Towards a Landscape of Attack Vectors against Users in the NTF Ecosystem

1st Daniel Köhler
Internet Technologies and Systems
Hasso-Plattner-Institute
Potsdam, Germany
daniel.koehler@hpi.de

2nd Christoph Meinel
Internet Technologies and Systems
Hasso-Plattner-Institute
Potsdam, Germany

***Abstract*—The Internet and the Web have impacted and influenced the world as we know it today. Currently, we are on the verge of new development: Web3, to be interpreted as a decentralized, online ecosystem.**

Backbone technology of the web3 is building on lessons learned from the development of the Internet in terms of IT security technologies by incorporating security thoughts closely into the technology design. The current first steps into web3, namely by exploring the use of Non-Fungible Tokens (NFTs), already show technical feasibility and explore user adoption. However, plenty of prominent examples from the past months show that users of the NFT ecosystem are a central target for attacks. This work proposes a foundation for further research by outlining an NFT ecosystem landscape. The overview incorporates and highlights connections between users, resources on the traditional Internet, and web3-based systems. Building on that landscape overview, we present a first approach to categorizing security threats and attack vectors against users. Our analysis thereby shows starting points to investigate and discuss solutions enabling a safe web3.

***Index Terms*—security, risks, attack vectors, nft, blockchain**

I. Introduction

Over the past years, the internet has become increasingly fragmented, controlled and less secure [1]. Modern, decentralized technologies attempt to reinvent the free and open internet utopia. As such, Blockchain-based systems and distributed ledgers are currently being widely developed as one of the Web3 technologies. Particularly Non-Fungible Token (NFT) systems claim to solve several problems imposed by untrusted communication partners in the digital world.

We consider NFT technologies and infrastructures to currently be in a state of a feasibility study regarding infrastructure and usability. Projects selling digital art, prominently pictures, to other users in the ecosystem dominate the current phase. Similarly, artists experiment with adopting NFT technologies for digital ownership in fields of, e.g., music and digital properties.

In the current feasibility study phase of Non-Fungible-Tokens on blockchain solutions, we foster secure adoption by providing a foundation of threats and attack vectors against ecosystem users. Our contributions are two-fold:

1) **Ecosystem Model**: we build upon previous models, providing a more detailed and publicly editable landscape overview. The landscape presented in Section III spans users and resources both in the traditional internet and across blockchain solutions.
2) **Threat Vectors**: Creating a secure NFT ecosystem requires industry, community, and research to develop resilient infrastructure across the ecosystem. In Section IV, we categorize eight (8) main attack vectors against users into *Phishing*, *Misleading Advertisement*, and *Inherent Issues in the Ecosystem*.

II. Background and Methodology

In the past years, several terms were coined for the different phases of the internet. The most prominent ones are the classification of the different phases of the Web into Web 1.0, 2.0 [2], and 3.0 [3], [4].

The term *Web3* was coined by Gavin Wood in 2014 [5] and refers to a novel interpretation of the web, the *decentralized* or *distributed* web [6]. Web3 operates on and uses blockchain technologies to decentralize information and systems. Gavin Wood recently reiterated that decentralized technologies are the only hope of preserving liberal democracy [7].

Blockchain-or Distributed-Ledger-technologies describe a set of technologies that allow storing and distributing data between multiple participants in a network so that each participant has a copy of the correct data. Changes to or deleting the data shall only be possible if the peers agree on a consensus.

A. Ethereum Blockchain

Blockchain technologies essentially offer infrastructure, technology, and environments for communication and exchange between participants in a network without any trusted third party that controls the network or the infrastructure. As such, the Bitcoin application [8] has initially fostered a great interest as a network for money exchange and transfer without a central ledger such as a bank. Blockchain networks implement various consensus protocols such as Proof of Work or Proof of Stake, which serve as the underlying security mechanism [9].

Ethereum is the leading distributed ledger technology for the use and application of smart contracts, and decentralized apps [10]. As such, Ethereum is the first widely-adopted network that operates by executing code in the so-called Ethereum

Virtual Machine (EVM) with the same security and trust requirements initially imposed on Blockchain technologies: no central and no trusted third party [11].

B. Methodology

To describe, identify and understand the problems surrounding the NFT ecosystem in its current state without influencing users' impressions, we chose to pursue an observational research approach [12]. Furthermore, to the best of our knowledge, hardly any previous research is available that properly documents or structures Security aspects in the NFT ecosystem. We, therefore, approached the problem and observation in the spirit of Grounded Theory without any prior hypothesis [13].

