



Frankfurt University of Applied Sciences

–Faculty of Computer Science and Engineering–

Using Non-Fungible Tokens to Track User Data Across Websites

A Supplementary Method to Cookies

Research Projekt - Winter Semester 2022/23

Submitted by

Hendrik Gruber

Matriculation Number: 1458240

Advisor : Prof. Gabriela Alves Werb, Ph.D.

DECLARATION

I hereby assure that I wrote the present work independently and that I did not use any other sources than those given in the bibliography.

All passages that are taken verbatim or correspondingly from published or not yet published sources are marked as such.

The drawings or images in this work were created by myself or provided with a corresponding source reference.

This work has not been submitted to any other examination authority in the same or a similar form.

Frankfurt, 10.02.23

Hendrik Gruber

ABSTRACT

Lorem ipsum ...

CONTENTS

1	INTRODUCTION	1
1.1	Motivation	1
1.2	Goals and Overview	1
2	BACKGROUND INFORMATION - COOKIES	2
2.1	Cookies	2
2.2	Tracking User Data	2
2.3	Privacy and Policies	2
3	PROBLEM STATEMENT	4
4	BACKGROUND INFORMATION - NON-FUNGIBLE TOKENS	5
4.1	Web3	5
4.2	Blockchain	5
4.3	Smart Contracts	6
4.4	Non-Fungible Tokens	6
4.5	Cryptocurrency Wallets	6
5	RELATED WORK AND MARKET PRODUCTS	8
5.1	Current State of the Art	8
5.2	Related Work	8
5.2.1	Cookies	8
5.2.2	NFTs and Web3	8
5.3	Current Market Products	8
5.3.1	MetaMask	9
5.3.2	Wallet Connect	10
6	METHODOLOGY	11
6.1	Example Case - Online Stores and Single Sign-On	11
6.2	Public Wallet Address	11
6.3	Further Obtainable Data	12
6.4	Example of Programmatically Obtaining Information Via a Wallet	13
7	RESULTS AND DISCUSSION	15
7.1	Results	15
7.2	Problems	15
7.2.1	Quality of Data	15
7.2.2	Privacy - Sharing Your Wallet's Content	15
7.2.3	High Entry Barrier	15
7.2.4	High Gas Prices	16
7.3	Application Potential	16
7.4	Discussion	16
8	CONCLUSION AND FUTURE WORK	17
8.1	Conclusion	17
8.2	Future Work and Path Forward	17
	BIBLIOGRAPHY	18

ACRONYMS

API Application Programming Interface

dApp Decentralized Application

NFT Non-Fungible Token

SSO Single Sign-On

INTRODUCTION

Non-Fungible Tokens (NFTs) have gained popularity over the years with the rise of cryptocurrencies (todo: citation). Although it is unclear in which direction the future of the internet is heading, it can be speculated that the next iteration of the web, named Web3, will be focused on decentralized technologies such as blockchain. While the current internet is based on user-generated content, Web3 will be based on decentralized apps (dApps), and will run on peer-to-peer networks instead of central servers.

1.1 MOTIVATION

With NFTs being brought to light by recent trends, it is a very current and hot topic. NFTs have commonly being traded as a financial investment in their early years. The most prominent example being the Bored Apes Yacht Club, which has a volume of *todo* as of January 2023 (todo citation). This and many other examples go to show that there is a general interest in this up and coming technology.

Beyond financial investments, NFTs may also see potential use cases in areas of tracking user data. This is possible by the very nature of blockchain technology.

1.2 GOALS AND OVERVIEW

The goal of this paper is to analyze to what degree and in what manner NFTs can be utilized to track user data in the web. Similar to how cookies are currently used to track users across websites.

This will be done by giving background information on cookies and their privacy issues in chapter 2. Afterwards, the problem statement will be elaborated on in chapter 3. This will allow for an introduction of the required technical concepts of Web3 in chapter 4. Chapter 5 will then give an overview of current literature and market products in the areas of cookies and NFTs. Chapter 6 will then take a look at how NFTs can be leveraged in order to gain private information about a user and make content recommendations, similar to how cookies are able to do so. The results will then be discussed in chapter 7. This paper will be concluded in chapter 8 with a conclusion and a look into possible future research directions.

