuels. At the time of writing, the Bitcoin Energy Consumption Index in [10] shows an annual carbon footprint of 52.10 Mt CO2. There are different alternatives for this algorithm that can considerably reduce the environmental impact, the most widespread solution is PoS.

In PoS, there are validators instead of miners and blocks are said to be forged or minted. To participate in the PoS validation process, nodes lock up a required amount of cryptocurrency in a wallet as a stake. An algorithm determines the next validator from a pool of candidates based on a number of considerations such as the node's hash value, which, according to the post in [11] is usually calculated by signing some network-related parameter using the private key, the amount of coins staked or the number of days the coins have been staked. Once the node is selected, it validates the transactions to be included in the block and adds it to the blockchain, receiving a share of the block's transaction fees as a reward (no coins are minted in PoS). If the network nodes detect a fraudulent transaction in one of the blocks, the validator who forged that block can be penalized loosing some of the cryptocurrency staked (higher than the transaction fees), also known as "slashing" or "burn" [12]. The 51% attack is highly impractical as it would imply to take control of the majority of the staked tokens which can be really expensive, for example, in the Ethereum network it would imply spending more than $110 billions, and even so, according to [13], the community can still use social recovery to restore the original state of the network.

Since the reward in the PoS mechanism is proportional to the amount of tokens staked, validators cannot benefit from economies of scale unlike it happens in PoW, where miners group together to form pools. It can be seen in Figure 2.2 how a few mining pools have control over a big part of the Bitcoin network. The absence of such economies of scale and the lowering of the entry barriers, since there is no need to acquire expensive specialized equipment to participate in the validation, reduce the centralization risk. Moreover, as nodes are not competing to find the next block, one of the main benefits it brings to society is the energy saving. The Ethereum webpage in [15] shows a 99.988% reduction in the energy consumption since the Gasper (name of their PoS mechanism) implementation. However, it also has some setbacks, such as the possibility of validators forming oligopolies or the problem known as "nothing to stake". When new forks of the blockchain appear, the most profitable option for validators is to work on all of them as they do not incur additional costs, maintaining all these multiple versions can lead to vulnerabilities such as the double-spending attack mentioned above.

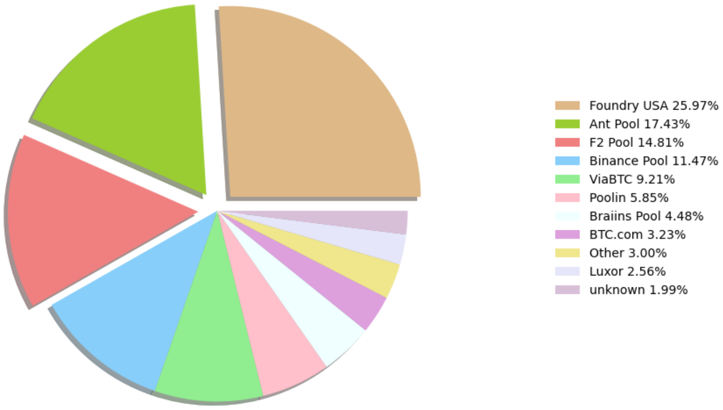


Figure 2.2: Hash rate distribution in Bitcoin network, Mar. 2022-Feb. 2023. Data source: [14]

.

2.1.2 Private and Public blockchains

Although the idea that fueled the growth and adoption of the blockchain technology is the elimination of the dependence on middlemen, the concept of private blockchain is starting to become widely adopted. Private blockchains do not align with the permissionless principle, leading to some reluctance from members of the public who view it as a fundamental characteristic, instead, the right to modify and add new entries into the ledger is reserved for only a few participants chosen by the entity running the network. The utilization of such blockchains has the potential to enhance the efficiency of antiquated processes in industries where the absence of competitiveness has hindered investment in process improvement, thereby enabling streamlining and optimization, Vitalik Buterin in [16] provides some interesting scenarios where it could be used as well as the advantages it could bring to society, he also acknowledges the potential setbacks, such as public distrust and possible coercion.

There is another solution that lies between the two options discussed so far, namely consortium blockchains. Here, the permissions to read and write in the ledger are restricted to a set of nodes instead of a single organization. Big insurance companies such as Allianz are adapting their processes using this type of blockchain-based solutions to settle faster and more efficiently international motor insurance claims. In the podcast in [17], Bob Crozier, Allianz's current Interim Chief Data Officer explains how the company is using the modular blockchain framework developed by the Linux Foundation, Hyperledger Fabric, to improve the intercompany billing process, from claim creation to settle status involving its different Europe's subsidiaries. By using a consortium blockchain they significantly cut down their frictional costs as well as the time required in the claim processing while keeping the deterministic finality (the time it takes for a transaction to be added to the blockchain, thus becoming irreversible), as opposed to the probabilistic nature of the permissionless blockchains for which it has been necessary to develop new solutions that allow the creation of more scalable networks such as the use of rollups in a separate layer in Ethereum. Rollups bundle many transactions and submit them back to the main network, distributing fees among all participants while also increasing finality without sacrificing security or decentralization, as outlined in [18]. Transactions data regarding the claims reside in the blockchain while personal information about the clients is placed in a separate relational database guaranteeing their confidentiality.

2.1.3 Smart contracts

As previously explained, the key pair in a blockchain is stored in wallets, not the native currency itself and it is the private key what give access to the funds which reside inside the blockchain. The way funds are stored vary across the different networks, for instance, Bitcoin utilizes Unspent Transaction Outputs (UTXOs), while Ethereum employs account balances to keep track of cryptocurrency holdings.

There are different ownership mechanisms to regulate the assets spending, apart from public keys, they can be owned by scripts specifying a set of conditions under which they can be accessed. Ethereum developed a low-level bytecode language, Ethereum Virtual Machine (EVM), which builds on and extends the capabilities of Bitcoin's scripting language. According to the Ethereum whitepaper in [19], the EVM adds Turing-completeness, value-awareness, blockchain-awareness, and state, thereby completing Bitcoin's programming language.

One of the most important features implemented using these added functionalities were the smart contracts. On Ethereum, smart contracts are distinct from Externally Owned Accounts (EOAs) in that they are governed by a piece of code rather than a private key. Smart contracts can interact with each other as well as with EOAs by encoding messages with the associated address as the receiving party of the transaction. They use the data contained in the message as input and translate it into opcodes, each of which corresponds to a specific action EVM can perform. The amount of gas consumed during the execution of these actions varies depending on the complexity of the task. To cover the computational effort required for each action, a dynamic price must be paid for each unit of gas consumed. This price varies according to the current network congestion, meaning that during times of high demand, the cost of gas will increase to incentivize miners to prioritize transactions with higher gas prices, ensuring the stability of the network. Smart contracts are written in high-level programming languages such as Solidity or Vyper and deployed in the network paying the corresponding fees. When called, they are compiled into bytecode that can be executed by the EVM, determining the state transition of the network based on the logic programmed into the smart contract. According to [20], Ethereum can be viewed as distributed state machine governed by the rules defined by the EVM instead of a distributed ledger.

Smart contracts are the base of the assets for which the policy framework is being developed. They also bring many exciting opportunities to the insurance industry by enabling a shift from the traditional business processes to a new value chain where most of the manual tasks can be automated achieving faster and more accurate results, some of the main benefits and examples of the current insurance landscape will be provided in a later section.

2.2 NFTs

NFT stands for Non-Fungible Token and unlike cryptocurrencies like Bitcoin or Ethereum, they can not be swapped for each other as their value is unique. They rely on smart contracts to create a tamper-proof record of ownership and link users to the specific asset they possess. First, an overview of their history will be provided, using the article in [21] as a reference for the chronology of events.

The emergence of the initial idea behind NFTs came a long time ago with the publication of the paper in [22] by Meni Rosenfeld in 2012. This paper discusses the idea of adding metadata to Bitcoin transactions creating a system by which coins can be traced back to their genesis state allowing a distinction to be made depending on the history of transactions associated with them. Limitations in the Bitcoin scripting language posed a challenge to their development which spurred the creation of more flexible platforms with advance features that allow the implementation of complex asset management functionalities.

In 2014, the artist Kevin McCoy partnered with the entrepreneur Anil Dash, aiming to find a solution to the problem of provenance in digital art, the partnership resulted in what is considered to be the first ever created NFT, Quantum [23]. After delving into the potential of blockchain technology, the duo opted to utilize the Namecoin network, one of the earliest forks of Bitcoin, to deploy the artwork. After years since its deployment and with the increasing popularity of NFTs, the artist made some promotional efforts for the artwork, and eventually, Quantum was sold for a whopping $1.47 million in a Sotheby's auction.

Namecoin was initially developed to extend the functionality of the Bitcoin network by enabling data storage, leading to the creation of decentralized services such as a domain name system. However, the network's unique features caused a surge of legal issues following Quantum's auction. It requires users to periodically create new transactions to update the encoded output with the asset's associated data to prevent it from expiring, something did not happen with Quantum as it can be seen in [24], where the output has not yet been redeemed. After the renewal period expired, another user claimed ownership rights of Quantum and filed a lawsuit against the artist, asserting that he was the rightful owner of the artwork. However, the lawsuit was recently dismissed by a federal judge in New York [25] who determined that the plaintiff was in possession of a different NFT since Quantum was later minted (similar to cryptocurrencies, NFTs can be minted and burned) on the Ethereum network [26].

Following the mint of Quantum, a first concept of platforms that allowed the creation of digital assets started to appear. 2016 was a significant year for the internet of memes, among which Pepe the Frog stands out. It is a creation of the artist Matt Furie and despite its notorious association with the alt-right movement, it played a pivotal role in the development of the NFTs. Creators started to mint variations of the meme on the Counterparty platform, a protocol running on top of Bitcoin that allowed users to trade digital tokens, thus becoming the first examples of digital assets being traded and valued as a unique, collectible item. Since Bitcoin was not tailored to that specific purpose, new alternatives began to emerge, Ethereum being one of the most prominent.

The shift to Ethereum and subsequent boom in the market started with the project known as CryptoPunks, created by the software developers Matt Hall and John Watkinson in 2017. It consists on a collection of 10.000 unique pixelated AI-generated images each of them with different traits. They used the smart contracts capabilities to create a code that allowed the buy and sell of the different punks among the network participants. There exists two different versions of the collection, the original, also referred to as V1 CryptoPunks, was released on 9 June 2017, it had some flaws in the code that allowed buyers to get back the money they paid for the tokens, meaning that the seller did not get any ether (native currency of the Ethereum network) for the sale. Therefore it was decided to create a new contract where the bugs were removed, the V2 Punks, and airdrop (term commonly used to to refer to the distribution of free NFTs to a group of people) them to the original claimants.

Similar to the BIPs, Ethereum has its own Ethereum Improvement Proposals (EIPs). Those submissions proposing a change related to the token ecosystem can become an Ethereum Request for Comment (ERC) if accepted by the community. ERCs provide a consistent interface for tokens, and the creation of CryptoPunks laid the groundwork for the now widely adopted ERC-721 standard, which has become the de facto standard for NFTs.

2.2.1 ERC-721 standard

As stated in the Larvalabs (company founded by Hall and Watkinson) webpage in [27], the tokens did not fully conform to any existing standards, although they closely resembled an ERC-20 compliant token. They added some extra functionalities to enable the buy and sell of the tokens and created their own marketplace.

The ERC-721 standard, authored by William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs, offers users a smart contract template that enhances network interoperability through a common interface that developers can adapt to their unique requirements. The specifications for this standard can be found in a Github repository in [28]. It is inspired by the ERC-20 standard, which was the first implemented standard, and it addresses some of its limitations, introducing a more complex interface that includes functions for creating, transferring, and querying unique tokens. The pair `(contract address, uint256 tokenId)` serves as a unique identifier for each token in a collection. The `contract address` refers to the smart contract where the collection is deployed, while the `tokenId` variable denotes the unique identifier of the item within the collection. Some of the common and most important functions typically included in ERC-721 smart contracts are the following:

1. `ownerOf(uint256 _tokenId)` - returns the owner of an NFT.
2. `balanceOf(address _owner)` - amount of tokens held by an owner.
3. `safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data)` - transfers the NFT only when called by the owner, an authorized operator or approved address and confirms that the address `_to` is capable of receiving the token.
4. `transferFrom(address _from, address _to, uint256 _tokenId)` - transfers the token, but the user is responsible for checking that the address `_to` is capable of receiving the token.
5. `approve(address _approved, uint256 _tokenId)` - approves another address to transfer the given token ID.
6. `setApprovalForAll(address _operator, bool _approved)` - sets or unsets the approval of a given operator to manage all the message sender's assets.
7. `getApproved(uint256 _tokenId)` - gets the approved address for a token ID, or zero if no address is set.
8. `isApprovedForAll(address _owner, address _operator)` - checks whether an operator is approved by a given owner.
9. `tokenURI(uint256 _tokenId)` - returns the URI with the token's metadata for a given ID.

In recent years, the Enjin development team, creators of a blockchain-based platform for gaming, have been working on an enhanced token standard known as ERC-1155. This standard builds upon the previous ERC-20 and ERC-721 standards, allowing for the creation of semi-fungible assets (SFTs), assets which possess some of the unique characteristics of NFTs, while also offering a degree of interchangeability.. Although the ERC-721 standard remains the most widely adopted option, the ERC-1155 standard provides several benefits in terms of scalability and space efficiency. Unlike ERC-721 contracts, which require a separate contract for each type of asset, ERC-1155 contracts enable multiple token IDs, each representing a distinct asset type, to be stored in the same contract. This reduces the amount of space required to store information on the network. Furthermore, it allows for batch transfers, where multiple items can be transferred simultaneously, improving the network scalability by reducing congestion and fees.