During our research, over the past months, we investigated various large-scale NFT communities (some of which consisted of more than 100.000 users)[1]. Our initial observations provided a relatively good understanding and helped us develop our model of the NFT landscape (c.f. Section III). We further started to interact, e.g., by exchanging messages with other users, project managers, or victims of previous attacks. During that time, we derived the first ideas for categorizing attacks in the field.

Further, several channels in Discord servers and Twitter are disseminating security alerts throughout the community. Twitter has already become a significant community in the cybersecurity space, and we observe a similar trend in the field of NFTs. Most prominent accounts in the NFT twitter space (>150.000 followers) usually quickly continue to spread information and awareness on current issues and threats observed in relevant and current projects.

III. The NFT Ecosystem

Figure 1 depicts an overview of our interpretation of the NFT ecosystem. Our research focuses on threats against users in the NFT ecosystem. Users can be, e.g., investors, artists, or project managers. Independent of their role, all participants in the ecosystem usually own (at least) one cryptographic wallet[2].

Most projects we observed in the space organize around a central Discord server. These provide scalable spaces for like-minded people to interact. Discord servers usually create and build a community around an NFT project. As such, the discord servers often contain the source of truth for links to project webpages and NFT marketplaces.

In the lifecycle of a project, aside from some previous marketing and community-building efforts, the NFT project usually comes to life with the *mint* of the NFTs. The *mint* describes the initial connection of a digital asset into the blockchain. From our experience, the project website usually serves as a user-friendly interface for the particular *Smart Contract*. Users must connect their wallet to *mint* an NFT through a project webpage.

Smart Contracts are programs stored on the blockchain that run in predefined and publicly visible ways. Most smart contracts in the current state of the NFT communities are running on the Ethereum Blockchain. This is due to the larger community as well as the higher market capitalization of Ethereum (∼390B USD) against, e.g. Solana[3] (∼40B USD)[4]. Contracts running on the Ethereum Blockchain are written in Solidity.

When interacting with the Smart Contract, users usually transfer a set amount of, e.g., Ethereum (ETH) from their wallet to the smart contract to transfer a Non-Fungible Token. In most cases, ownership of the cryptographic private keys of the user's wallet will authenticate the user's interaction with smart contracts. In practice, a user interacting with a smart contract, independent of the proxy (such as the project webpage or an *NFT Marketplace*), will get a signing request (popup) which he has to confirm through his wallet.

NFT Marketplaces such as OpenSea offer exchange platforms for NFTs. They offer features such as *verified* collections, current statistics about trending collections or items, and features for offering or bidding on NFTs. When using an NFT marketplace, users usually connect their wallets to serve as the backbone of their profile in the marketplace.

In the marketplaces, users will usually see the first connection between the NFTs - cryptographic values on the blockchain - and the connected digital assets such as digital art. Projects generally host their digital art on other hosting services. Those hosting services can either be, e.g., the Interplanetary File System, a peer-to-peer hypermedia protocol for the web, or even outside the blockchain infrastructure such as, e.g., on Amazon Web Services.

A. Related Work on Security Threats in Web3

Other research has previously analyzed security threats in parts of the NFT Ecosystem and Web3. Wang et al. have presented a first technical report which assesses and presents challenges and opportunities of the NFT ecosystem on a high level [14]. Building upon that overview, further fellow researchers dove into different aspects of the NFT ecosystem in more detail.

Vulnerabilities in Smart Contracts Various fellow researchers have already assessed security concepts and aspects in the so-called *Smart Contracts*, the programs running on the Blockchains. Recently, Kushwaha et al. published a systematic review of the state of security vulnerabilities in such *Smart Contracts* [15]. Like traditional programming languages, smart contracts can show security vulnerabilities when not used properly. In their work, Kushwaha et al. identified three primary root causes for vulnerabilities in Smart Contracts: (1) The Solidity Programming Language, (2) The Ethereum Virtual Machine, and (3) The Ethereum Blockchain Design.

[1]Examples of observed communities: *Crypto Bull Society*, *Champs Only*, *Magic Mushroom Clubhouse*, *Bored Ape Yacht Club*, *Invisible Friends*, ...