BACKGROUND INFORMATION - COOKIES

Intro sentence

2.1 COOKIES

Cookies are an easy way for websites to save the state or session of a user. In other words, cookies make it possible to create stateful web applications. This is done while browsing a website by sending information back and forth between the client and server. This information is saved as a simple text-file within the user's browser and contains a variety of arbitrary information. [1]

By saving cookies, the server knows details about the user's session such as who is currently logged in or what items are in the user's shopping cart. Thus, a user does not have to log in anew every time they visit the same website. With this information, a profile of the individual user is created and stored within the cookie. [1]

2.2 TRACKING USER DATA

It is clear how information about a state or session can be saved in a browser, but how does that allow for third parties to identify and track the current user?

Third parties, such as Facebook or Google, are able to display personalized ads on the website a user is currently visiting by utilizing cookie syncing. With this method, domains assign an ID to a user, which is then passed between domains. [2]

2.3 PRIVACY AND POLICIES

Gathering users' information in ways that they are not aware of begs the question if this is legal and what policies exist in order to save users of unwanted tracking.

A study from 2009 showed that 66% of Americans do not want to have targeted ads based on the information attained by being tracked. More so, when users were made aware of how the information was attained, 73% - 86% of users rejected personalized ads. [3]

This study exemplifies that typical users do not want to have detailed information of them tracked and used for advertising. Tracking and labeling users in ways that they do not understand is deemed to be unethical. However, advertisers argue that this allows them to give users what they want: personalized advertisements rather than generic ones. [3]

*Todo: More on privacy, since this is one of the main reasons to look for alternatives.
Can you find sources on how business models are being broken by privacy policies?*

PROBLEM STATEMENT

Creating individual profiles of users and utilizing these to display personalized ads lead to valuable business models. Creating laws and policies that make doing so more difficult can have shattering effects on a business's revenue.

The issue that this research paper analyzes is alternative methods to cookies to track users online behavior and collect their data. This will be done within the realm of Web3, which is built upon technologies such as blockchain and cryptocurrency wallets. Using Web3 technologies, it might be possible to replace or supplement cookies and continue to allow for detailed tracking of users. Even in an online world with more strict privacy policies and regulations.

The research question at hand is thus *How do NFTs and cryptocurrency wallets work as an alternative method to track users and collect their data? What are the pros and cons of using these technologies to do so?*. This will be answered by giving an overview of the necessary technologies in chapter 4 and what current literature and approaches exist on the subject in chapter 5. Chapter 6 will then go over the methodology to analyze how well Web3 technologies might supplement cookies. This is done based on a case study of online stores, where a user connects their wallet through SSO. These results are then discussed in chapter 7.

BACKGROUND INFORMATION - NON-FUNGIBLE TOKENS

As mentioned in 3, NFTs are a possible alternative to tracking users' behavior online. This chapter gives an overview of both the big picture beyond NFTs and the required technologies behind NFTs. These technologies are blockchain, smart contracts, NFTs themselves and cryptocurrency wallets.

4.1 WEB3

Previous iterations of the web include the original web, consisting of basic and static websites. Users did not have the possibility to interact with the content of websites in this original state of the internet. Web2 gave rise to a more interactive kind of web. This meant user generated content was at the center of the internet. Social media was born out of Web2. [4]

Websites in the era before Web3 fell under the standard client-server model. Here the program or website runs on a server, with which the client is connected to and sends requests to. All of the connecting clients are dependant on this central server, through which all bits of information must pass through. [5]

This centralized architecture served well for the first two iterations of the web. However, Web3 calls for decentralization, giving birth to decentralized applications (dApps). These applications no longer run on a single server, but rather on the blockchain itself. The advantage of this is that the benefits of the blockchain, such as availability and security, are baked right into the dApp. [5]

4.2 BLOCKCHAIN

Blockchain technology allows for peer-to-peer electronic cash payments. What makes blockchain different from other forms of electronic payments is that it takes out the trusted third party acting as a middleman between each transaction [6]. This means that two parties can execute a secure financial transaction without relying on, e.g. a bank, to verify each transaction.

