Frankfurt University of Applied Sciences

–Faculty of Computer Science and Engineering–

Using Non-Fungible Tokens to Track User Data Across Websites

What this paper is for (Abschlussarbeit zur Erlangung des ...)

Research Projekt - Winter Semester 2022/23

Submitted by

Hendrik Gruber

Matriculation Number: 1458240

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

DECLARATION (ERKLÄRUNG)

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

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

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

NFT	Non-Fungible Token
dApp	Decentralized Application

1

INTRODUCTION

2 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 what: 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?

3 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 single-sign on. These results are then discussed in chapter 7.

4

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 is then encoded into the NFT on the blockchain when a transaction takes place. With a public key 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. [11]

Wallets also allow users to see their account balances and to execute transactions.

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 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.

5 CURRENT STATE OF THE ART AND RELATED WORK

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 are. 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 nec- essary 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 areas of research together to answer the question at hand.

5.3 CURRENT MARKET PRODUCTS

Although no company openly speaks about acquiring data through wallets in order to learn more about their users, 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).

5.3.1 *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 first 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: A single-sign on by connecting your wallet to dApps. This means that a user does not have to create an individual account for each platform. [12]

- Chat: A wallet-to-wallet messaging system which writes to the blockchain. [12]
- Push: A notification system which will send push notifications to your phone any time any activity is detected within your wallet. [12]

Especially relevant for this paper is any type of application or product that allows single-sign on for a dApp using a user's wallet. Section 6.1 will go into more detail on this.

6 METHODOLOGY

6.1 CASE STUDY - ONLINE STORES AND SINGLE-SIGN ON

Explain the case study and example.

Maybe include a table with a comparison of some key features for tracking user data.

7 RESULTS AND DISCUSSION

7.1 PROBLEMS

7.1.1 *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 DISCUSSION

8

CONCLUSION AND FUTURE WORK

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.