2.2.2 NFT Metadata Storage

An important aspect of the NFTs, sometimes misunderstood is the difference between the actual token and the media file to which the token is referencing. Retaking the previous explanation of CryptoPunks, its creators embedded a hash of the composite image with all the punks [29] in the smart contract code, allowing users to verify the authenticity of the tokens being bought. It existed some controversy around the index corresponding to each token in the composite image as it was not specified how they are sorted, from top to bottom, left to right..., to clarify it they published in their webpage a separate image of each token with the corresponding ID, however this meant that Larvalabs had the control over which index belonged to each asset and, as in many other scenarios in the crypto space, centralization is not universally embraced by users. In 2021, a Twitter post [30] announced that they decided to move the images and attributes on-chain, something that is not always feasible due to size limitations as it will now be explained. This example illustrates the distinction between the content being acquired and the token stored in the blockchain. In this case, the content is a 24 x 24 pixel image that is part of a larger composite image of 2400 x 2400 pixels. On the other hand, the token is a record stored in the blockchain that proves ownership of a specific item in the collection, identified by its unique ID.

There are various alternatives available for storing NFT metadata, but concerns have arisen about the safety of these solutions and their potential impact on market consolidation. Moxie Marlinspike, Signal founder, posted an article in [31], criticizing some of the aspects of NFTs which raised again a concern that has been existing in the space for a long time. He discussed how many of the top NFT collections store the metadata and the media file using centralized servers which can be easily accessible, allowing users to change the NFT's description, image, title, etc. Marlinspike went further and created his own NFT that displayed a different image depending on the IP or User Agent of the requester. This experiment highlighted the low credibility of collections that use centralized storage solutions. Additionally, he pointed out how his NFT was delisted from major marketplaces for an alleged "violation of some Terms Of Service" with the NFT automatically disappearing from his Metamask wallet due to its high dependence on APIs provided by large entities operating in the space, one of which was the marketplace that delisted his token.

These issues underscore the need for better solutions for storing NFT metadata that prioritize decentralization, security, and independence from centralized marketplaces. While centralized solutions may be more convenient, they come with significant risks, including potential loss of control and censorship. During these years there have been many improvements aiming to seek a solution for these concerns, the article in [32] provides a deep understanding on two classifications schemes based on how the NFT data is stored and its practical implications. In terms of risk management, the technical scheme takes precedence over practical considerations since it emphasizes specific details.

This classification scheme, also referred to as the "Michelin guide" in the Dom Hoffman's Twitter post in [33], categorizes NFTs on the Ethereum network into four groups and assigns a score to each. The lowest score is given to NFTs whose smart contract returns a URI pointing to off-chain resources, which is the most common setup. Within this category, NFTs can be further divided into two groups based on whether the resources are stored in a centralized server or a decentralized file storage system. Figure 2.3 illustrates how a random user purchasing an NFT in this category can access the data. To purchase the token, the user sends the required number of coins to the smart contract address of the collection, with the token's unique ID determining its price. After the transaction is confirmed, a record is created with the user's address as the owner of the newly acquired token. The smart contract usually contains a link to a JSON file, accessible through the `tokenURI` function, that provides details on the token's attributes and points to the location of the media file.

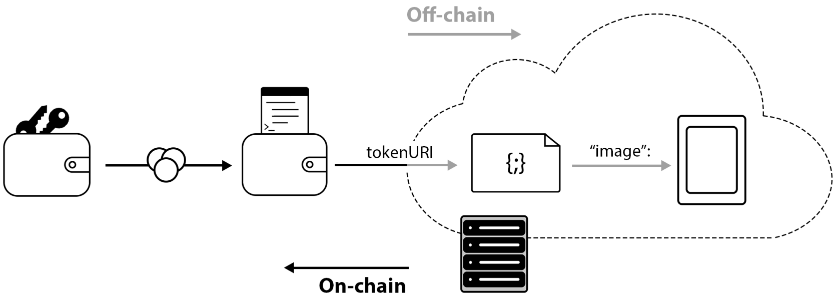


Figure 2.3: Metadata storage scheme for the lowest ranked NFTs in the Michelin guide

.

Decentralized vs Centralized Storage

In the early days of NFT projects, centralized solutions were commonly used to store the metadata associated with the tokens. This approach involved storing all data in a single location, which provided the benefits of easy accessibility and centralized management. Additionally, centralized storage offered a high degree of customizability, enabling developers to tailor the storage solution to meet the specific needs of their project. As the NFT ecosystem progressed, decentralized storage solutions were created as an alternative to centralized storage. The InterPlanetary File System (IPFS) emerged as a leading open-source project that provides a protocol for implementing this solution. IPFS is the most widely extended option to store NFTs' metadata nowadays. To better understand its components and how they interact with each other, the IPFS Camp Workshops in [34] and [35] are followed as well as the project site information in [36].

IPFS is not an implementation itself, rather it is a set of protocols designed to transfer and organize data in a decentralized manner. When an element is added to the system, it is split into smaller chunks, which can be of a fixed size or cleverly chunked (Rabin chunking), and then a Content Identifier (CID) is assigned to each of these chunks. The CID is created by running the data through a hash algorithm and adding a metadata prefix that identifies the algorithm used, how the data is encoded, the version of the CID specification and the number-based encoding used for the string (in the CID version 0 most of this is implicit, with the resulting CID as a raw multihash with no added prefix). Once split, IPFS uses a set of specifications called InterPlanetary Linked Data (IPLD) to represent all that information and its relationships using a Merkle Directed Acyclic Graph (DAG). A DAG is way to represent data where nodes are connected to each other by their edges without forming a closed loop, Figure 2.4 shows the two currently supported layouts.

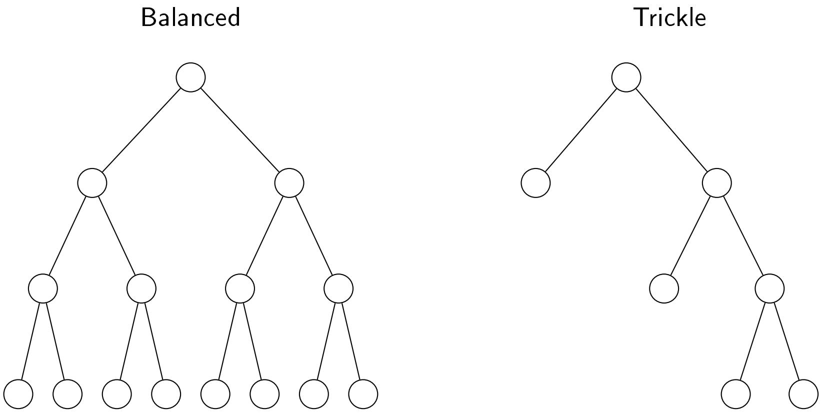


Figure 2.4: IPFS - DAG Layouts

In the Merkle DAG each node has a hash that is calculated based on its contents, therefore a slight modification on one of the chunks will propagate and create a complete different hash in the top node. Nodes are wrapped in something called the UnixFS wrapper, which includes metadata about the data such as its size, type, and other attributes. This allows IPFS to provide more granular control over how files, directories and their symbolic links are stored, accessed, and shared.

IPFS employs various mechanisms to locate a particular CID within the network. One such approach is Kademlia, which is a type of Distributed Hash Table (DHT) that maintains a record of peer IDs and the corresponding CIDs they can offer. Nodes can also use the Bitswap protocol, asking other members for CIDs and storing wantlists so that if they later receive the requested data can send it to the node who originally requested it. If a node do not have the computational resources required to use any of these mechanisms it can rely on an HTTP API, asking a delegated router to search for peers who have the CID on its behalf.

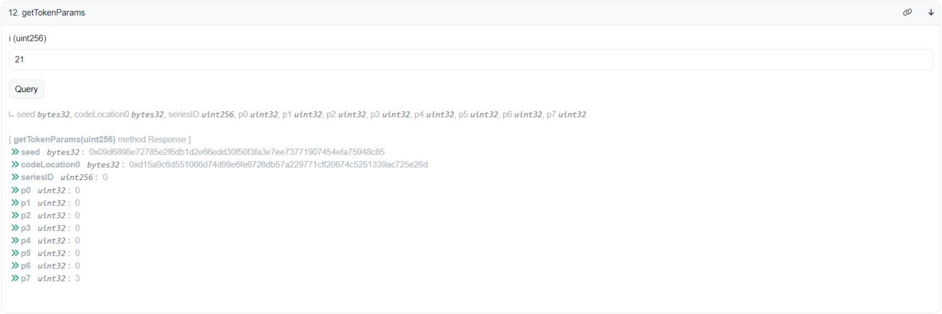
Once the peers in possession of the CID being searched are found, there are other systems used to distribute the content across the network of nodes. Apart from content routing, the Bitswap protocol can be used for this purpose. There are also nodes who offer HTTP Gateway APIs that allow other nodes not implementing any of the mentioned systems to fetch the data, being `ipfs.io` the official gateway maintained by the IPFS development team and the one used in this text to refer readers to content stored using these protocols such as the image of Quantum.

IPFS has multiple implementations, each developed using different programming languages. For example, Kubo is an IPFS implementation written in Go, Nabu in Java, and iroh in Rust. This allow for IPFS to be used across various platforms and integrated into a wide range of applications. In addition to the different implementations, there are also related projects that build on IPFS's capabilities. One such project is Filecoin, which incentivizes users to rent out their unused storage space and creates a marketplace for storage, thereby improving long-term data availability. Another project is NFT.storage, which uses a combination of IPFS and Filecoin to provide long-term storage for NFTs.

Overall, it can be said that decentralized storage solutions provide a high degree of security as data is distributed across nodes instead of a single location. Reliability, as the data is addressed based on its content, therefore it can be easily checked whether it has been tampered. Accessibility, while data remains unchanged the identifier will continue to be the same, this prevents issues that can arise when hyperlinks become invalid or point to the wrong resource. It eliminates the possibility of a person or entity gaining greater control over the data by distributing it in a more equitable manner. Deduplication is also one of its key benefits, it refers to the ability of removing added data already existing in the system, enhancing its scalability and efficiency.

IPFS still faces an issue with content that is not pinned. Pinning is a process that prevents items from being removed during garbage collection as part of the caching mechanism. The next class in the classification scheme consists of NFTs whose data is permanently stored through the "calldata" of a transaction. Calldata is where the information from an external call to the contract is stored [37], which solves the pinning problem of IPFS, as the data becomes permanently available due to the nature of blockchain technology. However, this solution limits the token's functionalities since the data is only accessible from an external call, such as using a full node or delegating the call to a blockchain explorer like Etherscan. The data cannot be used by other functions contained in the same contract. One example of such a collection is 0xmons [38], which offers tools to store the acquired token in the calldata of a transaction, whose hash will be later retrieved by the smart contract code as the location of the metadata. The images in 0xmons are gif files encoded in base64. This can be a cost-effective option since the cost of storing information in the calldata of a transaction is 39 times lower than that of storing it in the smart contract itself (16 gas per byte compared to 20.000 gas 32 bytes, respectively).

The third class in the classification scheme refers to assets whose data is stored in the contract, but requires a compiler to reconstruct the data from raw files. An example of this type of storage solution is 0xDEAFBEEF's Synth Poems, a collection of deterministic generative art. This means that the art is generated autonomously by a piece of code run in a computer, and the output will always be the same given the same input parameters. To enable users to retrieve the media file corresponding to a particular token, the author added the function `getTokenParams` (shown in Figure 2.5) to the smart contract. When provided with a token ID, this function returns the hash of the transaction where the code written in C is stored, as well as a hexadecimal variable called the seed. The seed must be included in the raw code as the input to deterministically generate the corresponding media file, which consists of a one-minute audiovisual piece.

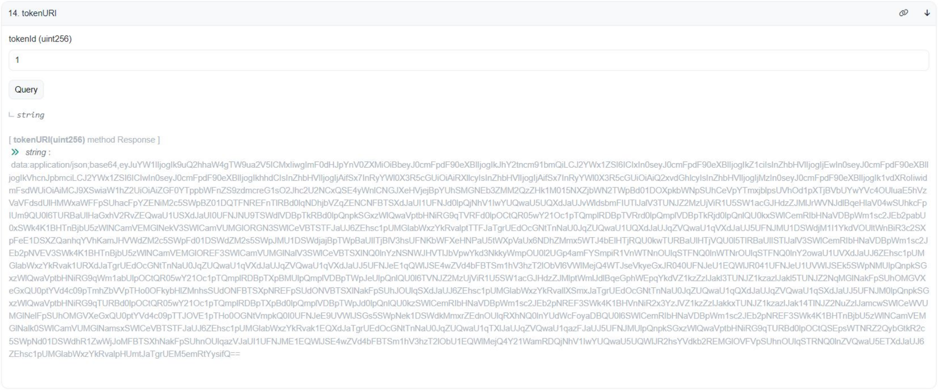


```
12. getTokenParams

i (uint256)
21

Query

∟ seed bytes32, codeLocation0 bytes32, seriesID uint256, p0 uint32, p1 uint32, p2 uint32, p3 uint32, p4 uint32, p5 uint32, p6 uint32, p7 uint32

[ getTokenParams(uint256) method Response ]
» seed  bytes32 : 0x09d6898e72785e2f6db1d2e66edd30f50f3fa3e7ee73771907454efa75948c85
» codeLocation0  bytes32 : 0xd15a9c6d551066d74d99e6fe6726db57a229771cff20674c5251339ac725e26d
» seriesID  uint256 : 0
» p0  uint32 : 0
» p1  uint32 : 0
» p2  uint32 : 0
» p3  uint32 : 0
» p4  uint32 : 0
» p5  uint32 : 0
» p6  uint32 : 0
» p7  uint32 : 3
```

Figure 2.5: Metadata retrieved by the Synth Poems' smart contract. Data Source: [40]

.

