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, 12.02.23

Hendrik Gruber

ABSTRACT

Non-Fungible Tokens (NFTs) have risen in popularity in recent years. While they are commonly used as a means of financial investment, they also have the potential to be leveraged to fulfill other use cases. One such use case is serving as a supplement to tracking user data. This research uses an example use case to demonstrate how NFTs can be used to gather user data. This data can then be used to serve targeted ads to the user. This paper walks through an example case study and how proves that this is possible with a JavaScript example. The results of this paper suggest that this is possible with the current technology. However, the problem lies in the fact that wide-spread adoption of NFTs is currently not possible because of hindering factors such as a high entry barrier to the blockchain and high gas prices to interact with it. Because of this, it is possible to supplement data gathering with NFTs, but they do not fully replace how cookies are conventionally used.

CONTENTS

ACRONYMS

API	Application Programming Interface
dApp	Decentralized Application
NFT	Non-Fungible Token
SSO	Single Sign-On

1 INTRODUCTION

Non-Fungible Tokens (NFTs) have gained popularity over the years with the rise of cryptocurrencies [1]. 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 in blockchain and cryptocurrencies such as Bitcoin, it is a very current and hot topic. NFTs have commonly been traded as a financial investment in their early years. The most prominent example being the Bored Apes Yacht Club, where some of the first minted NFTs sold for a total over $24 Million in 2021 [1]. 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.

2 BACKGROUND INFORMATION - COOKIES

This chapter gives a general overview on cookies and why they are problematic. With this information, the problem statement in the next chapter will be more clear.

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. [2]

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. [2]

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. [3]

These third-party cookies are what danger users' privacy. When visiting website *a*, there may be some cookies set by website *b* that track you. Even though you are not currently visiting website *b*, they are still obtaining information on you. Even when rejecting these cookies in the popup, tracking is sometimes still possible if there are implementation errors, misconfigurations, or unlawful behavior at work [4].

2.3 PRIVACY AND POLICIES

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. [5]

Name			Value
anonymousId	Copy	Copy&Delete	6DB06C34EBC6A1C91D3FE1390005F038
AnalysisUserId	Copy	Copy&Delete	2.23.208.149.115321675181001842
audience_segmentation_performed	Copy	Copy&Delete	true
AKA_A2	Copy	Copy&Delete	A
geoloc	Copy	Copy&Delete	cc=DE,rc=HE,tp=vhigh,tz=GMT+1,la=50.12,lo=8.68
s_ecid	Copy	Copy&Delete	MCMID%7C62245730017189234137942869322525575041
bm_sz	Copy	Copy&Delete	20CFC5513B665E9ACF4BAC361644FD78~YAAQldAXAjrYPs+F
AMCVS_F0935E09512D2C270A490D4D%40AdobeOrg	Copy	Copy&Delete	1
AMCV_F0935E09512D2C270A490D4D%40AdobeOrg	Copy	Copy&Delete	1994364360%7CMCMID%7C62245730017189234137942869 1675188213s%7CNONE%7CvVersion%7C3.4.0
bm_mi	Copy	Copy&Delete	249502A4BD0395A7E8942F31467EEFB0~YAAQm6AkF5wM8M
RT	Copy	Copy&Delete	"z=1&dm=nike.com&si=9763249d-980b-485e-bc34-659b424cecb9&ss=ldkfit5k&sl=1&tt=2r6&bcn=%2F%2F684dd32
ak_bmsc	Copy	Copy&Delete	7677A2025D84466D75DD449230A75BFF~0000000000000000
bm_sv	Copy	Copy&Delete	C3030AA41DF32FEE69162C0739893630~YAAQm6AkF34N8M
sq	Copy	Copy&Delete	0
_abck	Copy	Copy&Delete	CB9420A9948E3F686BE7E05D785A5515~-1~YAAQm6AkF5wC
anonymousId	Copy	Copy&Delete	6DB06C34EBC6A1C91D3FE1390005F038
ppd	Copy	Copy&Delete	homepage|nikecom>homepage

Figure 2.1: A screenshot of all active cookies being used when visiting https://www.nike.de

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 what: personalized advertisements rather than generic ones. [5]

Figure 2.1 shows a screenshot of all active cookies when visiting Nike's German domain. Notice how simply loading their website automatically sets 17 cookies, even before asking for permissions. While some of these may be required for the website to function properly, some may be used to gather information on the visitor. Each key-value pair is encoded, meaning they are not readable for humans. This means that a user is not able to understand what data is being tracked here. Nike may also track similar data on other websites by using third-party cookies.