[2]The cryptographic wallet can be compared with a traditional physical wallet, containing the identity and access information of the user. Wallets are available as Software wallets, often transferable across multiple devices or hardware wallets.

[3]Similarly to Ethereum, Solana is a blockchain infrastructure built for scalable, user-friendly apps, Website: https://solana.com

[4]Statistics taken from https://coinmarketcap.com in April 2022

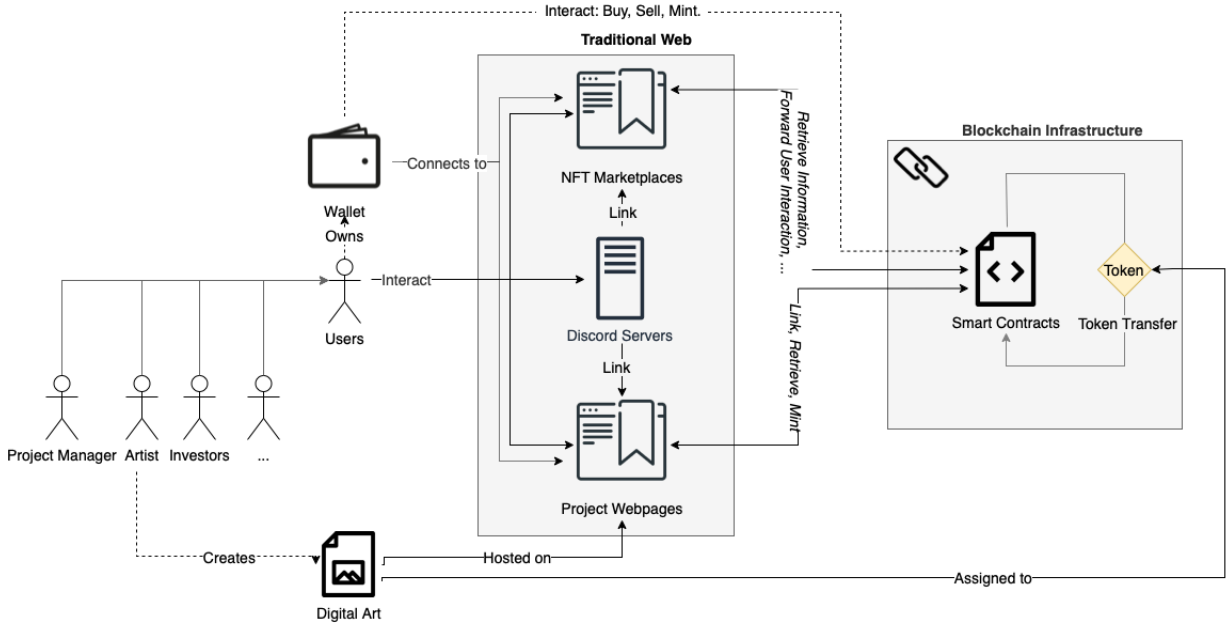

Fig. 1: Overview of the NFT Ecosystem including Users, Components from the Traditional Internet as well as Infrastructure in the Ethereum Blockchain

Researchers are invited to reuse and enhance our figure: <https://dkoehler.net/publications/NFT-Landscape-Overview.html>

The mentioned work provides a good overview of the technical vulnerabilities and solutions to those vulnerabilities.

Financial Issues in the NFT Ecosystem Das et al. provide a first deep dive into security and privacy issues in the NFT ecosystem [16]. In their work, they present a first overview of the NFT ecosystem. They perform a quantitative analysis using the APIs of the eight major NFT marketplaces.

Das et al. mainly focused on analyzing trading malpractices in NFT marketplaces and the dangers of financial nature these impose, such as tax evasion. The authors further developed models to detect common malpractices. To enrich the presented work, we provide the **User Perspective** on the ecosystem to identify another layer of problems, dangers, and attack vectors to solve and mitigate.

IV. Users' Security in the NFT Ecosystem

The NFT ecosystem has recently seen a significant boom favoring its feasibility test for future broader applications. We aim to foster the technical discussion about problems concerning users' security in the web3 technology. We present the following issues that each user is experiencing as a base ground for developing solutions to the problems. Generally, we formulate two ultimate goals of attackers, which they can achieve by various threat vectors or any combination of them:

1) Maliciously get control of somebody else's token; this could also be achieved by getting access to another user's wallet
2) Trick users into buying NFTs from dishonest, or illegitimate collections

A. T1 Phishing

Phishing attacks describe the attempt to gain sensitive information about a user by abusing social engineering tactics.