The most highly rated class of assets are those whose data is fully stored in the smart contract and can be reproduced within it without the need for any additional compilers. OnChainMonkey is an example of such a collection, as shown in Figure 2.6. When the `tokenURI` function is called, it returns a base64-encoded string containing the token's metadata. Once decoded to UTF-8, the resulting



```
14. tokenURI

tokenId (uint256)
1

Query

∟ string

[ tokenURI(uint256) method Response ]
» string :
```

data:application/json;base64,eyJuYW1lIjogIk9uQ2hhaW4gTW9ua2V5ICMxIiwgImF0dHJpYnV0ZXMiOiBbeyJ0cmFpdF90eXBlIjogIkJhY2tncm91bmQiLCJ2YWx1ZSI6ICIxIn0seyJ0cmFpdF90eXBlIjogIkZ1ciIsInZhbHVlIjogIjEwIn0seyJ0cmFpdF90eXBlI
jogIkVhcnJpbmciLCJ2YWx1ZSI6ICIwIn0seyJ0cmFpdF90eXBlIjogIkhhdCIsInZhbHVlIjogIjAifSx7InRyYWl0X3R5cGUiOiAiRXllcyIsInZhbHVlIjogIjAifSx7InRyYWl0X3R5cGUiOiAiQ2xvdGhlcyIsInZhbHVlIjogIjMzIn0seyJ0cmFpdF90eXBlIjogIk1vdXRoIiwid
mFsdWUiOiAiMCJ9XSwiaW1hZ2UiOiAiZGF0YTppbWFnZS9zdmcreG1sO2Jhc2U2NCxQSE4yWnlCNGJXeHVjejBpYUhSMGNEb3ZMM2QzZHk1M015NXZjbWN2TWpBd01DOXpkbWNpSUhCeVpYTmxjblpsUVhOd1pXTjBVbUYwYVc4OUluaE5hVz
VaVFdsdUlHMWxaWFFpSUhacFpYZENiM2c5SWpBZ01DQTFNREFnTlRBd0lqNDhjbVZqZENCNFBTSXdJaUl1UFNJd0lpQjNhV1IwYUQwaU5UQXdJaUJvWldsbmFIUTlJalV3TUNJZ2MzUjViR1U5SW1acGJHdzZJMlJrWVNJdlBqeHlaV04wSUhkcFp
IUm9QU0l6TURBaUlHaGxhV2RvZEQwaU1USXdJaUl0UFNJNU9TSWdlVDBpTkRBd0lpQnpkSGxzWlQwaVptbHNiRG9qTVRFd0lpOCtQR05wY21Oc1pTQmplRDBpTVRrd0lpQmplVDBpTkRqd0lpQnlRU0kxSWlCemRIbHNaVDBpWm1sc2JEb2pabU
0xSWk4K1BHTnBjbU5zWlNCamVEMGlNekV3SWlCamVUMGlORGN3SWlCeVBTSTFJaUJ6ZEhsc1pUMGlabWxzYkRvalptTTFJaTgrUEdOcGNtTnNaU0JqZUQwaU1UQXdJaUJqZVQwaU1qVXdJaUJ5UFNKMU1DSWdjM1I1YkdVOUltWnBiR3c2SX
pFeE1DSXZQanhqYVhKamJHVWdZM2c5SWpFd01DSWdZM2s5SWpJMU1DSWdjajBpTWpBaUlITjBlV3hsUFNKbWFXeHNPaU5tWXpVaUx6NDhZMmx5WTJ4bElHTjRQU0kwTURBaUlHTjVQU0k1TlRBaUlISTlJalV3SWlCemRIbHNaVDBpWm1sc2J
Eb2pNVEV3SWk4K1BHTnBjbU5zWlNCamVEMGlOREF3SWlCamVUMGlNalV3SWlCeVBTSXlNQ0lnYzNSNWJHVTlJbVpwYkd3NkkyWmpPU0l2UGp4amFYSmpiR1VnWTNnOUlqSTFNQ0lnWTNrOUlqSTFNQ0lnY2owaU1UVXdJaUJ6ZEhsc1pUM
GlabWxzYkRvak1URXdJaTgrUEdOcGNtTnNaU0JqZUQwaU1qVXdJaUJqZVQwaU1qVXdJa [illegible]
xzWlQwaVptbHNiRG9qWm1abUlpOCtQR05wY21Oc1pTQmplRDBpTXpBd0lpQmplVDBpT [illegible]
eGxQU0ptYVd4c09pTmhZbVVpTHo0OFkybHlZMnhsSUdONFBTSXpNREFpSUdONVBTSX [illegible]
xzWlQwaVptbHNiRG9qTURBd0lpOCtQR05wY21Oc1pTQmplRDBpTXpBd0lpQmplVDBpTW [illegible]
MGlNelFpSUhOMGVXeGxQU0ptYVd4c09pTTJOVE1pTHo0OGNtVmpkQ0I0UFNJeE9UVWlJ [illegible]
GlNalk0SWlCamVUMGlNamsxSWlCeVBTSTFKaUJ6ZEhsc1pUMGlabWxzYkRvak1EQXdJaT [illegible]
5SWpNd01DSWdhR1ZwWjJoMFBTSXhNakFpSUhnOUlqazVJaUI1UFNJME1EQWlJSE4wZ [illegible]
ZEhsc1pUMGlabWxzYkRvalpHUmtJaTgrUEM5emRtYysifQ==

Figure 2.6: Metadata retrieved by the OnChainMonkey's smart contract. Data source [42]

.

string containing the token's metadata. Once decoded to UTF-8, the resulting

JSON file contains the image description in SVG format, encoded once again in base64, this is usually done to handle special characters as discussed in the article in [41].

A quick examination of some of the top NFT collections traded in the largest marketplace, Opensea, provides meaningful insights about the storage solutions currently employed. Figure 2.7 illustrates the category under which 20 of the biggest collections based on sales volume fall. For a list of the selected collections refer to [43].

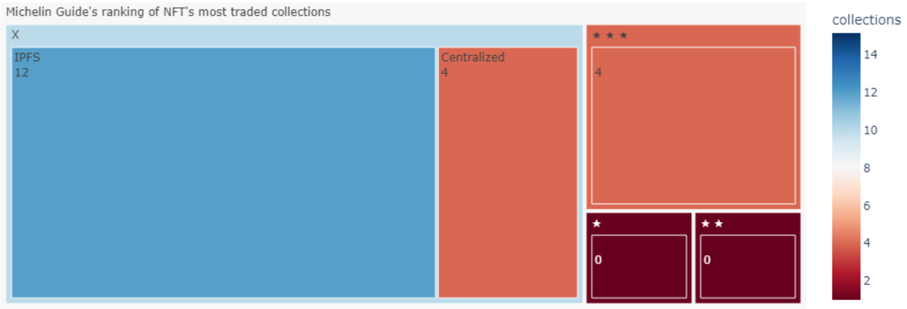


Figure 2.7: Tree map with the NFTs metadata storage distribution for 20 of the most traded collections. Data source [44]

.

IPFS is currently the preferred solution, and it appears that one- and two-starts collections are not among the most traded ones. The predominance of the 0-stars collections can be mainly attributed to the nature of the media files as discussed in the post in [45]. Fees in the Ethereum network are paid based on the amount of data being sent to the network, they are calculated as the product of the gas price at the time of transaction execution and the required gas (computational steps). 3-stars collections commonly use SVG files to store images within the contract. SVG stands for Scalable Vector Graphics and it is an XML-based format where the image is created using mathematical functions to represent the geometrical shapes that compose it. This format is easier to handle by the smart contract as the media file can be scaled to any arbitrary size, resulting in smaller files size. In contrast to vector-based SVG files, raster graphics are composed of a fixed grid of pixels, and the file size of an image is highly dependent on its resolution. This means that higher resolution images will require more pixels and therefore more storage capacity. Popular raster graphics formats include JPEG and PNG. However, they provide more granular control over colors, effects, and shapes than SVG. It is also worth noting that not all platforms support SVG natively, and additional software or plugins may be required to render these types of images. As a result, the decision to use different resolutions and graphics formats ultimately depends on the specific requirements of the project at hand. The development team must carefully consider factors such as the level of detail required for the media files, the computational resources needed to render them, the constraints of the EVM, and the limitations of the storage solution.

As an example, it can be considered Cryptoadz and Moonbirds, two popular collections published under the CC0 license [46]. When the contract code is summoned to return the image file for a particular token in these collections, the result is typically an encoded string. To visualize the image, the information contained in the string can be parsed using a simple Python script. After increasing the size of the image using the resample by approximation option in Photoshop to improve its display, the images can be viewed as shown in Figure 2.8. The Moonbirds collection uses GIF format to represent its images, while Cryptoadz uses BMP, both of which are types of raster graphics. By examining these images, it can be seen that all the necessary information is contained within a few pixels: 36×36 in the case of Cryptoadz and 42×42 in the case of Moonbirds. This makes it feasible to store the required layers to generate the images within the contract. These projects are also referred to as in-chain [49], as the images are rendered by the smart contract returning a bare-bones version of the image that does not require any additional computation to be displayed.

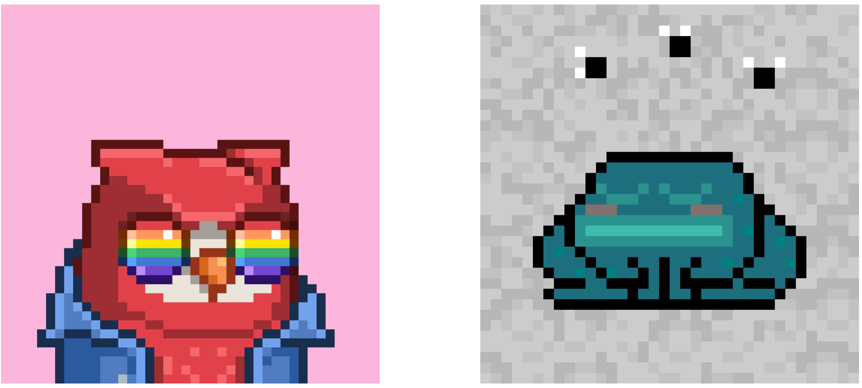


Figure 2.8: CrypToadz #1044 (right) and Moonbird #1 (left). Images sources [47] and [48]

ecc0s, a 3-stars collection under public license, provides an example of how images can be generated in SVG format, as opposed to raster graphics. Figure 2.9 displays two of the collection's items and demonstrates how the resolution of the images is significantly higher compared to that of Moonbirds and Cryptoadz. The use of simple geometric shapes in ecc0s makes it easier to generate the images using a markup language. In NFT projects like this one, when the `tokenURI` function is called, it often returns an URI with the data: scheme and the application/json;base64 MIME type (Multipurpose Internet Mail Extensions, used to indicate the nature of the file) to encode and embed the JSON file with the token's description. One of the objects in the JSON file, labeled under the name "image" or "image_data", contains another URI with the image/svg+xml;base64 MIME type that, when rendered, displays the media file. This approach is followed to ensure that the NFT conforms with the ERC-721 metadata standard (or its extensions, such the Opensea's standard [51]) and it can be easily displayed in-app by the different marketplaces. Furthermore, using this data structure enables the

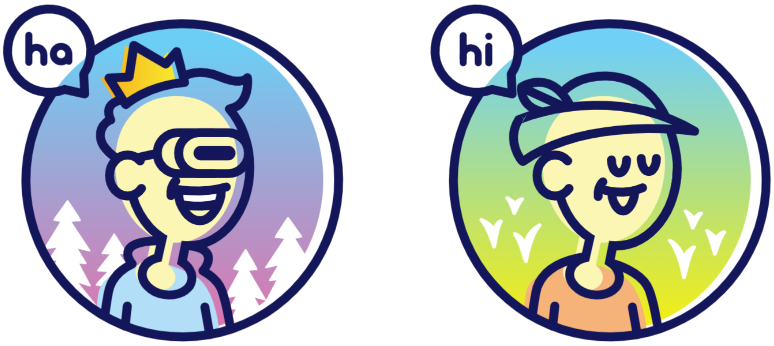
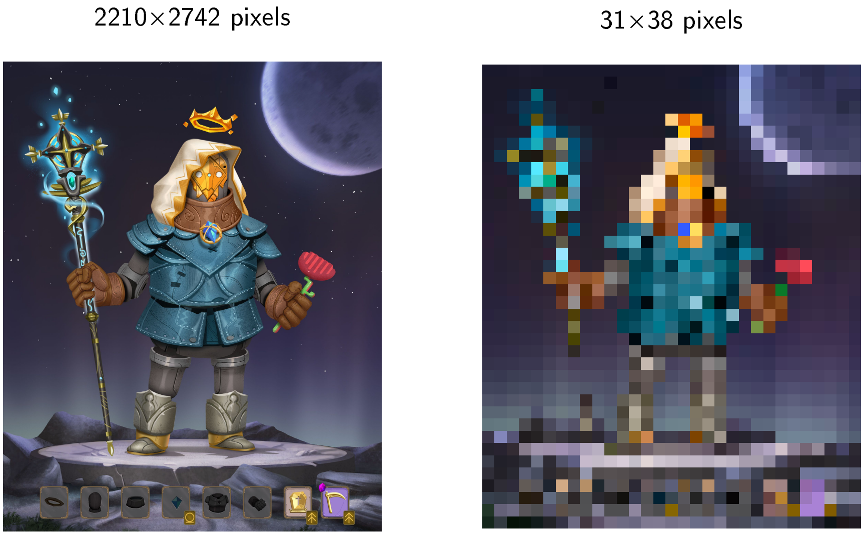


Figure 2.9: ecc0s #1 (left) and ecc0s #2 (right). Images source [50]

images to be displayed by web browsers and other software in a single HTTP request, rather than fetching it in multiple requests.