This is achieved via a distributed ledger system. The stored information is distributed across many nodes, which may be located anywhere in the world. Each transaction is transparent and secure, even without the parties' knowledge of each other. Transparency means that each transaction is immutably stored within the blocks and visible to anyone. Security is achieved via several measurements. Each block is hashed, meaning that tampering with data within a block leads to the entire block's data changing. The de-

centralized structure of the blockchain also means that each node has a copy of the blockchain, which makes it difficult to tamper with. [7]

Cryptocurrencies and NFTs are based on blockchain.

4.3 SMART CONTRACTS

Although Bitcoin does not natively support Smart Contracts, other blockchains such as Ethereum do. Smart Contracts are way to execute contracts between buyers and sellers, also without the need of a third party intervening. Once specific conditions of a contract are met, the underlying functions are automatically executed. [8]

The purpose of Smart Contracts in regard to NFTs is to ensure their uniqueness and specify the terms of agreement. An NFT's Smart Contract might specify that the NFT will be transferred from one party to the other if one party pays the other the agreed upon amount.

4.4 NON-FUNGIBLE TOKENS

NFTs are a type of cryptocurrency which is based on the Smart Contracts of the Ethereum blockchain. Cryptocurrencies, such as Bitcoin, are all the same. One coin is equal in value and indistinguishable from another. [9]

The value in NFTs thus lies in the fact that they are distinguishable from one another. Each NFT is non-fungible, meaning non-replaceable. This makes it possible to attach them to both digital and physical products in order to prove possession and authenticity of the product. [9]

For example, when buying a sneaker in an online store, it is feasible to receive an NFT with it as well. This NFT may contain the serial number

A common use-case of NFTs is to utilize them as an investment tool. Because NFTs have a price attached to them, it is possible to sell them at a higher price than what they were bought for. However, in the realms of this paper, NFTs will not be considered as an investment asset, but rather as a data-tracking mechanism.

4.5 CRYPTOCURRENCY WALLETS

Having tangible proof of ownership is what makes NFTs valuable. A cryptocurrency wallet serves the main function of allowing access to the data on a blockchain and transferring cryptocurrencies between two parties [10].

As mentioned in section 4.2, blockchain data is not stored in a central manner. This means that cryptocurrencies and NFTs are not stored inside of the wallet itself. Rather, a wallet gives a user a public and private key pair. This public key (or often referred to as the public address) is then encoded into the NFT on the blockchain when a transaction takes place. With a public address encoded into the NFT's transaction history, the corresponding user can verify ownership by owning the associated private key. In order to access the wallet, a user must associate a password with the private key. Wallets thus

allow users to access their cryptocurrency funds, NFTs, see their account balance, and execute transactions. [11]

It is important to note that a user's wallet does directly contain any personal information about the user. When creating a wallet, no name, username, or email is required. Although wallets are technically anonymous, back tracking a wallet's behavior and history may lead to identifying the user that the account is associated with.

Should a user forget or lose their private-key, then they lose access to their wallet without the possibility of recovery. The wallet and its contents are thus inaccessible. [11]

With the rise of Web3, many applications are being created with the use of wallets in mind. Later in section 5.3, we will discuss what current products are on the market that fall within the realm of this paper. An important use-cases of wallets, beyond directly communicating with the blockchain, is the use of single sign-on (SSO) for Web3 websites [12].

Cryptocurrency wallets are thus the gateway to any blockchain. They are the center pieces of any type of interaction with NFTs. Section 5.3 will have a look at market products which manage cryptocurrency wallets.

RELATED WORK AND MARKET PRODUCTS

This chapter takes a look at current literature in a similar area as well as existing companies developing products in this field.

5.1 CURRENT STATE OF THE ART

At the time of writing, research has yet to be conducted on how to mimic the functionality of cookies through cryptocurrency wallets and NFTs. There is an obvious research gap in this area. This paper attempts to fill that gap.

