5-2023

A Cookieless Future: Solving the UX Problems Caused by the Privacy Protections Method

Ibrahim S. Hanoglu

A COOKIELESS FUTURE: SOLVING THE UX PROBLEMS CAUSED BY THE PRIVACY PROTECTION METHODS

by

Ibrahim S. Hanoglu

Submitted in Partial Fulfillment of the
Requirements for the Degree of Master of
Science in

Digital Marketing
at

Lindenwood University

Ibrahim S. Hanoglu
Author's Name

5/3/23
Date

Author's Signature

Committee Chair
Andrew Allen Smith

Date 5.5.23

Committee Chair Signature

Clayton Smith
Committee Member Date 5.5.23

Committee Member Signature

Kyle Coble
Committee Member Date

5.5.23

Committee Member Signature

Lindenwood University

A COOKIELESS FUTURE: SOLVING THE UX PROBLEMS CAUSED BY THE PRIVACY PROTECTION METHODS

by

Ibrahim S. Hanoglu

A Prospectus of a Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Digital Marketing

May 2023

Abstract

To the author's knowledge, this article is the most comprehensive research study of its kind, if not the only example, as it examines the user experience issue caused by privacy protection methods from a theoretical and practical perspective. This study investigated where third-party cookies are used according to marketing techniques, the effects of these cookies, and the user experience problems that arise after these cookies are blocked by privacy protection methods. The research firstly determined the access to the user's computer in both methods by measuring the files and trackers left on the computer by comparing the Chrome browser, which actively uses third-party cookies, and the Brave browser, which also has a Chromium infrastructure but completely blocks third-party cookies, using CCleaner software. To do this, the world's 100 most visited websites, selected by Ahref.com, were used. Then, at least 100 people were asked to participate in a survey about their experiences with the Brave browser. Brave browser is known for its close relationship to the blockchain. Finally, considering the way these third-party cookies are used, UX problems caused by privacy protection methods and user feedback, and the features that the application should have, which can completely solve the privacy problem in the future without interfering with the UX, were determined.

Search Phrases/Keywords: "Third-party cookie", "Third-party cookies", "Cookieless" AND "marketing", "First-party cookies", "blockchain" AND "digital marketing" AND "consumer data", "blockchain" AND "third-party cookies", "third-party" AND "GDPR", "cookie less" AND "first party cookies", "cookieless" OR "cookie less" OR "cookie-less" OR "cookies" AND "marketing", "marketing" AND ("cookies" OR "web cookies" OR "cookieless" OR "third-party" OR "third-party" OR "cookie-less") AND "browser".

Acknowledgments

I would like to express my deepest gratitude to my thesis advisor, Andrew A. Smith, for his unwavering support, guidance, and encouragement throughout my graduate studies at Lindenwood University. Professor Smith's expertise and insight have been invaluable in the development and completion of this thesis.

I would also like to express my gratitude to members of my thesis committee, Clayton Smith and Kyle Coble, for their constructive feedback, valuable suggestions, and time spent reviewing and guiding me throughout the research and writing process.

I am also grateful to Lindenwood University for providing the necessary resources and support to complete this thesis.

Finally, I would like to thank my family and friends for their unconditional love and support throughout my journey. Without their encouragement and understanding, this success would not have been possible.

Table of Contents

Table of Figures

1. Introduction / Background:

Many people think when it comes to online presence, privacy is the main concern, but most share their personal information willingly to have better and faster cross-platform and cross-site experiences. Consumers sign up for a new website or an application with Facebook, or any other existing account. In addition, they click on and like the "follow this Facebook group" ads they come across, because they are interested in that topic, even if they complain about constantly being followed or watched by these companies. The results of Lakshmi Narayanan Jayakumar's study that explain the reasons for accepting cookies, even if users have the option to refuse, are given in the table below.