Hyperloot is another example of a collection published under the CC0 license whose metadata is stored off-chain due to the higher resolution of the images as it can be seen in Figure 2.10 where the original image is compared with one that has been resampled to 31×38 pixels using the approximation method. The representation is not 100% accurate as both images have had to be scaled to fit them within the page margins. Nevertheless, it provides a good visual representation of the idea to be conveyed. The increased level of detail of the images makes it


2210×2742 pixels

31×38 pixels

Figure 2.10: Hyperloot #1 original image (left) and resampled using a smaller number of pixels (right). Image source [52]

highly expensive to generate them on-chain, as the minimum number of pixels required to achieve that detail is considerably increased, in this case the images use 6.059.820 pixels, whereas in the Moonbirds and Cryptoadz collections they use about 1.600. They could be generated using SVG at a lower cost, but generating intricate details or unique effects can be time-consuming and require extensive knowledge and experience.

While the technical aspects of NFT metadata are important for understanding how these digital assets are stored and traded, it is also essential to consider the legal and ethical implications of using and owning NFTs. One important issue to keep in mind is that purchasing an NFT does not always grant the buyer with Intellectual Property (IP) rights to the underlying digital asset. In some cases, the creators or owners of the digital asset retain ownership of the IP rights, even if the buyer holds the NFT as proof of ownership. In this case, the creators or owners of the images being used have waived their copyrights and related rights, allowing for their free and unrestricted use for informational purposes.

After the technical explanation about the underlying architecture of these assets, the chronology of events leading up to their widespread adoption will be continued. Following the enormous success of CryptoPunks, during the October 2017 ETHWaterloo, a hackathon bringing together many Ethereum experts from across the globe, a test version of the blockchain game CryptoKitties was developed. The game consists of breeding cats whose appearance is determined by a number of attributes, the Cattributes, which can be inherit by the offspring. The cats are represented by ERC-721 tokens and can be obtained via breeding or acquiring them from sellers. The price of the NFTs is heavily influenced by their rarity, which in turn is determined by the perceived uniqueness and desirability of the item among users. This scarcity is a key driving factor in their value, as it is often based on the number of NFTs that share similar traits. NFTs with unique or uncommon traits are more likely to attract buyers' attention and command a higher price than those that do not.

The project was an enormous success, with the test version unveiled at the hackathon resulting in the sale of one of the earliest and most famous high-selling NFTs, Genesis, for a total of 246.9258 ETH ($113.082, considering the exchange rate at that time). The popularity of the game congested the network skyrocketing the gas fees, the monthly sales volume in December 2017 reached a total of 36.388 ETH, according to the information provided in [53]. This project set a significant precedent for NFT-based gaming, which is currently one of the most popular applications of NFTs. Its success was followed by the creation of new gaming and metaverse projects with Decentraland as one of the most prominent. Decentraland is a virtual world that uses both virtual reality and augmented reality technologies to create an immersive and interactive user experience. Decentraland operates on a unique governance structure that functions as a Decentralized Autonomous Organization (DAO). In this structure, decisions that will affect the virtual world are made through a process of decentralized decision-making and consensus-building among its members or token holders. This is achieved through the use of smart contracts that encode the rules and decision-making processes of the DAO. The versatility of this governance model enables its application in diverse contexts, including the insurance industry. Later, it will be examined a prevalent instance of a DAO already functioning within this sector.

The platform has hosted big events, such as the recent Metaverse Fashion Week 2023 [54] with the presence of highly reputable firms, including Dolce & Gabbana, Tommy Hilfiger, and Adidas. The popularity of the project resulted in of the most expensive virtual lands sales ever made, when one of the subsidiaries of the company Tokens.com acquired the token Fashion Street Estate for a total amount of $2.4 million, transaction details can be found in the market tracker in [55].

Cryptokitties also served as the catalyst for the creation of OpenSea [56], which has now become the largest NFT marketplace. OpenSea provides a simple interface for users to trade a diverse range of digital assets in one place. To list an NFT for sale on OpenSea, users must first grant permission to the marketplace to manage their token through the `approve` or `setApprovalForAll` functions. The marketplace protocol, such as Seaport in the case of OpenSea, then takes over the management of the token and handles the listing process. OpenSea offers various mechanisms for selling items, including different timed auctions formats such as Dutch and English auctions, in addition to the traditional fixed-price listing. According to DappRadar [57], over 4 million traders have used OpenSea, making it the most widely used NFT marketplace. As of the time of writing, OpenSea accounts for 57.86% of traded volume in the top 25 NFT marketplaces, with a total volume of $35.48 billion. The emergence of these user-friendly NFT platforms have made NFTs more accessible to people with a less in-depth understanding of the underlying technology.

It was in 2021, when the NFT market experienced an unprecedented bull run, with skyrocketing demand and interest in NFTs. The involvement of major auction houses like Christie's and Sotheby's added a significant level of credibility to the burgeoning industry, attracting attention from a wide range of media outlets and stakeholders. As a result, the NFT market saw an influx of new investors, collectors, and creators, leading to a surge in sales and a deluge of innovative new projects. In March of the same year, the art world witnessed a groundbreaking moment in the history of NFTs with the sale of "Everydays: the First 5000 Days" by renowned artist Mike Winkelmann. The artwork was auctioned off at Christie's and fetched a record-breaking price of $69.346.250 [58], making it the most expensive NFT ever sold to a single collector. This unprecedented sale not only demonstrated the growing popularity and value of NFTs, but also marked a turning point in the traditional art market's acceptance of digital art as a legitimate and valuable form of artistic expression. While some critics speculate that this sale was a publicity stunt arranged between the collector and the artist to drive up the value of other tokens in the collection, the fact that such a high price was paid for an NFT is a clear indication of the growing interest and demand for these digital assets.

The surge in popularity and interest in NFTs continued throughout the end of 2021, driven by various factors. The lockdowns brought a new wave of individuals into the financial markets, with cryptocurrencies like Bitcoin reaching all-time highs. This, in turn, led to a significant increase in demand for NFTs, as illustrated in Figure 2.11, which displays the sales and transaction volume history on the top two blockchains. New blockchains started to appear in the scene and many of the

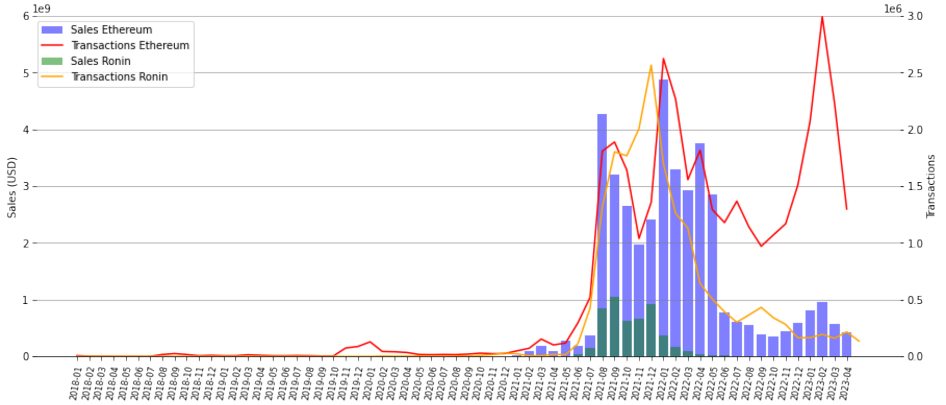


Figure 2.11: NFT sales and transactions volume history in the top two blockchains (excluded wash trades). Data source: [59]

.

existing ones, started to implement their own NFTs such as Solana, Cardano and Flow among others.

Facebook's new strategic plan and rebrand to Meta also played an important role in the increasing demand of the NFTs during 2021. The company's vision of bringing the metaverse to the masses opens up new use cases for NFTs beyond the art industry. While some skeptics view the NFT market as a Ponzi scheme benefiting only early entrants, the concept of tracking ownership and provenance of digital assets has far-reaching applications in industries such as real estate and finance. Veracity Protocols is one such companies leveraging NFTs in conjunction with computer vision and machine learning algorithms to unlock the full potential of these assets. By creating a direct, immutable link between physical objects and their digital representation, they eliminate companies' dependence on unsecure links which can be removed, replaced or tampered with [60].

2.3 Vulnerabilities and Insurance opportunities

The novelty of the technology underpinning digital assets has resulted in limited human understanding, leading to concerns about potential vulnerabilities that could be exploited by malicious actors. The intricate nature of the technology behind these assets has also deterred many from adopting them as readily as they would physical assets. Moreover, the escalating number and complexity of cyberattacks have hindered their widespread adoption. A study in [61] reported that out of the 1,700 CISOs and IT professionals surveyed, 59% believed that cyberattacks are becoming increasingly sophisticated, and it is estimated that cybercrime will cost the world around $8 trillion.

The digital asset space has witnessed an increasing number of theft cases and stolen value for both NFTs and cryptocurrencies in 2021 and 2022. Figure 2.12

illustrates the evolving landscape over two distinct but close periods of time. The left-hand graph demonstrates the total value stolen from the smart contracts of thirteen blockchains with high transaction traffic. The right-hand graph shows an increase in the number of NFTs stolen in 2022, despite a decrease in the average losses per item stolen.

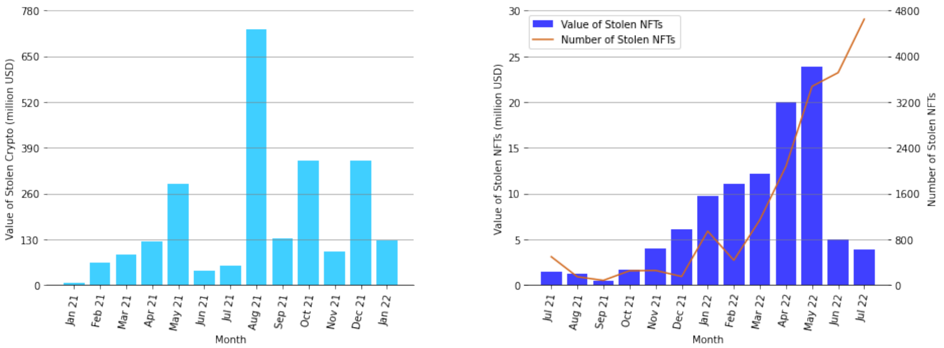


Figure 2.12: Cyrptocurrency lost to theft based on smart contract incidents on 13 different blockchains (left) and total value and number of stolen NFTs (right). Data sources: [62] and [63]

.

The lack of awareness among users regarding the potential risks associated with acquiring digital assets underscores the importance of having insurance coverage to safeguard their investments. Such coverage can bolster the reputation and credibility of these assets, paving the way for their expansion into other industries and driving the development of new applications to improve current business processes.

As reported in [64], currently only 1% of all crypto investments are covered under an insurance policy, which highlights the pressing need for insurers to start developing new policies in a market that is expected to grow at a CAGR of 11.1% and reach a value of $1.9 trillion by 2028 [65]. It is crucial for insurers to act quickly to provide insurance solutions that can mitigate the risks associated with digital assets and build confidence among users, thus promoting the long-term sustainability and growth of the cryptocurrency market.

The emergence of the Web3 economy presents a wealth of promising opportunities for the insurance industry, particularly with regard to the expanding range of insurable digital assets. This study delves into the rapidly expanding NFT market, with approximately $56.7 billion in total traded volume at the time of writing, based on the information provided in [59], making it a highly attractive market for early adopters who can develop scalable solutions and leverage their experience to redefine policy frameworks based on the increasingly available data and previous claims. As this market continues to evolve, those who are well-positioned to capitalize on these developments stand to reap significant profits.

Although the NFT market presents a compelling opportunity for insurers in the Web3 economy, it is not the only one. As previously mentioned, insurers can also leverage blockchain-based protocols to transform their traditional value chain, reducing inefficiencies and unnecessary work. This presents a fascinating opportunity to streamline their operations and create more value for their customers in the Web3 ecosystem. The report in [66] provides some of the Web3 capabilities insurers could leverage to improve existing insurance products:

- *Smart contracts*: Insurers could embed policy agreements into code that is automatically executed when certain conditions are met. This provides a high degree of transparency as the code of the contract can be publicly accessible (depending on the type of blockchain as it was previously explained in the difference between private, consortium and public blockchains). By utilizing smart contracts, customers would have a better understanding on what type of coverage they are acquiring, avoiding the problem of vague descriptions buried under legal terms that are often difficult to understand. For instance, Coinbase's description of their coverage in [69] is quite brief and may not provide enough detail for customers seeking specific information. However, this also requires insurers to ensure that the code is understandable to customers who may not have extensive experience in the Web3 ecosystem.
- *Oracles*: Entities used to bring real-world data into the blockchain where the smart contract with the policy agreement is deployed. To avoid the problem of relying on a central authority providing the data, Decentralized Oracle Networks such as Chainlink Price Feeds [68] have been created. Oracles enable the creation of blockchain-based parametric insurance products which is a type of insurance where claims payouts are executed when pre-specified events are triggered such as natural disasters, whether events or market fluctuations.
- *Governance and utility tokens*: Tokens can be issued by companies to incentivize user contributions to the capital pool. These tokens allow stakeholders to participate in decision-making processes such as funds allocation, protocol upgrades, and investment decisions. Additionally, companies can use utility tokens to engage users in specific tasks such as claim evaluation or risk assessment, creating a sense of community. Governance tokens grant stakeholders the ability to vote on important decisions, ensuring that their voices are heard and valued. This level of participation and transparency can foster a sense of ownership and loyalty among users. Meanwhile, utility tokens can be used to incentivize users to perform specific actions, rewarding them for their contributions and encouraging continued engagement with the project. By leveraging a combination of both, companies can build a strong community around their project.

Nexus Mutual is one such example of insurance companies operating as a DAO, concept previously discussed when examining the governance structure of Decentraland, as part of the broader history of NFTs. As a mutual insurance company, Nexus Mutual is owned by its policyholders, rather than shareholders as is the case with traditional stock insurance companies [70]. This unique ownership structure makes it well-suited to operate as a DAO, given the decentralized and democratic nature of the organization.

According to information available on their website [71], Nexus Mutual offers its own NXM token, which provides users with various benefits such as on-chain governance, DAO governance, claim assessment, and staking. This token is backed by the capital pool created from all the ETH and DAI (two types of cryptocurrencies) invested by members. To ensure a reliable feed for the ETH/DAI price, which is necessary to maintain the minimum capital requirement for the platform's operations, Nexus Mutual utilizes Chainlink's Price Reference Contracts, a decentralized network of price oracles [72].