Online Stores and NFTs / Wallets How is user data typically tracked online? Are there already nfts, sites, and tools to track data using nfts? Challenge of high entry barrier with nfts and wallets. A lot of necessary know-how

5.2 RELATED WORK

A plethora of relevant research has been conducted on cookies, including their privacy issues, and on wallets and NFTs. This paper aims to bring these two areas of research together to answer the question at hand.

5.2.1 *Cookies*

Todo

5.2.2 *NFTs and Web3*

Todo

5.3 CURRENT MARKET PRODUCTS

Within the realm of this research, no company was found that openly speaks about acquiring data through wallets in order to learn more about their users. However, there are a handful of companies and products that make it possible to do so.

The following companies and products support the case study of this paper (as will be mentioned in more detail later in section [6.1](#)).

Especially relevant for this paper is any type of application or product that allows SSO for a dApp using a user's wallet. SSO works by replacing the typical username and password login. Instead, a single ID such as your Google account can be used to login across all websites that support a Google login.

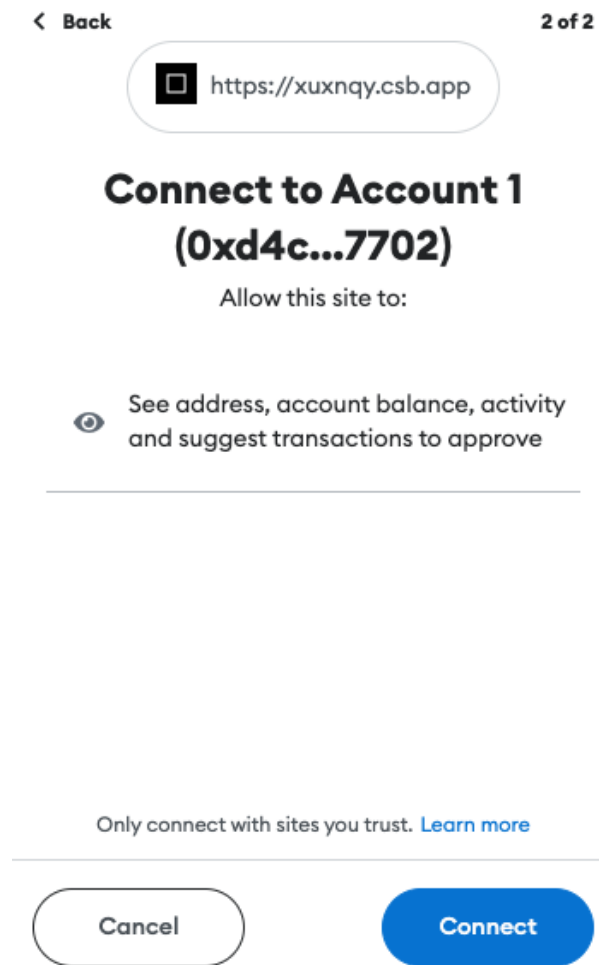


Figure 5.1: MetaMask’s popup screen when a website requests to connect to a user’s wallet.

This can also be done with a cryptocurrency wallet, so long as the wallet offers an API for developers to create a SSO with it on their website.

5.3.1 *MetaMask*

MetaMask is a popular browser extension which works on most major browsers. It is a digital wallet and allows for interaction with the blockchain and dApps. With the extension installed, a user can use their wallet to sign in to any dApp that utilizes MetaMask’s SSO. [13]

Figure 5.1 displays MetaMask’s popup, when a website requests to connect to your wallet. As can be seen in the figure, the user’s public address (0xd4c...) is displayed. With just this information, a plethora of information can be gathered on the user. The website is also requesting to see the wallet’s account balance, activity, and will request transactions (which the user will manually have to accept or decline).

5.3.2 *Wallet Connect*

Wallet Connect [12] is a company developing various open source products which allow dApps to connect to your wallet. At the time of writing, their portfolio includes 4 products. However, only the *Sign* product is so far released to the public.