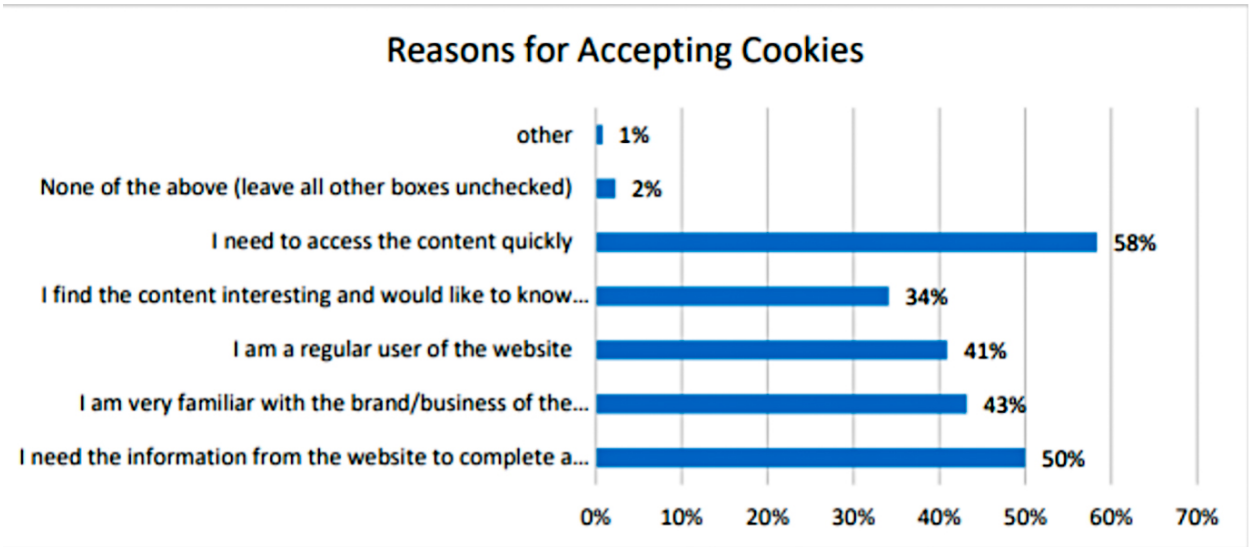


Fig. 1: Jayakumar, Chart 4, p. 35

Consumers love the convenience of web2 even though web2 makes them nothing but a marketing tool in its ecosystem. When saying "Web", that means World Wide Web, or the internet more generally. The term "web2" is the first version of the internet to undergo a major change, and at this stage, users are more active and interactive than in the early days of the internet. Web2 also includes social media platforms, blogs, and other user-generated content. It is a more

interactive and collaborative version of web1 where users can communicate and share information more easily.

One of the first things that come to mind when it comes to marketing is competition between companies. The goal is always to be better than others and generate more sales or leads so the goal of the marketing effort is the consumer. In the traditional marketing and web1 era, this was mostly implemented as the consumption of information provided by companies, so they were throwing out their ads hoping it will hit the consumer, the target. The first online commercial came in 1994 when just 30 million individuals had access to the internet (Sadeghpour and Vlajic 804). With the transition to web2 in the late 1990s, marketing evolved into a different dimension. New marketing techniques began to emerge with more successful web2-based inbound techniques than traditional outbound techniques. At the same time, web2 allowed users to establish an interactive relationship with the brands they like. With the spread of social media, this relationship has completely turned into a relationship of interest, and the personal information of individuals has been hijacked in return for free services that are also used as an ad platform in the background. According to Sadeghpour and Vlajic, ad platforms are infrastructures that bring together publishers, advertisers, and users(consumers) and enable them to interact. Publishers or sellers are providers of ad system inventory and provide a space for ads to display. Advertisers (ad buyers) are individuals or companies that want to promote a product or brand. Users (consumers) are the reason for the system's existence and those who interact with the advertisements (Sadeghpour and Vlajic 805-806). Web2 couldn't stop where it was beneficial for consumers because marketing is a continuing race and requires constant improvement of advertisement techniques. Owners of such social media platforms, who play the middleman between the advertiser and the user, made huge profits from this system.

All middlemen, also known as trusted third parties, are expected to become obsolete as a result of blockchain technology (Chang and Hsieh 29; Ertemel 35). According to Ertemel, this includes Google, Facebook, and other major technological organizations. They store and commercialize customers' data as trusted third parties. Although customers are used to this situation, it is illogical if they do not own their personal information (Ertemel 35). As also mentioned by Ertemel, this system could not continue indefinitely, as the consumer who had the real power, namely the money, could not go beyond being a marketing tool in this system and never become the focus of the marketing effort. The most valuable personal information of the consumers was taken, they were tacked in between the platforms by the third-party cookies placed on their computers and the websites they visit, and a service or product was shown to the consumers by using this information. Simply, the system charged the consumer to see the ads which he hated. Web3, which is built on the blockchain eco-system, is coming to stop the intermediary companies from extorting the advertisers' budgets and give back the consumer the value they deserve. It seems a little difficult to return to the world of web2 after all the benefits provided to those who hold the real power, consumers, even if they are not aware of it.

On the other hand, the rollout of web3 and restoring privacy rights to consumers means disabling third-party cookies altogether. In this case, the consumer who regains their privacy will lose their cross-platform and cross-site user experience. As mentioned earlier, most consumers are willing to give up some of their personal information for this convenience and this is called the "Privacy Paradox". This research aims to identify the problem of third-party cookies and find a possible solution to the problems created by the solutions to these privacy concerns caused by third-party cookies. There is a lot of research on third-party cookies and solutions to privacy issues caused by third-party cookies. This research is unique because in this research, the author does not

explore privacy issues or solutions to these issues but instead explores the user experience issue arising from privacy protection methods. The author believes that blockchain is the ultimate solution to this problem, but research will show how necessary it is to use blockchain technologies at this stage of web3. Blockchain infrastructure is extremely complex (Chang and Hsieh 39) and requires the involvement of multiple platforms, businesses, and possibly the government.