Gathering users' information in ways that they are not aware of, i.e. through third-parties, begs the question of how long this type of data collection will be possible and if there are any alternative methods to it.

3 PROBLEM STATEMENT

Creating individual profiles of users and utilizing these to display personalized ads have 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 topic that this research paper analyzes is possible 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 rather supplement, cookies and continue to allow for detailed tracking of users. Even in an online world with more strict privacy policies and regulations where third-party cookies are becoming less frequent.

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 to the website. These results are then discussed in chapter 7.

4 BACKGROUND INFORMATION - NON-FUNGIBLE TOKENS

As mentioned in chapter 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. [6]

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. [7]

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. [7]

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 [8]. This means that two parties can execute a secure financial transaction without relying on a middleman, 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 decentralized structure of the blockchain also means that each node has a copy of the blockchain, which makes it difficult to tamper with. [9]

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 a 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. [10]

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. [11]

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. [11]

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 of the product. With this serial number of the physical shoe saved into the NFT, they are linked together. But how do you I know that the NFT of a product is the original and not a copy with the same serial number? By looking at who created the NFT, which is stored in the blockchain's public information. If you bought a shoe from Nike, then you can verify that the NFT along with the shoe was created by the official NFT account of Nike.

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 digital twin to both digital and real-world products. Utilizing NFTs like this, they can be leveraged as a data-tracking tool.

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 [12].

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. This public address is similar to a conventional account transaction number and may be publicly displayed without security hazards.

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. [13]

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 in 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. [13]

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 [14].

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.

5 RELATED WORK AND MARKET PRODUCTS

This chapter takes a look at current literature in similar areas 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 are. This paper attempts to fill that gap.

5.2 RELATED WORK

A plethora of relevant research has been conducted on cookies, including their privacy issues. Some general research has been conducted 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*

In the paper *HTTP Cookies: Standards, Privacy, and Politics*, author David M Kristol takes a look at what cookies are, how they are used, and what security implications come along with them. This was done analyzing one of the first cookie standards that was created in the late 90s. [2]

One of the main security concerns regarding cookies, even back in 2001 when then paper was published, was information leaking to unwanted servers. The paper also mentions the security concerns of using third-party cookies to gather more detailed user data and thus being able to serve ads catered better towards the end-user. [2]

5.2.2 *Non-Fungible Tokens, Wallets, and Web3*

Although there is a gap in the literature as to how NFTs and Wallets can be leveraged to collect user data, there is some general research on Wallets and NFTs.

The 2020 paper *SoK: A Taxonomy of Cryptocurrency Wallets* by Kostis Karantias gives the first general definition of what cryptocurrency wallet is and how it facilitates transfers between two wallets. [12]

Qin Wang et. al give an overview on NFTs in their 2021 paper *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*. They explore how it is made technically possible to distinguish between two tokens and how the underlying technology of NFTs work. The paper gives an overview of the current state of NFTs and is a good starting point for readers new to the subject. However, the described opportunities of NFTs are very basic. The authors mention boosting the gaming industry by linking in-game characters to the NFTs in a wallet, or by verifying ownership of digital assets through NFTs. They do not describe more advanced mechanisms such as using the publicly available data of NFTs and Wallets to track user behavior.

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. 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. [15]

Figure 5.1 displays MetaMask's popup, when a website requests to connect to a user's 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 [14] 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. [14]

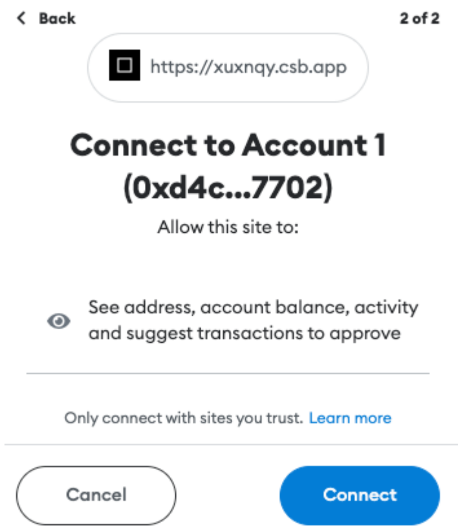

Figure 5.1: MetaMask's popup screen when a website requests to connect to a user's wallet.