- Sign: A secure way to connect your wallet to dApps and make secure transactions between them. [12]
- Auth: An SSO which works by connecting your wallet to dApps. This means that a user does not have to create an individual account for each platform. This is similar to MetaMask. [12]

METHODOLOGY

This section works through an example case and uses that to demonstrate how an online store may gather data on a user and thus create a profile of them to create specific, targeted content for them.

6.1 EXAMPLE CASE - ONLINE STORES AND SINGLE SIGN-ON

In a hypothetical and not-so-distant future, Web3 technologies might reinvent how we use the internet. From alternate currencies to dApps; the future internet may not be as we know it today in its current Web2 state. A hypothetical scenario will be described in this section in order to look at how user data might be tracked in this future version of the internet.

Imagine Alice visits an online store for shoes. She does not have a profile for this website yet and sees that she can create a profile using her wallet's SSO function. After doing so, she purchases a pair of shoes. She receives a notification from the website that they would like to gift an NFT to Alice. She accepts and a digital twin of her newly bought shoe as an NFT is placed into her wallet.

A few days later, Alice visits a different online shop. She also does not have an account here and again uses the SSO function to create a profile. Her wallet is thus connected with this new website. Immediately, she receives shoe recommendations from the website that fit her exact taste.

How is the second online shop able to give specific recommendations to Alice just by having a connection set up to her wallet?

6.2 PUBLIC WALLET ADDRESS

In the above scenario, the user grants wallet access to the online stores. As mentioned in section 4.5, the online stores are thus able to view the public address of the wallet. Although the stores do not know anything about the user specifically (i.e. name, age, etc.), this information alone is enough to be able to make specific recommendations to a potential buyer.

This is possible because everything written to the blockchain is public knowledge. When an online store, as in the example above, places an NFT into a user's wallet, the transaction is recorded with both parties' public addresses.

Etherscan [14] and OpenSea [15] are two popular websites for viewing transactions and profiles. When looking up a user's public address on Etherscan, every transaction associated with that public address can be viewed [14]. Figure 6.1 shows an example OpenSea profile, also viewable by anyone. OpenSea is a marketplace to view and trade NFTs [15]. In the example, the

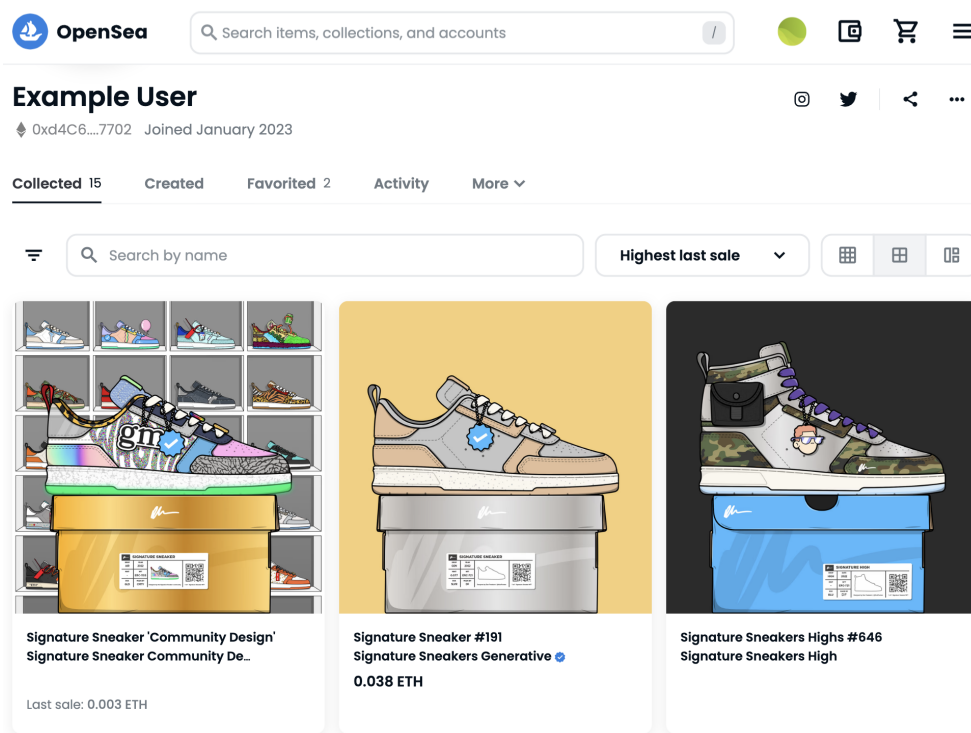


Figure 6.1: An example profile on the online NFT marketplace *OpenSea* [15].

user with the public address starting with *oxd4C6*, is displayed. This user has three NFTs currently in their wallet.