This research handles the problem in three parts. In the first part, the literature is reviewed, and it examines marketing techniques, consumer data collection and use of this data, features and working structure of third-party cookies, decentralized networks, and methods that claim to solve the privacy problem. In the second part, firstly, when third-party cookies are blocked and unblocked, the amount of access by trusted third parties to consumers' computers is compared. The author used the chromium-based Brave browser to experience cookies in web3 browsing and the original Google Chrome to experience cookies in web2. CCleaner software is used to measure the number of files left on a MacBook Pro with macOS Monterey Verison:12.6 without any additional privacy software after each browsing experience. To do this, the author visited the world's 100 most visited websites, selected by Ahref.com while keeping the variables like IP address, Wi-Fi, computer, day, time of the day, etc. the same. Next, at least 100 people were asked if they used the Brave browser for at least 30 days to analyze the user's cookie-free browsing experience, as Brave offers the closest user experience to web3 browsing. With this research, information was collected about the cookieless browsing experience of consumers as well as web3 ad placement techniques. Finally, the collected information was analyzed. After the development and existence of the problem have been proven, the author analyzes whether this problem can be solved with blockchain applications and uses expert opinion to suggest the structure and working principles of the blockchain application that can completely solve this issue.

2. Literature Review:

Marketing techniques have often changed according to the time it was applied, the available technologies, and customer demands. According to Graesch et al., the question of what marketing is may vary depending on the period in which the question is answered. The meaning of marketing today is very different from what it was twenty years ago, or what it will be in the future (Graesch et al. 125). With the invention of web2, consumers' reliance on technology and digital media has evolved rapidly. Consumers are becoming more self-sufficient as a result of digitalization and personalization and can manage the majority of their procurement without depending on a single point of contact with a salesman or marketer (Graesch et al. 125). As technologies like smartphones and Wi-Fi become ever-present, people spend more and more time on digital devices, music and video streaming services, and social networks. The way these technologies are interacted with is shifted by this —and with the people and brands that make them more convenient—and it also changes the way marketers connect with consumers (Chomiak-Orsa and Liszczyk 10). The idea behind the creation of digital marketing is that meaning is created through interactions between users and marketing professionals (Aydin Aslaner and Aydin).

Fig. 2: Centralized Digital Marketing

This graphic shows the two different working principles of digital marketing strategies. According to this graphic, if the content creator is involved in the strategy, also called inbound marketing, marketing practice adds value to the user and is generally intended to use first-party

cookies. This technique causes no privacy concerns and is very likely to remain as it is. If the ad provider directs the audience to the campaign directly, it most likely means that is an outbound marketing practice and third-party cookies are used and/or will be used during this practice. Outbound marketing is the practice of using marketing communications that are traditionally performed via paid advertising and marketing messages to attract, persuade, or inform customers. While there is no agreement on whether outbound marketing is old-fashioned or not, it is agreed with Kali Hawlk that great benefits have been provided to businesses from the past to the present by outbound marketing and can be of great benefit even today when used in conjunction with more value-adding practices (30).

Behavioral marketing is a type of marketing that takes the customer's journey on the web into account to deliver more relevant and customized messages by keyword analysis (Wajde et al. 96). The method that makes behavioral marketing successful is following the consumer's cross-site and, if possible, cross-platform experiences (Graham et al. 343) over some time and showing the most appropriate ad for their experience but this causes some other problems. According to Sadeghpour and Vlajic, although behavioral marketing works very well for ad buyers, it raises privacy concerns (808). As of now, many web browsers that take this type of research into account and integrate with web3 standards have blocked third-party cookies. This was a good result in terms of privacy, but it was designed without a personalized web experience in mind.

2.1. Third-Party Cookies:

Third-party cookies are small software placed on the user's computer to infect and track their browser through the websites. They are often used by advertisers and third-party analytics providers to monitor users' browsing habits on web statistics. These cookies are extremely common (Al-Ibrahim et al. 309) and can be used to track users on different websites, create a

profile based on their interests, and target them with ads. According to Hahn et al., tracking systems have been condemned for breaking user security and data privacy, decreasing publisher revenue, and costing advertisers money due to ad fraud (26). Some browsers have a feature that allows users to block third-party cookies, but this may limit users' ability to use some website features. Even though Price claims that none of the data collected by third-party trackers (cookies) can be personal information, according to Pantelic et al., any data collected and related to a person's identity is considered personal data (9).