The backbone of the platform are its smart contracts, which require comprehensive security audits to ensure their reliability. The corresponding addresses of the smart contracts deployed on the Ethereum Mainnet can be found in [73]. Nexus Mutual policies are represented as NFTs, which contain the agreement details in their metadata. When a customer purchases a policy, a new NFT is minted and sent to the insured address. They currently offer coverage for a range of assets, including protocols deployed on EVM-compatible networks, validator node's stake, assets held in centralized crypto custodians, assets deposited into a vault strategy, and protection for cover providers.

Nexus Mutual's protocol provides a great example of how insurance companies can leverage the previously mentioned Web3 capabilities. The platform has already provided coverage for assets worth over $4 billion and has paid out more than $17 million in claims, as reported on their website [74]. These numbers demonstrate the potential profitability of the Web3 ecosystem and highlight the opportunities that will continue to emerge as human understanding of the technology evolves.

Chapter 3

Review and selection of digital assets

NFTs can be classified according to their potential uses. Several websites provide different categorizations based on their own criteria. In this instance, Opensea's classification will be followed, providing a brief explanation of each category:

Art. As discussed in their history, NFTs in the art category have become increasingly popular due to the need for a secure method of recording provenance and ownership of digital art. These NFTs have similar use cases to traditional art, such as collecting, exhibiting, and selling. In addition, a subcategory of art NFTs known as generative art has emerged, which involves art that is algorithmically generated by an autonomous system, it was already mentioned when giving the example of Synth Poems as a two-stars collection. Generative art NFTs have gained popularity due to their unique and unpredictable nature, with each piece being one-of-a-kind.

Gaming. Play-to-earn (P2E) games use a unique class of assets that offer players the opportunity to earn rewards as they progress through the game. These blockchain-based games have revolutionized the gaming industry by allowing players to monetize their in-game achievements. Cryptokitties is widely recognized as the first P2E game, while other popular titles like Axie Infinity and Gods Unchained have also gained immense popularity in recent times. With P2E games, players can earn valuable assets that can be sold for profit, adding a new dimension to the gaming experience.

PFPs. When most people think about NFTs, the first thing that comes to mind is Profile Picture NFTs. These digital assets are often used as avatars on social media platforms, especially among Twitter Blue subscribers. The popularity of Profile Picture NFTs is on the rise, with famous collections such as the Bored Ape Yacht Club, CryptoPunks, and Doodles gaining massive traction in recent times. Beyond their aesthetic appeal, PFPs hold significant value as unique, one-of-a-kind assets that reflect the personality and tastes of their owners.

Photography. With the advent of NFTs, photographers now have a broader market to sell their artwork to, thanks to the exposure they get through various NFT marketplaces. Although photography may not be the most prominent category in the NFT space, it has been attracting new users and garnering significant attention. Collections such as Where My Vans Go have achieved remarkable sales volumes, exceeding 4.000 ETH.

Domain names. They serve a similar purpose to traditional Domain Name Services, providing human-readable addresses that are easier to remember than long hexadecimal strings, making it simpler for users to verify that money is being sent to the right address. Ethereum Name Service domains are the most popular in this category, with names like paradigm.eth selling for over $700,000.

Music. NFTs are transforming the music industry by offering tokenized versions of artists' songs. Unlike the traditional purchasing model where the buyer pays for a license to listen to the song, NFT buyers purchase ownership rights of one of the minted tokens. This model creates a more equitable relationship between artists, labels, and streaming platforms, which in the traditional Web2 model, take a significant cut of artists' profits and creativity freedom. Moreover, fans play a more participative role, receiving royalties on streaming rights in some cases or even exclusive access to concerts or merchandise. By giving fans a direct stake in the success of the artist, NFTs have opened up new avenues for creative expression and monetization, offering a more democratic and transparent model for the music industry.

Sport collectibles. Tokens capturing memorable moments in the history of sports or featuring well-known celebrities. It represents a shift from the traditional sports card market, which has experienced a boom in recent years. By incorporating Web3 capabilities, these digital cards enable buyers to track the full history of each and ensure its authenticity. Examples of these can be found on NBA Top Shot, a marketplace featuring numerous tokens displaying basketball video clips.

Virtual worlds. Assets that represent ownership of lands, wearables, properties, and other items in alternate realities. As mentioned earlier, people can purchase virtual plots of land in Decentraland for vast amounts of money. This category of assets opens up new and exciting applications in the insurance industry, where analogies such as insuring a house or a vehicle could be adapted to this new alternate dimension. The introduction of NFTs in virtual worlds offers a unique opportunity to create new digital economies and redefine the way we people interact in virtual spaces.

It is crucial to distinguish between the different categories of NFT assets because they pose varying levels of risks. For instance, PFPs are among the most popular NFT collections and have been targeted in multiple theft cases in the past, making them a high-risk category. As a result, this study focuses on PFPs since they provide valuable insights into mitigating potential risks and offer a wealth of historical data about previous heists.

3.1 NFT Cybercrimes

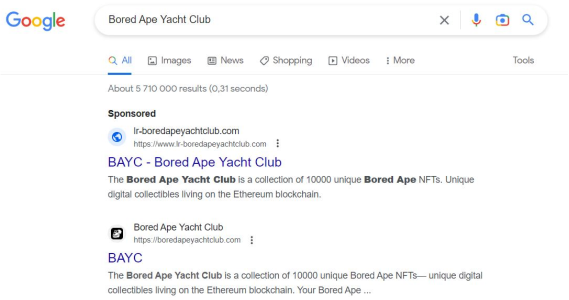
NFTs can be compromised in various ways, with varying levels of sophistication. To gain a better understanding of the potential attacks, some of the most relevant from an insurance perspective will be mentioned following the extensive guide provided by Elliptic, a blockchain analytics firm, in [63].

3.1.1 Phishing Scams

Phishing scams encompass various types of attacks that share similar characteristics. These attacks usually involve a malicious actor attempting to trick a user into clicking on a harmful link or visiting a website and granting the attacker permission to manage the user's tokens. In some cases, the attacker may try to set their own address as the operator in the `setApprovalForAll` function, giving them control over the user's tokens, this family of attacks was defined by Microsoft in early 2022 as "ice phishing" in their post in [75], and it is one of the most common vectors of attacks. In other cases, hackers simply infect with a malware the user's computer. Phishing attackers use a combination of engineering and psychological techniques to develop elaborate plans that can be difficult to detect. Some of the common forms these attacks can take will be discussed.

Domain Squatting and Impersonation

Cybercriminals often create counterfeit websites that mimic authentic ones, using search engine optimization techniques to boost their rankings. Figure 3.1 illustrates a recent search in Google for one of the most popular collections, showcasing an example of this practice.



About 5 710 000 results (0,31 seconds)

Sponsored

lr-boredapeyachtclub.com
https://www.lr-boredapeyachtclub.com

BAYC - Bored Ape Yacht Club

The **Bored Ape Yacht Club** is a collection of 10000 unique **Bored Ape** NFTs. Unique digital collectibles living on the Ethereum blockchain.

Bored Ape Yacht Club
https://boredapeyachtclub.com

BAYC

The **Bored Ape Yacht Club** is a collection of 10000 unique Bored Ape NFTs— unique digital collectibles living on the Ethereum blockchain. Your Bored Ape ...

Figure 3.1: Fake website replicating the original BAYC's website in Google Chrome

.

Social Media Compromises

NFT collections teams and marketplaces often create their own social networks to communicate with customers and provide updates on the project's roadmap.

Discord is one of the most commonly used social media platforms for this purpose. However, these communities are also vulnerable to malicious users who take advantage of the need for communication by posting fake links that can harm unsuspecting users.

Malicious users can employ various techniques, including social engineering, to manipulate a member of the project and gain access to sensitive information such as login credentials for their Discord account. Once a hacker gains access to a server, they can pose as the legitimate account owner and post malicious links to a wide audience.

To prevent such attacks, it is crucial for those managing the server to ensure that their security measures are effective and that there are no exploitable bugs. An example of an attack derived from a faulty tool occurred in the Opensea Discord server. Collector Jeff Nicholas, told in the post in [76], how he brought a Zendesk ticket to the Discord channel to expedite a process (as many other reputable collectors used to do), but was then contacted via private message by a hacker impersonating an Opensea help center staff member using permissions only granted to moderators. The hacker guided Nicholas to display a QR code of his MetaMask wallet, which was subsequently drained. This incident highlights the need for improved security measures, particularly when using external tools such as ticketing systems, and for increased awareness among community members regarding potential threats.

Another common failure among NFT collection developers is the display of broken links on their servers. This can provide an opportunity for hackers to reuse the link and create fake servers associated with it, which are then filled with malicious links.

Phishing Emails

Phishing emails are a common type of attack that can be similar to social media compromises. However, the scope of these attacks is often smaller as the targeted audience is typically segregated rather than concentrated on a single platform. To carry out a phishing attack, the hacker needs access to the victim's email address.

An example of a phishing attack occurred during Opensea's migration to a new protocol that required users to migrate their listings within a short time frame to avoid paying gas fees [77]. This created an opportunity for hackers to exploit users' Fear Of Missing Out (FOMO) by sending them emails that appeared to be from the Opensea team, providing instructions on how to migrate their assets. These emails included a malicious link that, when clicked, could lead to a variety of harmful consequences.

Airdrops Phishing Scams

The example of Cryptopunks airdrop was already shown in the text, it refers to the practice of distributing items from a collection for free to users as a way to promote the collection or reward loyal members. However, this practice has also been exploited by hackers who create fake websites with simple interfaces that trick users into claiming the airdrop. These fake websites can lead to malicious transactions and result in significant financial loss for the victim.

One way hackers promote these fake websites is by airdropping items into random users' wallets and including a reference to the website where they can mint the actual token or receive some sort of reward. Additionally, they may also impersonate legitimate airdrops by replicating their websites, a practice similar to domain squatting.

Trojan Horse NFTs

In some cases, unexpected airdropped items, instead of pointing to an external website, contain a malicious code that can execute harmful actions on the user's device or wallet. One example of this is the vulnerability discovered by software company Check Point in Opensea's platform, as detailed in their article in [78]. The vulnerability allowed for the embedding of malicious code into an SVG file that, when displayed in a web browser, would prompt victims to sign a malicious transaction under the Opensea operation domain.

These are the most common forms in which phishing scams can be seen, however as attackers become more sophisticated, it is likely that new and advanced techniques will emerge in the future, it is therefore necessary for insurers to educate users on how to avoid falling victim to these tricks by following strict safety checks.

In addition to phishing scams, there are other forms of attacks that can lead to the theft of NFTs. Although these attacks may not be as frequent as phishing scams, they still pose a significant threat to the security of the NFT, accounting for a high number of reported cases.

3.1.2 Swap Scams

In addition to NFT marketplaces, there are platforms that allow users to swap NFTs with each other. Hackers can exploit poorly designed user interfaces to pass off worthless NFTs as if they were from the original collection, tricking genuine users into trading with them. One example is the KiwiSwap platform, which used a flawed verification mechanism for official NFTs, displaying a green checkmark alongside the image to let users confirm they were receiving the original token. However, this allowed a malicious actor to create knock-off NFTs displaying the same checkmark and trade them with victims, as described in the post on [79].

3.1.3 Recovery Scams

Recovery scams are particularly insidious as they prey on the vulnerability of users who have already suffered a security breach. In these types of attacks, hackers create bot accounts on social media platforms like Twitter that automatically reply to users who have posted about losing access to their wallets, seed phrases or tokens. The bots offer to help the victim recover their funds and often include a link to a website that appears to provide recovery services. However, the website is actually a front for the hacker to steal the victim's funds.

3.1.4 NFT-based Protocols Exploits

These are probably the most sophisticated attacks, usually executed by experienced users with extensive knowledge of the space. Due to the complexity of these attacks, preventing them can be challenging since they can take various forms depending on the vulnerabilities they exploit. However, based on past experiences, it is possible to identify certain groups based on similar patterns.

Marketplaces Code Exploits

As seen in the previous numbers when discussing Opensea's influence in the space, there are some NFT marketplaces who have become the go-to platforms for buying and selling NFTs, resulting in a certain level of centralization in the ecosystem. Collections restore to these entities to promote their collection in exchange for part of the earnings that are paid as a percentage of the sells. Opensea currently charges users a 10% on the minting earnings [80] and 2.5% on secondary sells [81]. The life cycle of an NFT project can be separated in two parts: the minting process, where users create the NFTs (a record on the blockchain stating they own an item with a certain id), and the secondary sales, where users trade it with other assets. The minting process is fairly standardized, and developers can create smart contract code for the primary sales event, thereby avoiding marketplace fees. However, some developers still choose to use these marketplaces, as they provide access to a wider audience and benefit from the marketplace's trust and reputation as a battle-tested solution.

During the minting phase, collections receive all the revenue from the sale, which is usually set at a lower price due to the random assignment of tokens. In some cases, the reveal of the media files is postponed so that users do not lose their interest in the minting phase as the rarest tokens are bought. In contrast, the secondary sales revenues are set as a percentage of the sales, the royalties, which, for example at Opensea are capped at 10%. The small size of these roayalties incentivize users to trade their tokens, making it an appealing option for collection creators as it helps to attract a broader audience. The relatively modest profits from secondary sales make it appealing for collection creators to utilize these "centralized marketplaces". Even though they are mostly run by smart contract code, they have a certain level of control over the collections, such as the ability to pause the sale of an item, exclude an entire collection from their platform and in some platforms, they even control the assets being listed for sale as it is the case of the custodial option in marketplaces like Nifty Gateway or Binance.