- 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. [14]

With an overview of current literature and market products, we can take a look at how it is possible to track user data with NFTs and Wallets in the next chapter.

6 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? Although this situation is fictitious, the technology to make it happen already exists.

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 with both parties' public addresses.

Etherscan [16] and OpenSea [17] 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 [16]. Figure 6.1 shows an example OpenSea profile, also viewable by anyone.

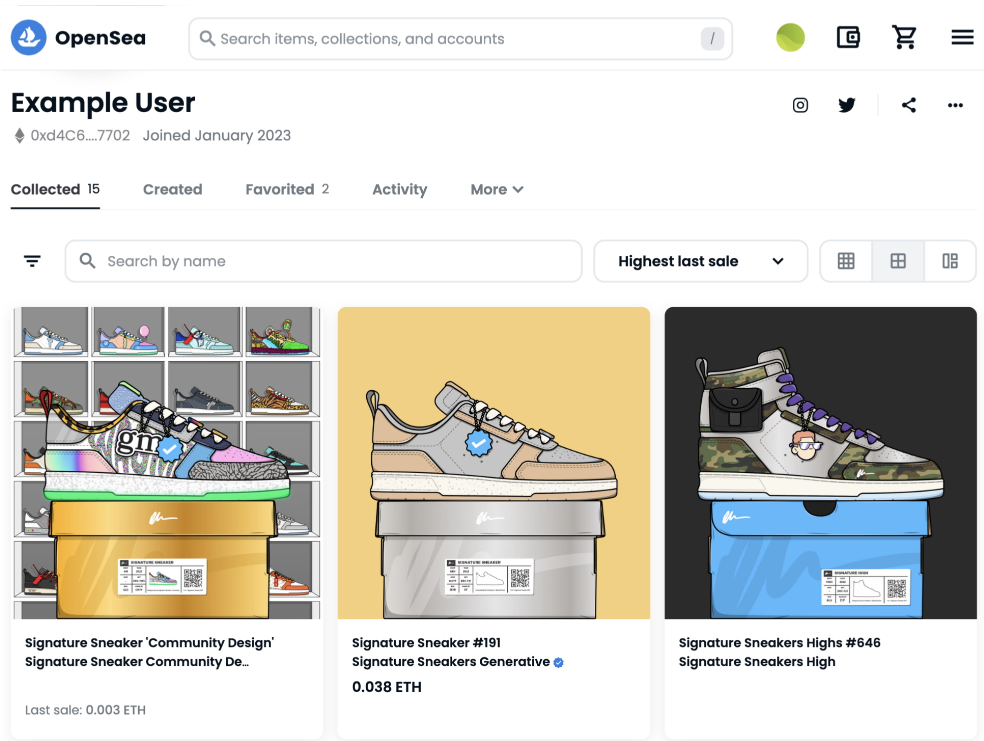

Figure 6.1: An example profile on the online NFT marketplace *OpenSea* [17].

OpenSea is a marketplace to view and trade NFTs [17]. In the example, the user with the public address starting with *0xd4C6*, 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.

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 buying, selling, etc. which might be useful information of the current user as well.

6.3 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* [18]. 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* [19].

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.

Listing 6.1 shows an example of a simple React component which utilizes the Rainbowkit UI Library. The *ConnectButton* component comes preconfigured with everything necessary to connect a wallet. Therefore, no logic needs to be implemented for a simple connect button.

```
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 [18].

Once the wallet has been connected successfully, it is possible to access a variety of information on the wallet. Listing 6.2 is an example of how *wagmi*, a type of React Hook which utilizes the Ethereum blockchain, is able to retrieve the address of a user. The example then displays the public address in the browser.