To make a simple assumption, most of the websites with active visitors right now include third-party cookies from companies such as Facebook or Google to take advantage of different benefits. These companies offer some features for free, such as liking, sharing, video viewing, and analytics that forces webmasters to add a few lines of code to their websites. This code provides great benefits to webmasters in terms of managing, distributing, and socializing their content, but the matter does not end there. Since the same codes are available everywhere, these codes also give trusted third parties a chance to follow their visitors cross-platforms, with the great help of the cookies placed on visitors' computers. The alleged free service provides an enhanced cross-platform experience and a more enjoyable time for users and most of the time this is true. In other words, when trusted third-party companies place this code on as many sites as possible and therefore on the user's computer, they will know more about the visitor than visitors know about themselves. These cookies do not stay only on visitors' computers during the visit. The average cookie stays on a computer for 30 days. Of course, changing this is very simple and the cookie can be set to remain on the visitor's computer until deleted. This gives consumers a more customized experience on the internet. According to Al-Ibrahim et al., cookies are useful for helping users

browse the web, but attackers use them for certain types of attacks, such as “SSL Heart Bleeding Attacks” to hijack a session or “Man in the Browser Attacks” to steal personal information (308).

2.2. Problem Solved by:

2.2.1. Browser privacy mode:

Browser privacy mode can be a useful tool when it comes to online privacy. It’s available in most browsers, but the amount of security varies from browser to browser. Privacy mode is also named incognito mode, InPrivate, and Private Browsing by different browsers (Parkyn 62). When a person chooses the private mode to access the internet, the browser creates a temporary folder where all the activities and information are saved. This information is not saved on the device indefinitely and is not transmitted to the server. This means that the browser history, cookies, and other information will not be stored. The more restricted the browser’s privacy settings, the better the protection against third-party cookies. This can be useful if the main concern is online privacy and wanting to prevent information from being tracked or recorded. Privacy mode can also help prevent websites from placing cookies on the device. With this structure that does not allow the data to leave the user’s computer, it is similar to the technique Brave browser uses but is it as safe?

According to Parkyn, they may be named differently but the lack of privacy provided by the private browsing modes given by Chrome, Edge, Firefox, and other browsers is alarming. The only benefit of the privacy mode to the user is that it hides the internet history from the people with whom the user shares their computers. To make this explanation easier to understand, Parkyn uses an example of a Christmas gift research that should remain a surprise (Parkyn 62).

2.2.2. VPN:

Even if the Incognito mode is enabled, websites can identify users based on their IP address or detect their location (Parkyn 62). A VPN, or Virtual Private Network, encrypts and routes the

internet traffic through another server. This makes it far more difficult for third-party cookies to track online activity. Furthermore, a VPN can assist to protect online behavior from being watched by ISP, Internet Service Providers, or, in certain situations, the government. Even though he founds VPNs more beneficial, according to Parkyn, VPNs also have some downsides. First of these is the free VPNs that are used in large numbers, and many of them generate income from the user information they sell. In addition, they are limited and therefore cannot remain active all the time. Another problem is that paid ones have monthly or annual plans (Parkyn 63). This means adding a new subscription to subscriptions people are having a hard time managing.

The author talks about his firsthand VPN experience with Surf Shark VPN:

> First, the VPN was very appealing to me. It was perfect and very convenient considering its technical features and advantages, but I had to cancel my membership after a week. VPN had turned my browsing experience into a nightmare. I could not even enter the sites that have proven their security. Also, some apps on my phone had become inoperable. When I spoke to the tech, I was told to disable the "Clean Web" option, which blocks ads, trackers, and malware, and the system will go back to normal. It was very illogical because then I am not protected but despite this, I did what he said, the system didn't work properly.

2.2.3. Google Privacy Sandbox:

Google has been criticized in the past for handling user data unethically, so the company hopes the privacy sandbox will be a way to address these privacy concerns. Google's Privacy Sandbox is a set of browser APIs (Application Programming Interfaces) to enhance web privacy while maintaining the benefits of internet advertising (Sadeghpour and Vlajic 811). Here is what is known so far about the APIs being used by Google:

> The trust API is Google's alternative to CAPTCHA; it will ask a Chrome user just once to fill out a CAPTCHA-like program and then rely on anonymous "trust tokens" to prove in the future that this person is a real-life human. The privacy budget API will limit the amount of data that websites can glean from Google's APIs by giving each one a "budget." Google's conversion measurement API alternative to cookies will let an advertiser know if a user saw its ad and then eventually bought the product or landed on the promoted page. The Federated Learning of Cohorts will rely on machine learning to study the browsing habits of groups of similar users. The final component is PIGIN (referring to private interest groups, including noise), which lets each Chrome browser track a set of interest groups a user is thought to belong to. (Joseph)