This information about a user is automatically accessible to any platform that a user connects their wallet to. In the above example, the second online store would be able to see the contents of the users wallet, recognize that they have previously bought a certain shoe from another store by seeing the associated NFT. Knowing what shoe a user has previously bought, they are able to recommend similar products to the user. For example, if a customer has previously bought a certain shoe from Nike and received an NFT for their purchase, then Adidas can use the information of that NFT to recommend products of their own.

6.3 FURTHER OBTAINABLE DATA

Todo: Something about transactional data that can be viewed on Etherscan. Not only can companies see our wallets and what NFTs we're holding, but they can also see who we are interacting with and can use that information to find things out about us.

Wallet Balance wird auch angezeigt

You can also see all transactions. Meaning you can see who an individual is interacting with. Using their public address you can gain insight as to what they're selling, etc. which might be useful information on the current user as well.

6.4 EXAMPLE OF PROGRAMMATICALLY OBTAINING INFORMATION VIA A WALLET

In order to demonstrate that the above information can truly be gathered on any connecting wallet, a short example will be run through. The frontend will be created using React. The example uses the Web3 component library *Rainbow Kit* [16]. Using this UI kit, a connect button for wallets is created. The connection to the Ethereum blockchain is created using the React hooks Library named *wagmi*.

When the button is clicked and specified that you wish to connect via MetaMask, the same popup as in figure 5.1 appears. Once connected, the frontend receives connection details such as the wallet link, the wallet's connection status, and most importantly the public address of the wallet. This is shown in listing 6.4.

```
import { ConnectButton } from '@rainbow-me/rainbowkit';

export const YourApp = () => {
  return <ConnectButton />;
};
```

Listing 6.1: An example of implementing a connect wallet button within the frontend of a webapp using the *RainbowKit* UI Library [16].

```
import { useAccount } from 'wagmi'

function App() {
  const { address, isConnected, isDisconnected } = useAccount()

  if (isConnecting) return <div>Connecting</div>
  if (isDisconnected) return <div>Disconnected</div>
  return <div>{address}</div>
}
```

Listing 6.2: An example of getting a wallet's public address using *wagmi React Hooks for Ethereum* [17]. This can be used once the wallet has been connected successfully.

```
https://api.etherscan.io/api?module=account
&action=tokenfttx
&contractaddress=0x708E73c7A0D81e00e848c902217d2d39e56d65AF
&address=${address}
&page=1&offset=100
&startblock=0
&endblock=27025780
&sort=asc
```

```
&apikey=${apiKey}
```

Listing 6.3: asdf.

```
[
  {
    "blockNumber": "16526088",
    "timeStamp": "1675159439",
    "hash": "0
      xdeebo4083dce62a599e4df0050f29eace79a517649dce48b8a1f00961f39742c
    ",
    "nonce": "55820",
    "blockHash": "0
      x8bcdc1acada5e191ecde74131f3098e42c1d886a48a6edd766425c725d976455
    ",
    "from": "0x36c72892fcc72b52fa3b82ed3bb2a467d9079b9a",
    "contractAddress": "0x708e73c7a0d81e00e848c902217d2d39e56d65af",
    "to": "0xd4c656b454bae586ff3afc28171d2981a1f17702",
    "tokenId": "1009",
    "tokenName": "BoredApeFrens",
    "tokenSymbol": "BAF",
    "tokenDecimal": "0",
    "transactionIndex": "92",
    "gas": "400000",
    "gasPrice": "20873221741",
    "gasUsed": "260812",
    "cumulativeGasUsed": "6383822",
    "input": "deprecated",
    "confirmations": "1357"
  }
]
```

Listing 6.4: asdf.