```
import { useAccount } from 'wagmi'

function App() {
  const { address, isConnecting, 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* [19]. This can be used once the wallet has been connected successfully.

Utilizing the Etherscan API, it is possible to obtain the entire transaction history of any Wallet. Plugging the public address obtained into the API call in listing 6.3, it is possible to retrieve user data. The listing contains an example public address used for the purpose of this research.

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

Listing 6.3: A real-world example API call made from the frontend in order to retrieve all of a user's transactional data. The API is provided by *Etherscan* [16].

Figure 6.4 shows the response to the API call in listing 6.3. The response is an array of all of the public address's transactions. In this example, only one transaction has been made with the address. The response contains the blockchain's block number, the timestamp when the transaction was written to the blockchain, the public address of the sender (from), the public address of the recipient (to), the name of the token, the token ID, and a variety of information on the gas usage for the transaction.


```
[
  {
    "blockNumber": "16526088",
    "timeStamp": "1675159439",
    "hash": "0xdeeb...",
    "nonce": "55820",
    "blockHash": "0x8bcdc...",
    "from": "0x36c7...",
    "contractAddress": "0x708e...",
    "to": "0xd4c6...",
    "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: A real-world example of the response to the API request from listing 6.3. The result contains a variety of information, such as the transaction timestamp, the sender's public address (from), and the receivers public address (to). The response is provided by the *Etherscan* API [16].

Creating this quick example shows that obtaining personal information through a Wallet can easily be achieved. With enough transactions in a user's account, the behavior can be analyzed and used to create content catered toward their interests.

For example, with several transactions in a Wallet's history, it is possible to look at who the user is interacting with. Who are they receiving NFTs from? Who are they sending them to? If they are receiving large amounts of NFTs from shoe brands, it is feasible to conclude that they have an interests in shoes.

By looking at the token name, the token ID, and the image associated with the token, it is possible to know what the NFT represents. This can be, for example, a specific sneaker from a specific brand.

Even the timestamp of the transaction can be used to gather information. How frequently is the user obtaining NFTs of a shoe? If they are receiving them in consistent time intervals, then that can be used to deliver ads to the user in the timeframe shortly before their next predicted purchase.

With just a few transactions in a Wallet, it is possible to gather behavioral information on a user. The possible applications of this are still in their infant stages. However, the potential can be great. The next chapter will discuss the results of this paper.

7 RESULTS AND DOWNSIDES

7.1 RESULTS

This chapter discusses the results of this paper by covering the downsides of using this method to track user data.

7.2 RESEARCH CHALLENGES

The lack of existing research around this subject comes with both advantages and disadvantages. A gap in research presents a large opportunity to have an impact in the research field at hand. Analyzing problems that no one has done before and being the first to market with research has its perks. On the other hand, not having any existing literature or research to use as a foundation of this paper deemed to be a large challenge. With everything being unanalyzed, in what direction should the research go? Narrowing this down and gathering a solid foundation to base this research on was a challenge in and of itself.

7.3 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. [15]

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.

7.4 HIGH ENTRY BARRIER

The technical possibilities of NFTs and Wallets are seemingly endless. However, actually creating a wide user-base, where it would be worthwhile to gift NFTs with real-world purchases and track users with the data of wallets would be a large challenge.

One problematic factor is that the technical entry barrier to Web3 is very high, compared to previous iterations of the web. In Web2 a user virtually only requires a smartphone and an internet connection to interact with social media sites. Comparing this to Web3, a user is required to have at least a very basic understanding of blockchain, which is a complicated technology. On top of this, they are required to create a wallet and understand how to use it and how it differs from conventional accounts created in the space of Web2.

This is a lot to ask of non-technical users. Getting Wallets and NFTs to the masses will require the products leveraging this technology to mature. They must become more user friendly and more seamlessly integrated into websites. Otherwise, the technical understanding will be too high and only a niche set of users will adopt the technology in their every day lives.