Google considers the current state of web privacy to be unsustainable, and new techniques are needed to protect users' privacy while keeping the internet useful and accessible to publishers and advertisers. Privacy Sandbox aims to solve these problems by allowing publishers and advertisers to target ads without collecting personally identifiable information. According to Jayakumar, removing third-party cookies makes users more vulnerable due to the integration of Google's new technology, Privacy Sandbox, into the browser, making it impossible for the user to set any preferences or disable them entirely (Jayakumar 42). If Jayakumar's observations are correct, this means that Google, which will phase out third-party cookies, will have much more access to user data with more advanced "Walled Garden" techniques and will have absolute control over this data. Walled Gardens use free services to keep the original data owners, namely users, in their ecosystems and the data buyers, namely advertisers, by offering the right to use the encrypted/hidden version of this user data for a specific period of time or number of clicks without revealing the original data. Because they impose tighter access control on their platforms than

publishers on the open web, several of the largest digital advertising platforms (Google, Facebook, etc.) are known as “walled gardens” (Van Auken 24). Until Privacy Sandbox is activated, it seems like it will continue to be discussed as a system praised by Google supporters and seen as extremely worrying by some people who are uncomfortable with Google’s current use of data.

The most important topic to talk about in the Google Privacy Sandbox will be “The Federal Learning of Cohorts” (FloC) which will replace third-party cookies. Although Google says this is a more robust method to protect privacy, it would not be wrong to think that a company that derives its income from advertisements will not sacrifice much of this income. When the content of FloC and the working principles of APIs are examined, some problems that may arise in the future are encountered. First, FloC will only work with Chrome Browser and is not yet accepted by other major browsers, including chromium-based browsers, and it doesn’t look like it will be because of its data collection infrastructure. This is an issue that people who use multiple browsers at the same time experience even today. If they visit the same website on another platform (browser), they cannot be identified because third-party cookies saved on their last visit are stored in the previous browser and are not shared with the existing one. The bigger issue is the way FloC works. FloC collects user information such as third-party cookies. The only difference is that it doesn’t show it to advertisers or limit what they can see. Using the information only available to itself, Google places users in groups, cohorts, of several thousand, so that they become a group target rather than a personal one. According to Graham et al., with contextual marketing, advertisers are more concerned with what the audience is doing than what an individual is doing (343). Based on this statement by Graham et al., it can be said that contextual marketing forms the basis of the Google Privacy Sandbox. However, it is not impossible to access this information collected on the user's computer by reverse engineering or hacking because it is not distributed ledger. According to

Wajde et al, a distributed ledger is synchronized, replicated, decentralized, and encrypted data transactions shared by the parties (79). In addition, this structure of FloC confirms Jayakumar's claim that Google's new technology will prevent people from making any personal choices and make them more vulnerable (Jayakumar 42).

Privacy Sandbox is still in beta and may be subject to changes, but as can be seen at this stage, Privacy Sandbox is trying to fix one security issue with another while randomizing it a bit. Also, even if it can provide great success one day, it is very unlikely to reach full validity as it will only provide this benefit to Chrome users.

2.2.4. Privacy protection laws:

At a time when the internet plays such an important role, the privacy of citizens' personal information is one of the top concerns of governments. Consumers want to know that their personal information is protected when making online transactions. Online privacy protection laws aim to ensure the safety of consumers when sharing their personal information with businesses. There are several different online privacy laws that businesses must comply with. These are to prevent advertising fraud, protect information under the age of 13, and force businesses to openly disclose the information they collect. In comparison to their American or Asian equivalents, the European Commission has made significant advances in legislating consumer data protection rights (Jayakumar 42). According to Pantelic et al., a link to the privacy policy or cookie policy page, whichever is describing admission requirements, is one of the criteria observed for evaluating the site's GDPR compliance. Other criteria include information on data sharing with third parties, acceptance of cookies, and a description of the method of using cookies. Although the CCPA (California Consumer Privacy Act) contains comparable standards, the primary distinction is that some cookies can be downloaded without authorization and an opt-out option is necessary to

prevent information from being sold to third parties (Pantelic et al. 5). According to Jayakumar, the benefits of GDPR for the protection of personal information cannot be denied, but some of the biggest failures of this system are that privacy regulations cannot be adequately controlled, and visitors are not aware of their rights (Jayakumar 31).

While third-party cookies have already been blocked by major online advertising companies and browsers, including Apple, Microsoft, and Mozilla, Google claims they will remove cookies in a few years (Jayakumar 31), despite the continued delay of the Privacy Sandbox. After a few years, third-party cookies may appear invalid and individual consent may not be required for each website (Jayakumar 42). The effectiveness of privacy policy laws depends on the level of knowledge consumers have about their rights, the working principles of cookies, and the impact of cookies on their personal information (Pantelic et al. 12). Considering that many people will not investigate this issue, legal protection of privacy rights in the internet environment will not go beyond having a compelling effect on companies and will either become dysfunctional or aggravate and negatively affect the industries. Research conducted by Nelissen and Funk on 33 designers of varying professionalism proves how GDPR makes businesses feel. At the end of the research, according to the explanation of some of the designers who made unethical designs by not complying with the "Privacy by Design" rules of GDPR, the reason for this attitude was the reasons such as the customers' unwillingness to compromise their design needs or their responsibilities to their employers (Nelissen and Funk 86). These people or businesses ask their designers to design this way because they think that they are unnecessarily giving up this data and that it will harm their business activities if they comply with the law.