RESULTS AND DISCUSSION

7.1 RESULTS

Maybe include a table with a comparison of some key features for tracking user data. Cookies and NFTs side by side.

7.2 PROBLEMS

7.2.1 *Quality of Data*

Todo: How is the data that is gathered different from cookies?

7.2.2 *Privacy - Sharing Your Wallet's Content*

It might be a problem who an individual shows their wallet to, i.e. with which platforms a user connects their wallet to. Because an online store receives the public address of a user, and can thus see the contents of their wallet, certain privacy issues may arise with SSO.

MetaMask even warns to be careful about which websites access is granted to. It recommends to check how well-known a project is, how often the user intends on using the dApp, and whether or not known security breaches have happened before on the connecting website. [13]

Although a user's name is not directly associated to their wallet, it is often possible to obtain this information by analyzing the wallet's activity and transaction history. Aggregating this information, it can be possible to trace back who the wallet belongs to.

This may force users to own several wallets. Each time a user connects to an online store, they would have to think about which wallet they want to use, meaning which wallet's content they want to share with the website they are connecting to and whether or not they want information from this site written to their address. Again, once a transaction takes place on the blockchain, it is immutable and cannot be reversed. That bit of information is thus permanently and publicly recorded on the blockchain and associated with the given public address of the user.

7.2.3 *High Entry Barrier*

Todo: How is the high entry barrier of NFTs going to influence the wide spread use of tracking via NFTs? It might not be very practical to track users this way.

7.2.4 *High Gas Prices*

Todo: How is the high entry barrier of NFTs going to influence the wide spread use of tracking via NFTs? It might not be very practical to track users this way.

7.3 APPLICATION POTENTIAL

Go into detail of what potential use cases may arise from NFTs being used in this way. For example, if I buy a Werder Ticket and that gets saved into my wallet, and I then get a hotel somewhere in Bremen, they may see that I'm there for the game and may give me a discount or something. The prerequisite for something like that is that everyone supports NFTs.

7.4 DISCUSSION

CONCLUSION AND FUTURE WORK

8.1 CONCLUSION

8.2 FUTURE WORK AND PATH FORWARD

BIBLIOGRAPHY

- [1] David M Kristol. "HTTP Cookies: Standards, privacy, and politics." In: *ACM Transactions on Internet Technology (TOIT)* 1.2 (2001), pp. 151–198.
- [2] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. "The web never forgets: Persistent tracking mechanisms in the wild." In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 674–689.
- [3] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. "Americans reject tailored advertising and three activities that enable it." In: *Available at SSRN 1478214* (2009).
- [4] S Filipčić. "Web3 & DAOs: an overview of the development and possibilities for the implementation in research and education." In: *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*. IEEE. 2022, pp. 1278–1283.
- [5] Siraj Raval. *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.", 2016.
- [6] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system." In: *Decentralized Business Review* (2008), p. 21260.
- [7] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." In: *Business & Information Systems Engineering* 59.3 (2017), pp. 183–187.
- [8] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. "An overview on smart contracts: Challenges, advances and platforms." In: *Future Generation Computer Systems* 105 (2020), pp. 475–491.
- [9] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." In: *arXiv preprint arXiv:2105.07447* (2021).
- [10] Kostis Karantias. "Sok: A taxonomy of cryptocurrency wallets." In: *Cryptology ePrint Archive* (2020).
- [11] Saurabh Suratkar, Mahesh Shirole, and Sunil Bhirud. "Cryptocurrency wallet: A review." In: *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE. 2020, pp. 1–7.
- [12] WalletConnect, Inc. <https://walletconnect.com/products>. Accessed: 2023-01-22.
- [13] MetaMask - A ConsenSys Formation. <https://metamask.io/>.
- [14] Etherscan. <https://etherscan.io/>.
- [15] OpenSea - Ozone Networks, Inc. <https://opensea.io/>.
- [16] Rainbow Kit. <https://www.rainbowkit.com/>.

- [17] *Wagmi React Hooks for Ethereum*. <https://wagmi.sh/>.