T1.1 Sending Faked Project Links One typical attack vector we observed is attackers using fake Twitter or Discord accounts to impersonate project owners or managers. Using such an account, frequently even with an identical profile picture, the attackers attempt to send malicious links to fake project webpages.

In most cases, we observed attackers using the traditional factor of urgency. Often, scammers lure users into supposedly private mints of NFTs, which only last for an hour. Users following these links will see a webpage that looks identical to the original project. Whenever the user connects his wallet to mint the project, we observed one of the following to occur:

1) The user could buy an NFT from a fake collection. In that case, the NFT can be considered worthless.
2) Interacting with the contract drains the user's wallet of any amount of cryptocurrency currently available in the wallet.
3) The user unknowingly provides the attackers with access to his wallet, enabling them to drain it and steal any NFTs currently in his wallet.

T1.2 Discord Account Takeovers An advanced form of T1.1 is phishing attacks by using highjacked accounts of users (usually with higher privileges) in discord servers. Attackers can obtain Those accounts by various attack vectors, which we omit in this work but range from weak passwords to phishing attacks for stealing users' credentials.

When attackers abuse such highjacked and trustworthy accounts, they have a higher chance of success when performing phishing attacks. Furthermore, with more elevated privileges such as those of a project's discord manager, attackers will be able to place faked project links inside the project's central and trusted resources. Such would be, e.g., the list of official project links, which - as previously outlined - serves as the primary connection between a project's Discord server and, e.g., the official webpage.

B. T2 Misleading Advertisement

Similar to advertisement campaigns in the traditional world, most NFT projects rely on users' traction and interest to promote quick sellouts during the minting phase of a project. In the past, we observed various methods of illegitimate and misleading advertisement:

T2.1 Fake Projects and Rug Pulls The intention of most misleading advertisement practices is to sell as many NFTs as possible through fake projects. Fake projects, often referred to as Rug Pulls, are projects that promise plenty of benefits or an excellent roadmap to their investors but never deliver those. The anonymity of the internet often helps dishonest project creators to disappear, leaving almost no traces once the project has been sold and they have received the money.

T2.2 Fake Airdrops To help (legitimate as well as dishonest) projects gain traction and sell out, project owners often airdrop[5] NFTs into wallets of reputable collectors. Many investors use data mining tools to crawl transactions and identify respected users who are supposedly invested in a project.

If a collector owns an NFT from a specific project, other investors could be likely to buy tokens from the same project as well. In combination with airdrops, however, they have not necessarily purchased the tokens but only received them airdropped into their wallet. Closer inspection will show facts for such behavior, such as that the collector has not paid for the NFT. However, the practice is sufficient to mislead a majority of users.

C. T3 Inherent Issues in the Ecosystem

The NFT ecosystem currently contains further issues which are not replications of traditional threats:

T3.1 Malicious Airdrops Besides airdrops used to promote new projects of any kind, airdrops can further impose an imminent security threat. Users who interact with airdropped tokens in their wallets will be required to sign the transaction. Actions that a user could perform are *unhiding* a token or transferring it to other wallets. Unhiding refers to importing airdropped NFTs into the public and visible wallet. Attackers could persuade users to interact with an airdropped token because it contains charming art, and they do not know better. Often, crypto wallets do not adequately show information on the requests to be signed[6]. Thereby the user could, e.g. provide access to his account to somebody else without intending to do so.

T3.2 Missing Trust Anchors One inherent issue in the NFT ecosystem is missing trust in the environment. While this is natural and expected by design in a Blockchain system, it states an essential factor of threat. The threat of missing trust reinforces or even enables previously mentioned threats such as *T1.1 Faked Project Links* or *T2.1 Fake Projects and Rug Pulls*. Often, founders of projects choose to dox themself, i.e., show their real identity, and thereby aim to generate trust with the community. Nevertheless, doxed creators are no guarantee of a successful or honest project. *Das et al.* also identified the missing verification of users, accounts, and smart contracts [16]. The inherent issue of trust in the ecosystem can only be faced by investors from the community looking out for red flags and being careful in what they invest. Coherently, the issue of the missing trust anchor could also be considered an issue of too much trust by investors in any project and too quickly providing leaps of faith to project owners.