2.2.5. Analyze the data:

After an in-depth analysis, briefly examining the “Browser Privacy Mode”, “VPN”, “Privacy Sandbox”, and “Privacy Protection Laws” the author realized that each has its own unique structure. In special cases, they can produce excellent solutions to privacy problems; the Google Privacy Sandbox is perfectly designed. Considering its structure and features and ignoring its working principles, it stands out as a system that can really solve the privacy problem and offers a very successful solution to the user experience problem arising from the privacy protection method. On the other hand, VPN offers a near-perfect solution to privacy issues. In this respect, browsers’ privacy modes are very similar to VPNs, but privacy protection laws are probably the best solutions. The advantage of privacy protection laws is government control, which compels firms to comply with ethical rules. Of course, although these systems solve the problem from their perspective, they cannot solve the problem exactly as the author intended because they often focus on maintaining the privacy and nothing else.

As for why these techniques fail, it is not possible to examine them as a group because they all have different failures. First, if “Browser Privacy Mode” is taken into consideration, according to the literature, this technique is not successful because it can expose personal information even more. When looking at the working principle while many browsers work in privacy mode, third-party cookies are generally blocked by default. Even if third-party cookies are in use, they are stored in a temporary file and are deleted when the browser is closed. The device can only be tracked as the browser is kept open. From this point of view, although it is technically successful in terms of protecting personal information when it comes to user experience, it is a complete failure because every time a browser is opened, the device can browse the sites as if it is a newly formatted device, without remembering the previous visits. Although VPNs are more successful

in this regard, since many modern websites try to protect themselves from attacks by using IP blocking systems, the IP addresses given to the device by VPNs can be determined as dangerous and cause the device to be blocked out from the sites. Also, VPNs are often paid, otherwise limited services. If it's paid, the VPN offers as much protection as it's paid for, but if it's free, the consumer is the product. In other words, VPN companies usually sell consumer information to provide this service for free. But what about the Privacy Sandbox, a free system designed purely on perfection? It does not sell personal information as personal information.

The failing point of Privacy Sandbox is that it claims that only Google can see the information and most people think that it is the scariest part. Yes, as discussed in the literature, Google does not share private information with advertisers directly, but Google can see the information and group them with the same or similar people and not fully but partially and a little more anonymously sells the information as advertising data. As a result, these solutions either do not completely solve the problem or create different user experiences or privacy issues while trying to solve the problem. This is because many of these solutions persistently refuse to use decentralized data communication (web3) techniques.

2.4. Blockchain & Decentralized Network:

The decentralized network, which is one of the most important topics in the marketing industry today, is a new infrastructure for digital marketing that uses blockchain technology that brings a brand-new breath to digital marketing. The concept of blockchain can be compared to the internet with its feature of hosting many technologies and applications (Wajde et al. 79) and blockchain has the potential to reshape digital advertising (Hahn et al. 28). According to Ertemel, blockchain uses cryptography technology and peer-to-peer computing to enable secure and direct transactions without middlemen (trusted third parties) (36). Blockchain is essentially a

decentralized ledger, that is shared and agreed upon among a peer-to-peer network (Jain et al. 2; Ertemel 36). It is impossible to access this feature of the blockchain using other technologies (Madhani 11). One of the main reasons for having a reliable mediator is to believe that when an unexpected event occurs, the situation will be resolved fairly. Blockchain is using self-executed smart contracts, so it does not need such third parties. To do this, all parties sign an unalterable, programmed contract called a smart contract (Madhani 12). In other words, smart contracts program all the possibilities that may occur, and what will happen when that situation occurs is specified in advance (Wajde et al. 84). It is important to consider the problems that may arise while preparing smart contracts and include them in the contract. For example, if the seller cannot deliver the product or the service in the promised conditions, the payment made by the consumer will be refunded (Ertemel 40). However, there is still a lack of direction on how organizations may use this new technology to improve consumer experience and engagement. According to Chang and Hsieh, blockchain technology is no longer in baby steps; it is growing (27) and as it grows, organizations are forced to adopt it.

Decentralized (Blockchain based) marketing is a concept that has been brewing for several years. It has been suggested to disrupt the current marketing industry and improve how businesses interact with their customers (Madhani 7). Decentralized marketing has set up a platform where the consumer is the owner of the data and can sell their data if they want to. It seems that with this new marketing system, companies that are third parties, between the advertiser and the consumer, will be eliminated (Ertemel 35). Thus, companies will be able to make more successful advertising campaigns at lower costs and consumers will be able to get real value from the advertisements they see.