Given the high volume of transactions managed by NFT marketplaces, these entities must deploy strong safety measures and security checks, as they are prime targets for attackers. Elliptic's report highlights two different marketplaces with faulty tools that allowed users to exploit them for profit, including Opensea. In this particular attack, users took advantage of an error in the user interface that did not display tokens as not being listed. Traders on Opensea commonly send items to another wallet to avoid paying gas fees to delist an item, but while Opensea's frontend displayed the item as not being for sale, the changes were not reflected in the backend API. This allowed attackers to exploit the loophole and make a profit of around 332 ether, as reported by blockchain security firm Peckshield [82].

Airdrop Exploits

While most secondary sales of NFTs take place on major marketplaces, some developers choose to reward their loyal members by promoting their collections and offering free incentives, implementing their own solutions to do so. One common method to achieve this is to allow current owners of items within the collection to claim rewards. However, developers must exercise caution when writing the conditions in the smart contract that users must meet to claim their rewards. This is to prevent malicious users from taking advantage of these airdrops.

The article in [85] describes how an attacker stole unclaimed items from five users of the Bored Ape Yacht Club (BAYC) collection. In March 2022, the BAYC team decided to airdrop 10.094 ApeCoin, their own cryptocurrency, to all BAYC holders. However, due to a flaw in the code that did not check how long users had owned the items, an attacker was able to use a flash loan, a type of uncollateralized loan that can be borrowed and repaid within a single transaction, to borrow five items that were deposited in a vault on NFTX. NFTX is a platform that creates liquidity for NFTs by allowing users to earn yield from protocol fees.

In NFTX, users deposit an NFT in the corresponding collection vault and receive a token in exchange, whose value is determined by the balance of ETH and NFTs in the liquidity pool. Each time a trade is made in the vault, users providing liquidity by staking NFTs (inventory providers) or ETH and NFTs (liquidity providers) are rewarded with a share of the fees that have been paid. To execute the flash loan, the attacker purchased an ape that was listed for sale, needed to pay the protocol's fees. Then, in the same transaction, borrowed five items whose reward had not been claimed by their owners and subsequently claimed the reward and returned the items to the vault, netting a profit of approximately $350k. The whole transaction details can be found in Etherscan in [86].

This incident highlights why users often prefer to use established NFT marketplaces such as OpenSea rather than white-labeled marketplaces. Even large teams of developers, such as those behind Yuga Labs' collections (which includes BAYC), may not have the same level of experience in creating robust solutions as marketplaces that have been battle-tested by managing a high volume of daily transactions.

Cross-chain Bridges Exploits

Bridges provide a means for interconnecting different blockchain networks, but their maturity level is not yet sufficient, and they remain vulnerable to various types of attacks. Bridges have been a common target of many of the biggest cryptocurrency thefts over time. According to the article in [83], bridge attacks accounted for 70% of all cryptocurrency losses in the past year alone.

Network congestion on blockchain networks such as Ethereum has led to the development of new solutions, commonly referred to as domains, including layer 2 scaling solutions and new layer 1 blockchains. These domains offer faster transaction confirmation times and lower fees than their predecessors. To facilitate the transfer of assets between these new solutions and existing ones, bridges have been developed. However, the implementation of bridges presents a challenge known as the "interoperability trilemma," which is discussed in the article referenced in [84].

This trilemma refers to the trade-off between security, generalizability, and extensibility when implementing mechanisms for transferring assets between domains. Achieving high levels of security, generalizability, and extensibility simultaneously is difficult, and typically, one of these capabilities must be sacrificed to achieve the other two.

One commonly used mechanism for transferring assets between domains is the lock-mint/burn-release process. In this approach, the assets being transferred are locked in the source domain, and an equivalent amount is minted in the destination domain. To reverse the process, the destination's minted tokens are burned, and the locked assets can be redeemed. However, native crypto assets residing on one blockchain, such as Bitcoin, cannot be used on other chains, such as Ethereum. To solve this problem, a wrapped version of the token is created to meet the destination standards. Bridges typically rely on a relayer to handle communication between domains, and there are several implementation options. Trusted bridges, are the most common choice, they utilize a federation of off-chain relayers that validate and verify transactions. To achieve consensus on which transactions to include in the bridge, relayers may use a multisignature (multisig) mechanism that requires a certain number of signatures from a pre-selected group of validators. While this solution supports the exchange of arbitrary cross-domain data and is compatible with all domains, it is censorship-prone due to the interoperability trilemma. If the majority of nodes in the federation is compromised, funds can be stolen.

While most bridge attacks to date have targeted fungible tokens, new bridges are now facilitating the transfer of NFTs between domains. As a result, it is essential to explore the safest options for NFT transfers between domains.

3.2 Policy Rating Factors

The subsequent sections will concentrate on the statistical analysis that actuaries must undertake to develop a pricing model.

To establish the premium for a policyholder, a set of rating factors is utilized to categorize them according to their insurability risk. These rating factors are determined based on the available data, which is currently limited due to the nascent nature of the industry. As a result, a general classification has been developed based on the storage methods of the keys safeguarding the assets. This classification primarily focuses on solutions within the Ethereum blockchain, considering that it is the primary platform for NFT trades, but it can also be extended to other domains.

Initially, a classification can be established based on the type of account where assets are deposited. While EOAs are the native accounts on the Ethereum blockchain, recent developments have emerged to adapt smart contracts' behavior to function similarly to wallets. These are commonly referred to as smart contract wallets, with Argent being an example. The logic associated with these wallets is more intricate since smart contracts cannot independently initiate transactions; they require triggering by an EOA.

In the case of Argent wallets, when a user creates an account, both a smart contract and an EOA are automatically deployed. The private key of the EOA, securely stored in the user's device, communicates off-chain with a relayer responsible for on-chain interactions with the smart contract containing the wallet logic [87]. These wallets enhance the capabilities of conventional EOAs by introducing new features, such as setting guardians. Guardians are a designated set of accounts with specific permissions over the smart wallet. They can perform actions like locking and unlocking the wallet or initiating a recovery procedure in case the user loses the device with the EOA associated with the smart contract.

If a user misplaces the device with the EOA registered as the owner of the smart wallet, they can request one of the designated guardians to lock the account, preventing unauthorized access to the funds. Account recovery is also possible, allowing the user to set a new device as the wallet owner, subject to approval from a specified number of guardians. Additionally, ownership of the wallet can be easily transferred without interruptions by obtaining signatures from the required number of guardians and the current owner of the account. Furthermore, certain functionalities like implementing a prolonged waiting time for spending a significant amount of assets can be incorporated into these wallets. They are sometimes referred to as "vaults" and are considered one of the safest mechanisms for long-term asset storage. However, when users wish to trade their NFTs, they must transfer them to an EOA since this is the wallet supported by major marketplaces.

Secondly, wallets can be classified based on how the keys are stored. This classification does not impact smart contract wallets since the private key can be replaced in case the user's device, where it is stored, becomes compromised. EOAs can be broadly categorized as hot and cold wallets (there is also an intermediary group called warm wallets, but it will not be discussed here). Hot wallets store the private key online, which is highly convenient for users requiring frequent daily transactions. They can simply access the wallet extension like MetaMask and authorize transactions within seconds. However, hot wallets are more vulnerable to theft as the window of potential vulnerabilities is wider. On the other hand, cold wallets store the private key offline on a separate device. Users must connect this device with the private key every time they want to perform a transaction. A commonly used solution for cold wallets is Ledger. Cold wallets that are specifically used to store NFTs, without interacting with any other party apart from the wallet used to list the token for sale, are sometimes also referred to as vaults.

Lastly, wallets can be classified based on how they are custodied. There are custodial wallets, where users entrust the management of their keys to the entity providing the wallet service. This is commonly observed in centralized exchanges such as Coinbase or Binance. On the other hand, there are non-custodial wallets where users have complete responsibility for how their keys are stored. Custodial entities typically implement robust security measures, safeguarding private keys in physically secure locations. However, they remain enticing targets for attackers. Hackers may also attempt to circumvent the multi-factor authentication process required for users to access their funds and transfer them to their own wallets.

Custodial wallets are a popular choice for many users due to their simplicity and user-friendly experience, particularly for those with less technical expertise. These wallets offer a streamlined onboarding process, making it easier for users to get started and manage their funds.

Smart contract wallets can be implemented in various ways, each with different security features. These features may include the number of guardians, waiting time for transaction execution, withdrawal limits, and more. Due to these variations, it is challenging to classify them into a single group. However, considering their high level of security and the limited available data on historical thefts associated with smart contract wallets, categorizing them as a type of cold wallet is a prudent assumption to mitigate unexpected losses. Similarly, NFTs stored in custodial wallets, such as those obtained from the Binance NFT marketplace, can also be categorized as cold wallets due to the lack of data and the safety measures implemented in these solutions.

This classification simplifies the rating factors to how keys are stored, allowing policyholders to be categorized into hot and cold wallets. Given the relative newness of the space, insurers may initially develop slightly overpriced models as a precautionary measure. These models can be further refined to create more accurate and competitive policies as more data becomes available.

3.3 Data collection

In order to tackle the challenge presented by the absence of publicly accessible registries containing data on NFT theft cases, two distinct approaches have been explored in an effort to find a viable solution. Both approaches focus on gathering data specifically from the Ethereum network, which has experienced a significant number of cyberattacks in recent years.

3.3.1 Process automation based on patterns identification

The initial strategy involves utilizing pattern identification from prevalent attacks to create a Python script that stores the hash of fraudulent transactions in a dictionary, along with the potential type of attack that compromises the wallet.

There are two approaches to implementing this automated process. The first and most versatile method involves running a full node and locally storing a copy of the blockchain. This allows for quick retrieval of all the necessary information. The second option is to utilize public APIs provided by blockchain explorers like Etherscan. This option is more feasible as it doesn't require storing the entire blockchain, which can be cumbersome due to its large size. According to [88], the blockchain's size is 972.55 GB at the time of writing for a full node. To overcome the storage limitations, a free API key was requested from Etherscan, and a Python script was implemented to fetch data from the available API endpoints within the free plan. Some information was directly extracted from the retrieved JSON files, while others required parsing using BeautifulSoup objects before being stored in the respective dictionary objects. The script can be found in [?], which primarily aims to identify two types of thefts: ice phishing and compromised private keys. The patterns shown in Figure 3.2 were identified for most of these thefts.

As previously explained, ice phishing refers to cases where a user is deceived into signing a malicious transaction that designates the hacker's address as the operator of tokens in a collection using the `setApprovalForAll` function. Subsequently, the hacker transfers the tokens to his own address. In many of these cases,

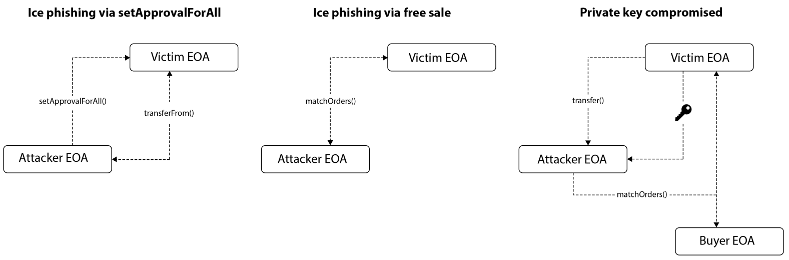
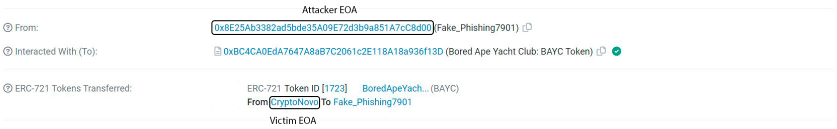


Figure 3.2: Common Strategies Employed to Steal NFTs

a recurring pattern emerges: the transaction is initiated by the same address that receives the tokens from the victim's wallet. An example of such transactions is depicted in Figure 3.3.


Attacker EOA

From: 0x8E25Ab3382ad5bde35A09E72d3b9a851A7cC8d00(Fake_Phishing7901)

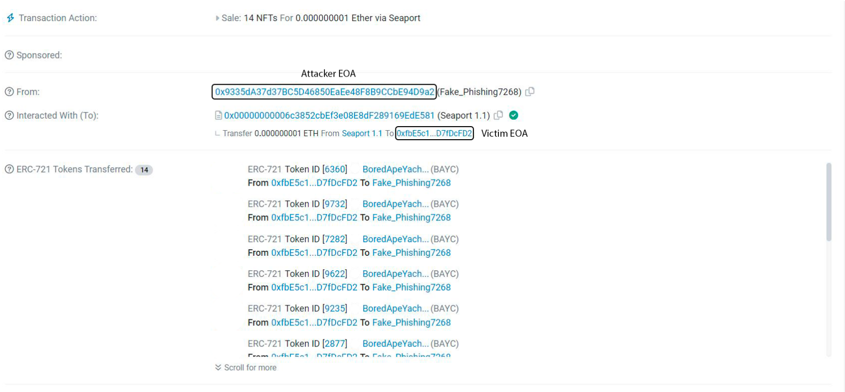
Interacted With (To): 0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D (Bored Ape Yacht Club: BAYC Token)

ERC-721 Tokens Transferred: ERC-721 Token ID [1723] BoredApeYach... (BAYC)
From CryptoNovo To Fake_Phishing7901

Victim EOA

Figure 3.3: Example of Ice Phishing via `setApprovalForAll`. Data source [89]

Another method of deceiving users involves tricking them into signing a transaction where the offer side is empty, and the victim's tokens are listed in the consideration side. Figure 3.4 showcases an example of a highly sophisticated theft, wherein a user was lured into listing his 14 BAYC items for a mere 0.00000001 ETH. Further details about this scam can be found in [91].