7.5 HIGH GAS PRICES

According to the official Ethereum page, gas prices in regard to cryptocurrencies is the required computational effort in order to interact with the Ethereum network (blockchain). [20]

Because the blockchain consists of highly complex cryptographic calculations, it is not a trivial matter to execute transactions on it. Even though the blockchain is decentralized, it is still required by some computer to execute the computation. The gas prices for the example in section 6.3 totalled a network fee of 11.91€. A higher price than the NFT used in the example itself, which cost 7.27€.

Discussing gas prices in-depth is worthy of its own research. In short, the high gas prices for interaction with the blockchain may be another hindering factor for wide-spread adoption. Although it is technically trivial to send a user an NFT after purchasing a real-world good, it might come with too high costs. These costs would need to be reduced before wide-spread adoption is possible.

8 CONCLUSION AND FUTURE WORK

8.1 conclusion

In conclusion, the idea behind using NFTs and Wallets in order to track user data is interesting. A large amount of data can be gathered on users by using NFTs and Wallets. By looking at a Wallet's transaction history, it can be determined who they are interacting with, what they may be interested in, what products they are buying, and to what time they are completing these purchases. The main benefit of Wallets is that all of this information is public knowledge.

However, while technically possible to implement, tracking user data with this method comes with flaws. As discussed in chapter 7, there are several factors that need to be overcome before wide-spread use can be considered. The variety of information gathered is neither as large, nor as in depth. The high entry barrier and high gas prices needed to interact with the blockchain need to be overcome before wide-spread adoption can be considered.

This means that NFTs and Wallets are a good supplement to tracking user data with cookies, but they do not replace cookies. The full potential of this method remains unfulfilled thus far.

8.2 future work and path forward

This paper is just the first step in research towards the power of NFTs, other than leveraging them as a financial investment. It only scratches the surface of this topic and a deep-dive into the subject matter would require both more time and dedication.

More research in this subject area would be interesting to see. There are many questions still open at the end of this writing, such as:

- *How to calculate the required product price to justify the gas price?*
- *How could potential changes in laws affect potential wide-spread adoption of this method?*
- *How does the high entry barrier affect potential application of this method?*

Obviously this paper is not able to cover all of the above points. Many questions are still open, as there is a research gap surrounding this subject. Diving into any of the above subjects would achieve very interesting results which may have a big impact on the future of the web.

A Master's Thesis would allow for the necessary environment to analyze any of these subjects in more detail.

BIBLIOGRAPHY

[1] *How Four NFT Novices Created a Billion-Dollar Ecosystem of Cartoon Apes*. https://www.rollingstone.com/culture/culture-news/bayc-bored-ape-yacht-club-nft-interview-1250461/. Published: 2021-11-01, Accessed: 2023-02-11.

[2] David M Kristol. "HTTP Cookies: Standards, privacy, and politics." In: *ACM Transactions on Internet Technology (TOIT)* 1.2 (2001), pp. 151–198.

[3] 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.

[4] Gertjan Franken, Tom Van Goethem, and Wouter Joosen. "Who left open the cookie jar? a comprehensive evaluation of third-party cookie policies." In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018, pp. 151–168.

[5] 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).

[6] 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.

[7] Siraj Raval. *Decentralized applications: harnessing Bitcoin's blockchain technology*. " O'Reilly Media, Inc.", 2016.

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

[9] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." In: *Business & Information Systems Engineering* 59.3 (2017), pp. 183–187.

[10] 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.

[11] 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).

[12] Kostis Karantias. "Sok: A taxonomy of cryptocurrency wallets." In: *Cryptology ePrint Archive* (2020).

[13] 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.

[14] *WalletConnect, Inc*. https://walletconnect.com/products. Accessed: 2023-01-22.

[15] *MetaMask - A ConsenSys Formation*. https://metamask.io/. Accessed: 2023-01-28.

[16] *Etherscan*. https://etherscan.io/. Accessed: 2023-01-30.

[17] *OpenSea - Ozone Networks, Inc*. https://opensea.io/. Accessed: 2023-01-30.

[18] *Rainbow Kit*. https://www.rainbowkit.com/. Accessed: 2023-01-31.

[19] *Wagmi React Hooks for Ethereum*. https://wagmi.sh/. Accessed: 2023-01-31.

[20] *GAS AND FEES*. https://ethereum.org/en/developers/docs/gas/. Last Edit: 2023-02-02, Accessed: 2023-02-11.