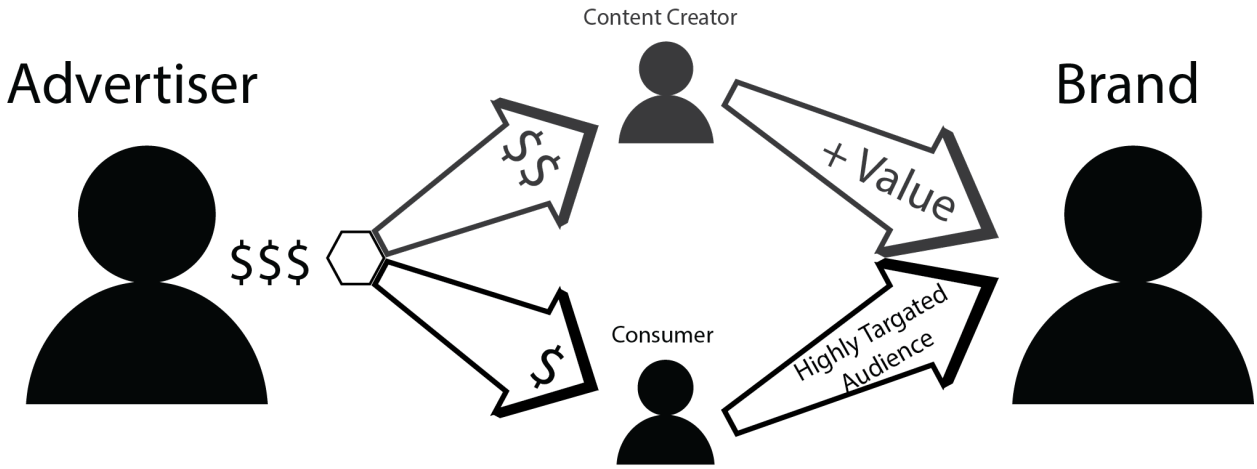


Fig. 3: Decentralized Digital Marketing

Decentralized marketing is a marketing approach that focuses on the single platform user experience and, more importantly, the relationship between the brand and the user. In order to create more direct and close relationships with consumers, brands need to move away from using intermediaries (trusted third parties) in their online advertising campaigns and pay more attention to finding ways to encourage and/or reward consumers for sharing their personal information (Boukis 317). The aim is to improve the storytelling practices behind diverse portfolios of brands and improve internet usage by designing more informative, authentic, and interactive experiences among businesses, consumers and creators (Madhani 14). According to Routray, Blockchain-based businesses offer applications like the Basic Attention Token (BAT) that change the way advertisers, users, and publishers interact through the Brave platform. Powerful ad blockers and tracking blockers are included in the Brave Browser by default (Hahn et al. 26) to override the ads supposed to be displayed by trusted third parties. With this method, consumers will be able to choose to see only the ads related to the topics they are interested in, as much as they want, or not to see any ads at all. If a user sees an ad, a small portion of what the advertiser pays to purchase the ad is paid to the person who sees the ad, and a larger portion to

the publisher in BAT (Routray 56). “Browser-based Contextual Marketing”, would be a nice name to call this marketing technique. According to Chang and Hsieh, the consumer gets 70% of the payment made for that ad (33). The pay rate may have changed in the time between these two studies, but the fact that consumers are paid BAT for the ads they see has not. BAT is a token created in blockchain that challenges digital marketing networks through the Brave browser using the technology backed by Brendan Eich, the creator of JavaScript and co-founder of Mozilla and the world-famous Firefox browser (Hahn et al. 26). BAT claims that it will eliminate the need for digital advertising platforms by establishing more reliable partnerships. These benefits will prompt consumers to quickly adopt these platforms.

Based on the qualitative expert interviews done by Hahn et al., the main problem with decentralized marketing is a lower number of active users. Other than that, decentralized marketing is way more beneficial for both parties compared to centralized marketing and has the potential to reshape digital advertising (Hahn et al. 28). The graphic below by Boukis provides easy-to-understand information about the benefits of decentralized marketing and the benefits of adaptation (The image was redrawn for clarity purposes)