Transaction Action: Sale: 14 NFTs For 0.000000001 Ether via Seaport

Sponsored:

Attacker EOA

From: 0x9335dA37d37BC5D46850EaEe48F8B9CCbE94D9a2(Fake_Phishing7268)

Interacted With (To): 0x00000000006c3852cbEf3e08E8dF289169EdE581 (Seaport 1.1)
Transfer 0.000000001 ETH From Seaport 1.1 To 0xfbE5c1...D7fDcFD2 Victim EOA

ERC-721 Tokens Transferred: 14

ERC-721 Token ID [6360] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

ERC-721 Token ID [9732] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

ERC-721 Token ID [7282] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

ERC-721 Token ID [9622] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

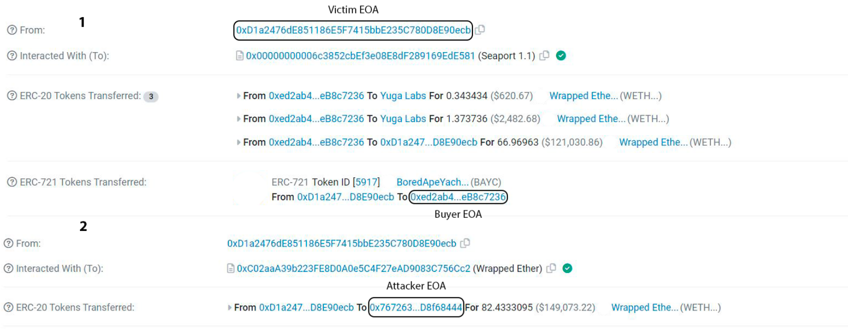
ERC-721 Token ID [9235] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

ERC-721 Token ID [2877] BoredApeYach... (BAYC)
From 0xfbE5c1...D7fDcFD2 To Fake_Phishing7268

Scroll for more

Figure 3.4: Example of Ice Phishing via free sale. Data source [90]

When a private key is compromised, a common behavior observed is the immediate sale of the token to one of the existing bids, followed by the transfer of the proceeds from the sale to an external account controlled by the attacker. Figure 3.5 illustrates an example of such transactions.



From: 0xD1a2476dE851186E5F7415bbE235C780D8E90ecb
Interacted With (To): 0x00000000006c3852cbEf3e08E8dF289169EdE581 (Seaport 1.1)

ERC-20 Tokens Transferred: 3
- From 0xed2ab4...eB8c7236 To Yuga Labs For 0.343434 ($620.67) Wrapped Ethe... (WETH...)
- From 0xed2ab4...eB8c7236 To Yuga Labs For 1.373736 ($2,482.68) Wrapped Ethe... (WETH...)
- From 0xed2ab4...eB8c7236 To 0xD1a247...D8E90ecb For 66.96963 ($121,030.86) Wrapped Ethe... (WETH...)

ERC-721 Tokens Transferred: ERC-721 Token ID [5917] BoredApeYach... (BAYC)
From 0xD1a247...D8E90ecb To 0xed2ab4...eB8c7236

From: 0xD1a2476dE851186E5F7415bbE235C780D8E90ecb
Interacted With (To): 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2 (Wrapped Ether)

ERC-20 Tokens Transferred: From 0xD1a247...D8E90ecb To 0x767263...D8f68444 For 82.4333095 ($149,073.22) Wrapped Ethe... (WETH...)

Figure 3.5: Example of transactions executed by an attacker who gained access to the victim's private key. Data source [92], [93]

The intention behind using this approach was to identify transactions that follow the specified patterns, manually examine them, and iteratively refine the code until achieving an automated mechanism with a desirable level of accuracy. However, only a trial version was developed due to the API's call rate limitations, making it challenging to fetch a high volume of transactions within a reasonable timeframe. As stated on their website [94], there is a specified limit of 5 calls per second in the free plan. However, during code execution, the observed limit was 100 calls per minute, as depicted in Figure 3.6 that illustrates the calls made per minute after an hour of running the program. This discrepancy could be attributed to other operations performed by the script, network latency, server load, among other factors. Since the time required to discover a significant number of cases became impractical, the decision was made to collect the data manually.

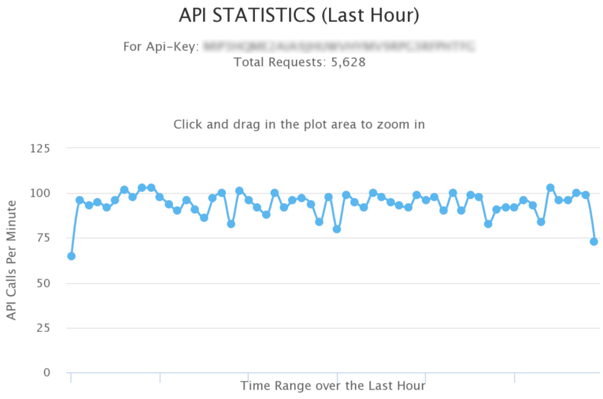


Figure 3.6: API calls per minute after an hour running the Python script

3.3.2 Manual collection

Chapter 4

Statstical modeling

4.1 Claim frequency

4.2 Claim severity

Chapter 5
Results

5.1 Estimation of the overall policy cost

5.2 Statistical significance

5.3 Risk prevention measures

Chapter 6
Future work and conclusion

Chapter 7
Time management and budgeting

Chapter 8

Comments on LaTeX references

If you want to know more about LaTeX there is a (free) manual at [95]. For more specific questions, it is recommended to have a look at the forum StackExchange [96], where the most common questions already have answers. All official packets can be found, and downloaded, from CTAN [97]. Finally, for the hardcore programmer who thinks LaTeX is a bit inflexible, I can recommend the TeX introduction in [98].

For questions about how you should do to get your imported graphics as you want, have a look at [99]. If you instead want to do the images inline from the TeX code you are recommended to use TikZ [100]. However, it is known to have a relatively high learning threshold.

Group	Test 1	Test 2
A	253	54
B	636	33

Table 8.1: A nice table.

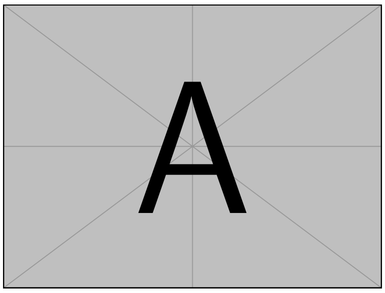


Figure 8.1: Image A

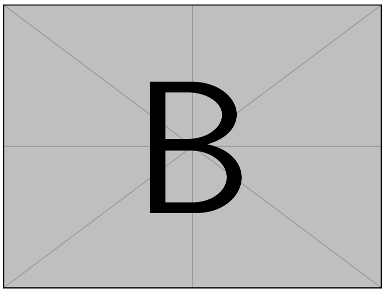


Figure 8.2: Image B. It can also be a long caption even if the space is narrow.

References

[1] "Introduction to Web3", ethereum.org. https://ethereum.org/en/web3/ (accessed Mar. 15, 2023).

[2] him.eth [@himgajria], Web 1: Read Web 2: Read-Write Web 3: Read-Write-Own, *Twitter*, May. 29, 2020. Available: https://twitter.com/himgajria/status/1266415636789334016 (accessed Mar. 15, 2023)

[3] D. Tapscott, *How the blockchain is changing money and business.* (Sep. 16, 2016). Accessed: Mar. 21, 2023. [Online video]. Available: https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Oct. 31, 2008. Accessed: Mar. 22, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] "Byzantine Fault Tolerance Explained.", academy.binance.com. https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained (accessed Mar. 23, 2023).

[6] M. Palatinus, P. Rusnak, A. Voisine and S. Bowe, "Mnemonic code for generating deterministic keys", GitHub repository, Sept. 10, 2013. Available: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki. (accessed: Mar. 25, 2023)

[7] P. Wuille, "Hierarchical Deterministic Wallets", GitHub repository, Feb. 11, 2012. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki. (accessed: Mar. 25, 2023)

[8] M. Palatinus, P. Rusnak, "Multi-Account Hierarchy for Deterministic Wallets", GitHub repository, Apr. 24, 2014. Available: https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki. (accessed: Mar. 25, 2023)

[9] "What Is a Blockchain Consensus Algorithm?" academy.binance.com. https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm (accessed Mar. 26, 2023).

[10] "Bitcoin Energy Consumption Index." digiconomist.net. https://digiconomist.net/bitcoin-energy-consumption (accessed Mar. 26, 2023).

[11] "In Proof of Stake, what is the hash value parameter in randomized block select?" ethereum.stackexchange.com. https://ethereum.stackexchange.com/questions/126504/in-proof-of-stake-what-is-the-hash-value-parameter-in-randomized-block-select (accessed: Mar. 29, 2023).

[12] Slance. *What is Proof of Stake - Explained in Detail (Animation).* (Nov. 23, 2021). Accessed: Mar. 29, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=YudpU58uYuM&ab_channel=Slance

[13] "PROOF-OF-STAKE (POS)." ethereum.org. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed Mar. 29, 2023).

[14] "Pool Distribution." btc.com. https://btc.com/stats/pool?pool_mode=year (accessed Mar. 29, 2023).

[15] "Ethereum's energy expenditure." ethereum.org. https://ethereum.org/en/energy-consumption/ (accessed Mar. 29, 2023).

[16] V. Buterin "On Public and Private Blockchains" blog.ethereum.org. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains (accessed Mar. 31, 2023).

[17] B. Crozier, Speaker "How Allianz took a blockchain platform from pilot to 1 million transactions," *CIO Priorities 2022*, 2022. Info-Tech Research Group [Podcast]. Available: https://www.infotech.com/research/how-allianz-took-a-blockchain-platform-from-pilot-to-1-million-transactions. [Accessed Apr. 19, 2023].

[18] "Layer 2," Ethereum.org, [Online]. Available: https://ethereum.org/en/layer-2/. [Accessed: Apr. 21, 2023].

[19] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/. [Accessed: Apr. 20, 2023].

[20] "Ethereum Virtual Machine (EVM)," ethereum.org, 2021. [Online]. Available: https://ethereum.org/en/developers/docs/evm/. [Accessed: Apr. 20, 2023].

[21] A. Hamilton, "The Beginning Of NFTs - A Brief History Of NFT Art," Mar. 6, 2023. [Online]. Available: https://www.zenofineart.com/blogs/news/the-beginning-of-nfts-a-brief-history-of-nft-art. [Accessed: Apr. 23, 2023].

[22] M. Rosenfeld, "Overview of Colored Coins," Dec. 4, 2012. [Online]. Available: https://bitcoil.co.il/BitcoinX.pdf. [Accessed: Apr. 20, 2023].

[23] K. McCoy, "Quantum", May. 3, 2014, [Online image]. Available: https://ipfs.io/ipfs/QmPkJoCk1vZ7wGMhfDer9fwpQtRGWwPn7NrocaCn7JS2SM. [Accessed Apr. 22, 2023].

[24] "Details for Transaction fa8b9a6ad4d266f...d3bb48f8d", chainz.cryptoid.info. Available: https://chainz.cryptoid.info/nmc/tx.dws?1217290.htm. [Accessed: Apr. 22, 2023].

[25] E.Lee, "Lawsuit Against Sotheby's and Kevin McCoy Dismissed," nftnow.com. Mar. 21, 2023. [Online]. Available: https://nftnow.com/news/lawsuit-against-sothebys-and-kevin-mccoy-dismissed/. [Accessed: Apr. 22, 2023].

[26] "Contract 0xE81a4543...9E578F8771D9 ", etherscan.io. Available: https://etherscan.io/address/0xe81a45439ff9bc5841202ce4b2049e578f8771d9. [Accessed: Apr. 23, 2023].

[27] "CryptoPunks," larvalabs.com. Available: https://www.larvalabs.com/cryptopunks. [Accessed: Apr. 23, 2023].

[28] W. Entriken , D. Shirley, J. Evans and N. Sachs, "Non-Fungible Token Standard", GitHub repository, Jan. 24, 2018. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md. (accessed: Apr. 24, 2023)

[29] Larvalabs, "CryptoPunks Composite Image," [Online image]. Available: https://www.larvalabs.com/public/images/cryptopunks/punks.png. [Accessed: Apr. 23, 2023].