T3.3 Miner Extractable Value (MEV) Attacks Traditionally, (Ethereum) miners process transactions in an order based on the transaction fee, gas, which is assigned to the transaction. However, miners are not obliged to follow the outlined principle. They can instead arbitrarily decide on the order of transactions in their block. This enables adversaries to re-order blocks and transactions to benefit themselves. MEV is considered the profit a miner can achieve by arbitrarily including, excluding, or re-order transactions [17], [18]. For users of the NFT ecosystem, MEV attacks can induce rising prices and unpredictability of transactions. Since first being outlined in 2019 by Klages et al. [18], MEV attacks are already being carried out to a great extent in the wild[7].

D. Traditional Security Threats

We acknowledge that many of the traditional threats we observe in the cybersecurity field translate to the NFT ecosystem. Examples of such are conventional phishing attacks, which can compromise NFT wallets. Similarly, we do not list, e.g., traditional malware gaining access over a device and thereby being able to access the cryptographic wallets on the device. Developments in the NFT ecosystem can only partly tackle such threats. One such solution could, e.g., be the use of hardware wallets.

V. Conclusion

We use the current phase of feasibility study of one central web3 technology, Non-Fungible Tokens (NFTs), to examine the ecosystem for security issues and threats against its users. The ecosystem model we created by observation and interaction with the community can serve as a foundation for future refinement, explanation, and improvement in the landscape. We evaluate the landscape and the inherent problems deriving eight major threats in three categories. Our discovered threats span the categories *Phishing*, *Misleading Advertisement*, and

[5]Airdropping: To send an NFT to a user's wallet without them actively initiating the transfer and without them paying for the token

[6]Metamask, a software wallet, has recently started improving on the UI for signing messages, now offering more details.

[7]The MEV Explore Tool shows statistics of MEV attacks as extracted from Ethereum transactions, available at https://explore.flashbots.net

Inherent Issues in the Ecosystem. As we learned from the internet, security principles must be followed and assessed throughout the development phase. Our highlighted threats shall enable developers, engineers, and the security community to issue, evaluate and solve security issues while the ecosystem is still being created. Thereby allowing us to create and experience a more secure and resilient future with web3.

REFERENCES

[1] N. Fick, J. Miscik, A. Segal, and G. M. Goldstein, "Confronting reality in cyberspace," Council on Foreign Relations, New York, NY, Tech. Rep. Independent Task Force Report No. 80, 2022.

[2] T. O'Reilly, "What is web 2.0," Online-Article, oreilly.com, September 2005, last accessed: April, 2022. [Online]. Available: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1

[3] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific american*, vol. 284, no. 5, pp. 34–43, 2001.

[4] B. Hiremath and A. Y. Kenchakkanavar, "An alteration of the web 1.0, web 2.0 and web 3.0: a comparative study," *Imperial Journal of Interdisciplinary Research*, vol. 2, no. 4, pp. 705–710, 2016.

[5] G. Wood, "Dapps: What web 3.0 looks like," Online-Article, gavwood.com, April 2014, last accessed: August, 2022. [Online]. Available: https://gavwood.com/dappsweb3.html

[6] S. Voshmgir, *Token Economy: How the Web3 reinvents the Internet*. Token Kitchen, 2020, vol. 2.

[7] G. Edelman, "The father of web3 wants you to trust less," Online-Article, wired.com, November 2021, last accessed: April, 2022. [Online]. Available: https://www.wired.com/story/web3-gavin-wood-interview/#main-content

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[9] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[10] C. Dannen, *Introducing Ethereum and solidity*. Springer, 2017, vol. 1.

[11] V. Buterin *et al.*, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[12] P. Foster, "Observational research," *Data collection and analysis*, pp. 57–93, 1996.

[13] B. G. Glaser and A. L. Strauss, *The discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

[14] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-fungible token (nft): Overview, evaluation, opportunities and challenges," *arXiv preprint arXiv:2105.07447*, 2021.

[15] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, 2022.

[16] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the nft ecosystem," *arXiv preprint arXiv:2111.08893*, 2021.

[17] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," *arXiv preprint arXiv:1904.05234*, 2019.

[18] A. Klages-Mundt, D. Harz, L. Gudgeon, J.-Y. Liu, and A. Minca, "Stablecoins 2.0: Economic foundations and risk-based models," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020, pp. 59–79.