[30] CryptoPunks [@cryptopunksnfts], The Cryptopunks are now fully on chain!, *Twitter*, Aug. 18, 2021. Available: https://twitter.com/cryptopunksnfts/status/1428099416326557696 (accessed Apr. 23, 2023)

[31] M. Marlinspike, "My first impressions of web3," moxie.org. Available: https://moxie.org/2022/01/07/web3-first-impressions.html (accessed May 06, 2023)

[32] Takens Theorem, "Souls of Immortal NFTs," medium.com. Available: https://medium.com/etherscan-blog/souls-of-immortal-nfts-de212a840de5 (accessed May 06, 2023)

[33] dom [@dhof], the michelin guide to “”on chain”” nfts, *Twitter*, Jun. 30, 2021. Available: https://twitter.com/dhof/status/1410060181849919489 (accessed May 06, 2023)

[34] IPFS, "How IPFS Deals With Files - IPFS Camp Workshop", *YouTube*, Sep. 17, 2019. Available: https://www.youtube.com/watch?v=Z5zNPwMDYGg&ab_channel=IPFS. (accessed: Apr. 26, 2023)

[35] IPFS, "How IPFS Deals With Files - IPFS Camp Workshop", *YouTube*, Sep. 17, 2019. Available: https://www.youtube.com/watch?v=Z5zNPwMDYGg&ab_channel=IPFS. (accessed: Apr. 26, 2023)

[36] "How IPFS works," docs.ipfs.tech. Available: https://docs.ipfs.tech/concepts/how-ipfs-works/#subsystems-overview. (accessed: Apr. 26, 2023) https://www.youtube.com/watch?v=Z5zNPwMDYGg&ab_channel=IPFS. (accessed: Apr. 26, 2023)

[37] "What is calldata?," ethereum.stackexchange.com. Available: https://ethereum.stackexchange.com/questions/52989/what-is-calldata. (accessed: May 06, 2023)

[38] "0xmons v2 Cthulhu: On-chain Encoding," blog.0xmons.xyz. Available: https://blog.0xmons.xyz/79081566310. (accessed: May 06, 2023)

[39] "0xDEAFBEEF | About," deafbeef.com. Available: https://www.deafbeef.com/about.htm. (accessed: May 06, 2023)

[40] "Smart contract details 0xd754937672300Ae6708a51229112dE4017810934," etherscan.io. Available: https://etherscan.io/address/0xd754937672300ae6708a51229112de4017810934#readContract. (accessed: May 06, 2023)

[41] S. de la Rouviere, "Flavours of On-Chain SVG NFTs on Ethereum," blog.simondlr.com. Available: https://blog.simondlr.com/posts/flavours-of-on-chain-svg-nfts-on-ethereum. (accessed: May 06, 2023)

[42] "Smart contract details 0x960b7a6bcd451c9968473f7bbfd9be826efd549a," etherscan.io. Available: https://etherscan.io/address/0x960b7a6bcd451c9968473f7bbfd9be826efd549a#readContract. (accessed: May 06, 2023)

[43] R. Delgado, "NFTMetadataStorage.xlsx" GitHub repository, May 06, 2023. Available: https://github.com/rdf5/insurancenft/blob/main/NFTMetadataStorage.xlsx. (accessed: May 06, 2023)

[44] "Collection stats," opensea.io. Available: https://opensea.io/rankings?sortBy=total_volume. (accessed: May 06, 2023)

[45] nick.eth [@nicksdjohnson], Everyone is making NFTs that generate their artwork..., *Twitter*, Aug. 27, 2021. Available: https://twitter.com/nicksdjohnson/status/1431144024052690944 (accessed May 06, 2023)

[46] "CC0 "No Rights Reserved"," creativecommons.org. Available: https://creativecommons.org/share-your-work/public-domain/cc0/. (accessed: May 06, 2023)

[47] "Smart contract details 0xe8d8c0a6f174e08c44ab399b7ce810bc4dce096a," etherscan.io. Available: https://etherscan.io/address/0xe8d8c0a6f174e08c44ab399b7ce810bc4dce096a#readContract. (accessed: May 06, 2023)

[48] "Smart contract details 0xb1bEfc9E7B76C1e846EBBf3e6E1Ab029C86e7435," etherscan.io. Available: https://etherscan.io/address/0xb1bEfc9E7B76C1e846EBBf3e6E1Ab029C86e7435#readContract. (accessed: May 06, 2023)

[49] "Moonbirds art, preserved on the Ethereum blockchain forevermore," proof.xyz. Available: https://www.proof.xyz/moonbirds/in-chain. (accessed: May 06, 2023)

[50] "Smart contract details 0x94cB646dD34b3B0fF7C116208F7f7fF7Ac216079," etherscan.io. Available: https://etherscan.io/address/0x94cB646dD34b3B0fF7C116208F7f7fF7Ac216079#readContract. (accessed: May 07, 2023)

[51] "Metadata Standards," docs.opensea.io. Available: https://docs.opensea.io/docs/metadata-standards. (accessed: May 08, 2023)

[52] Hyperloot # 1 jpg file, metadata.hyperlootproject.com. Available: https://images.hyperlootproject.com/nft/1.jpg. (accessed: May 06, 2023)

[53] "Cryptokitties sales history," kittyhelper.co. Available: https://kittyhelper.co/sales-history/?period=custom&d1=2017-12-01&d2=2017-12-31&sort=1. (accessed: Apr. 27, 2023)

[54] "Tradition and Innovation Collide: Decentraland Metaverse Fashion Week 2023," decentraland.org. Feb. 27, 2023. Available: https://decentraland.org/blog/announcements/tradition-and-innovation-collide-decentraland-metaverse-fashion-week-2023. (accessed: Apr. 29, 2023)

[55] "Decentraland EST 4339," nonfungible.com. Available: https://nonfungible.com/market-tracker/decentraland/EST/4339. (accessed: Apr. 29, 2023)

[56] "Opensea - Our Story," opensea.io. Available: https://opensea.io/abou. (accessed: May 08, 2023)

[57] "NFT Marketplaces," dappradar.com. Available: https://dappradar.com/nft/marketplaces?period=all. (accessed: May 08, 2023)

[58] "Beeple (b. 1981), Everydays: The First 5000 Days," onlineonly.christies.com. Available: https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924. (accessed: Apr. 29, 2023)

[59] "Blockchains by NFT Sales Volume," cryptoslam.io. Available: https://www.cryptoslam.io/blockchains. (accessed: May. 1, 2023)

[60] P. Smith, Presenter J. Krcmar, Speaker, "Session 2," *NFT Educational Series*, Jun. 30, 2021. Institutes RiskStream Collaborative [Podcast]. Available: https://vimeo.com/572091172. (accessed: May. 1, 2023)

[61] Mimecast, "The State of Email Security 2022". Available: https://www.mimecast.com/state-of-email-security/. (accessed: May. 2, 2023)

[62] R. de Best, "Total value of cryptocurrency lost to and recovered from theft and other attacks between March 2020 and February 2022," Feb. 3, 2022. Available: https://www.statista.com/statistics/1285057/crypto-theft-size/. (accessed: May. 2, 2023)

[63] E. Arda, M. Nadini, C. De Pow and T. Annison, "NFTs and Financial Crime". Available: https://hub.elliptic.co/reports/nfts-and-financial-crime/. (accessed: May. 2, 2023)

[64] B. Lindrea, "Crypto insurance a 'sleeping giant' with only 1% of investments covered," cointelegraph.com. Sep. 12, 2022. Available: https://cointelegraph.com/news/crypto-insurance-a-sleeping-giant-with-only-1-of-investments-covered. (accessed: May. 2, 2023)

[65] Fortune Business Insights, "Global Cryptocurrency Market, Insights and Forecasts, 2017-2028," fortunebusinessinsights.com. Available: https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149. (accessed: May. 2, 2023)

[66] P. Ricard, J. Zwick, U. Koyluoglu, A. Flint and C. Freeman, "Will Web3 Reinvent Insurance?," oliverwyman.com. Available: https://www.oliverwyman.com/our-expertise/insights/2022/jul/oliver-wyman-will-web3-reinvent-insurance.html. (accessed: May. 3, 2023)

[67] Coinbase, "Insurance Coverage," coinbase.com. Available: https://www.coinbase.com/legal/insurance. (accessed: May. 3, 2023)

[68] Chainlink, "What Is a Blockchain Oracle?," chain.link. Available: https://chain.link/education/blockchain-oracles. (accessed: May. 3, 2023)

[69] Coinbase, "Insurance Coverage," coinbase.com. Available: https://www.coinbase.com/legal/insurance. (accessed: May. 3, 2023)

[70] J. Kagan, "Mutual Insurance Company: Definition and How They Invest," investopedia.com. Available: https://www.investopedia.com/terms/m/mutual-insurance-company.asp. (accessed: May. 3, 2023)

[71] Nexus Mutual, "Documentation," nexusmutual.io. Available: https://docs.nexusmutual.io/. (accessed: May. 3, 2023)

[72] K. Petrie, "Nexus Mutual is now using Chainlink's price reference data contracts for decentralized valuations of the multi-currency capital pool," medium.com. Available: https://medium.com/nexus-mutual/nexus-mutual-is-now-using-chainlinks-price-reference-data-contracts-for-decentralized-valuations-6a62c5d4e030. (accessed: May. 3, 2023)

[73] Nexus Mutual, "Smart Contracts Details," nexusmutual.io. Available: https://api.nexusmutual.io/sdk/. (accessed: May. 3, 2023)

[74] Nexus Mutual, "Cover Underwritten and Claims Paid," nexusmutual.io. Available: https://nexusmutual.io/. (accessed: May. 3, 2023)

[75] C. Seifert, "'Ice phishing' on the blockchain," microsoft.com. Available: https://www.microsoft.com/en-us/security/blog/2022/02/16/ice-phishing-on-the-blockchain/. (accessed: May 10, 2023)

[76] jeffnicholas.eth [@_jeffnicholas_], Today has been rough., *Twitter*, Aug. 25, 2021. Available: https://twitter.com/_jeffnicholas_/status/1430323445057744897 (accessed May 09, 2023)

[77] A. Sarkar, "OpenSea planned upgrade stalls as phishing attack targets NFT migration," cointelegraph.com. Available: https://cointelegraph.com/news/opensea-planned-upgrade-stalls-as-phishing-attack-targets-nft-migration. (accessed: May 09, 2023)

[78] D. Barda, R. Zaikin and O. Vanunu, "Check Point Research Prevents Theft Of Crypto Wallets On Opensea, The World's Largest NFT Marketplace," research.checkpoint.com. Available: https://research.checkpoint.com/2021/check-point-research-prevents-theft-of-crypto-wallets-on-opensea-the-worlds-largest-nft-marketplace/. (accessed: May 10, 2023)

[79] quit [@0xQuit], Today, bored ape holder "s27" lost their bubble gum ape and matching mutants, *Twitter*, Apr. 5, 2022. Available: https://twitter.com/0xQuit/status/1511198290565509120 (accessed May 10, 2023)

[80] "Part 3: Set your drop earnings," docs.opensea.io. Available: https://docs.opensea.io/docs/part-3-set-your-drop-earnings. (accessed: May 11, 2023)

[81] "What are OpenSea's fees?," support.opensea.io. Available: https://support.opensea.io/hc/en-us/articles/14068991090067-What-are-OpenSea-s-fees-. (accessed: May 11, 2023)

[82] PeckShieldAlert [@PeckShieldAlert], It appears that @opensea has a front-end issue and the exploiter gained about 332 Ether, *Twitter*, Jan. 24, 2022. Available: https://twitter.com/PeckShieldAlert/status/1485547426467364864 (accessed May 11, 2023)

[83] N. Bambysheva and M. G. Santillana, "Over $3 Billion Stolen In Crypto Heists: Here Are The Eight Biggest," forbes.com. Available: https://www.forbes.com/sites/ninabambysheva/2022/12/28/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/?sh=3cb28490699f. (accessed: May 11, 2023)

[84] A. Bhuptani "The Interoperability Trilemma," blog.connext.network. Available: https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17. (accessed: May 11, 2023)

[85] Amber Group, "Reproducing the $APE Airdrop Flash Loan Arbitrage/Exploit," medium.com. Available: https://medium.com/amber-group/reproducing-the-ape-airdrop-flash-loan-arbitrage-exploit-93f79728fcf5. (accessed: May 12, 2023)

[86] "Transaction Details," etherscan.io. Available: https://etherscan.io/tx/0xeb8c3bebed11e2e4fcd30cbfc2fb3c55c4ca166003c7f7d319e78eaab9747098. (accessed: May 12, 2023)

[87] J. Niset, "Argent Smart Wallet Specification", GitHub repository, Apr. 23, 2021. Available: https://github.com/argentlabs/argent-contracts/blob/develop/specifications/specifications.pdf. (accessed: May 14, 2023)

[88] "Ethereum Chain Full Sync Data Size", ycharts.com. Available: https://ycharts.com/indicators/ethereum_chain_full_sync_data_size (accessed: May 16, 2023)

[89] "Transaction Details," etherscan.io. Available: https://etherscan.io/tx/0xafc951c5aadc63dbff23ca7b628b36d9faf35ae38b484f91db1134b5558cb01d

[90] "Transaction Details," etherscan.io. Available: https://etherscan.io/tx/0xd82484e970a1a0a065f4e710da84990df5cee35e2305fcf88db44271a24c5ceb

[91] Serpent [@Serpent], Analysis of how a scammer stole 14 BAYCs worth over 852 ETH, *Twitter*, Dec. 17, 2022. Available: https://twitter.com/Serpent/status/1604074440941506560 (accessed May 17, 2023)

[92] "Transaction Details," etherscan.io. Available: https://etherscan.io/tx/0xf1877ae321b3e9dbf871d4f026df434fe12fc1ad3f64ce61e97789bc2e33ad07 (accessed: May 17, 2023)

[93] "Transaction Details," etherscan.io. Available: https://etherscan.io/tx/0xd554a83a3e4ff332620048c747647051d6d01ed465dd84ba55a2b9d918b80cc1 (accessed: May 17, 2023)

[94] "Etherscan API Plans", etherscan.io. Available: https://etherscan.io/apis (accessed: May 17, 2023)

[95] T. Oetiker, H Partl, I Hyna, and E. Schlegl, *A (Not So) Short Introduction to LATEX2e*, www.ctan.org/tex-archive/info/lshort/english/

[96] {TEX} StackExchange, tex.stackexchange.com/

[97] The Comprehensive TEX Archive Network, www.ctan.org/

[98] P. Abrahams, K. Hargreaves, and K. Berry, *TeX for the Impatient*, savannah.gnu.org/projects/teximpatient/

[99] K. Reckdahl, *Using Imported Graphics in LaTeX and pdfLaTeX*, www.ctan.org/tex-archive/info/epslatex/english

[100] T. Tantau, *The TikZ and PGF Packages*, www.bu.edu/math/files/2013/08/tikzpgfmanual.pdf. Warning: 400+ pages.

Appendix A
Some extra material

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

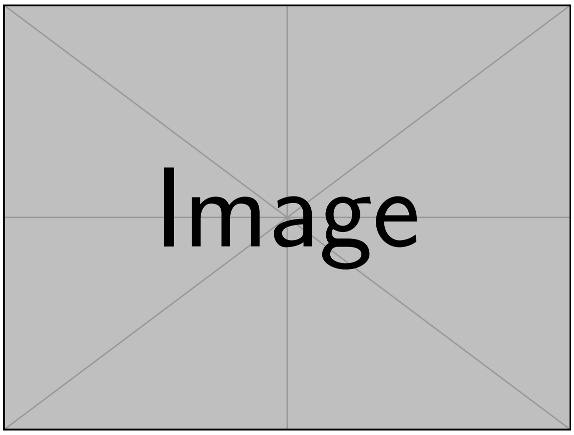


Figure A.1: A picture or table in the appendix is numbered accordingly.