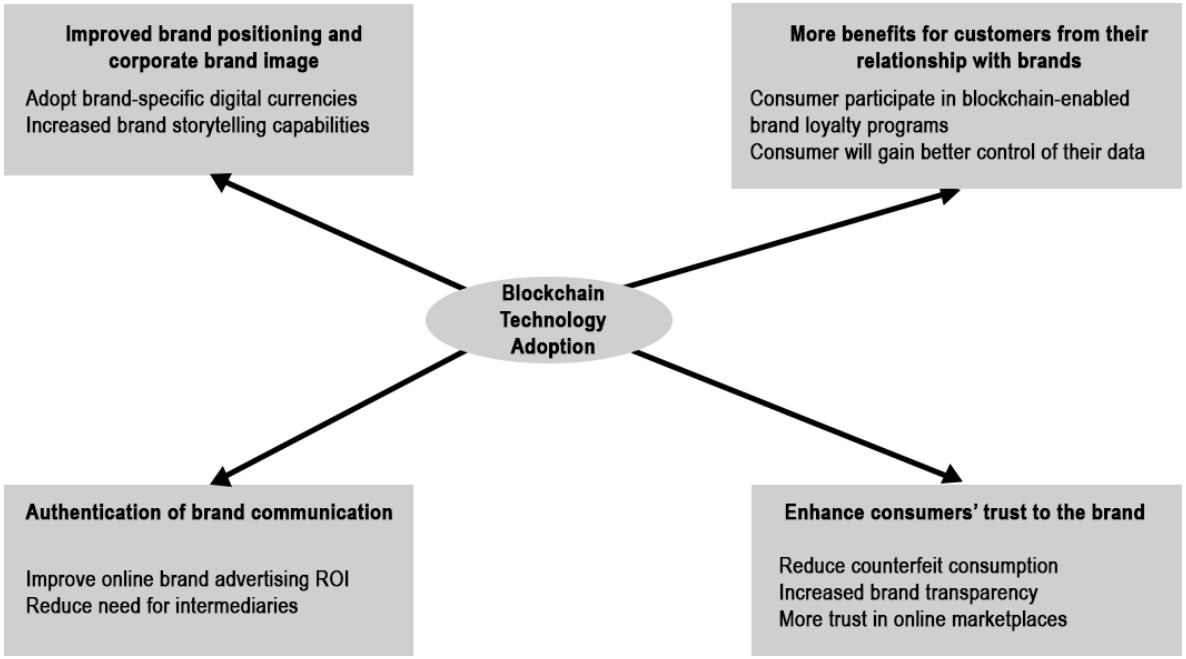


Fig. 4: Boukis, Achilleas., Figure 2, p. 310

Also, over time, all industries will be built on decentralized platforms, starting from the industries with low trust such as diamond merchants, art dealers, and banks (Boukis 310). As it is known, the marketing industry is among the most untrusted sectors in the world (Ertemel 36), so it will inevitably be taken over by decentralized marketing, and its structure will be changed completely. It is said that the use of such a core technology by businesses already has an impact on company marketing performance, especially in multiple areas such as brand messaging, internet marketing campaign design, and brand transparency for consumers (Boukis 308).

3. Methodology:

The information for the research was collected in two different stages and they aim to reach two different results. The first research was carried out to reveal the extent of the problem by measuring the number of files that visited websites leave on users' computers and are generally used to prove the existence of the issue. While conducting this research, the "Top 100 most visited websites in the world" list shared by Ahref, a program frequently used by digital marketers, was used (Hardwick). At the end of the research, the list of the visited websites can be found (see page 54). Before starting the investigation, the device to be used in the research, a MacBook Pro with macOS Monterey V12.6, was completely cleaned of leftover files using the CCleaner software. During the research, the Bitdefender virus protection software was passively run in the background for security purposes. After the system was prepared, the determined websites were visited using the Chrome Browser for at least 30 seconds each to let all the scripts fully load. Then, the number of files left by these websites on the system was measured by using the CCleaner program again, the system was cleaned again, and the same measurement was repeated using Brave Browser with the same standards. Since the second stage of the research is to examine how these files, which are proven to exist and are released to user devices as a result of visiting websites, affect the user experience, at least 100 people were asked to fill out the survey. The survey was provided to these people to learn about their user experience without third-party cookies, how safe they felt, and what they thought about web3 marketing techniques.

- Copy of Brave Browser user experience questionnaire:

1) How long have you been using Brave Browser?

   Options are "less than 30 days" and "more than 30 days". To continue, the user needs to answer "more than 30 days" here or the survey ends.

2) How would you rate your overall experience?

The options are “Far below average”, “Somewhat below average”, “Average”, “Somewhat above average”, and “Far above average”.

3) What OS (Operation System) did you use?

The options are “IOS (Mobile Apple Devices)”, “macOS (Apple Computers)”, “Android (Most Mobile Devices Other Than Apple)”, “Windows (Most Computers Other Than Apple)”, “Linux (Not Very Common OS for Mostly Computers)”, and “Others”.

4) Compared to your previous browser, how would you rate the browsing/loading speed?

The options are “Extremely slow”, “Somewhat slow”, “Average”, “Somewhat fast”, and “Extremely fast”.

5) How would you rate your ad experience? (Do not consider Brave Ads If Allowed)

I see more ads than I used to see in my previous browser.

I see fewer ads than I used to see in my previous browser.

I do not see ads, but I see a black screen when the ad is supposed to be displayed.

I do not see ads, but the experience is not seamless.

Great experience. I cannot even say where the ad that Brave removed was.

6) How safe do you feel when browsing with Brave?

The options are “Extremely negative”, “Somewhat negative”, “Average”, “Somewhat positive”, and “Extremely positive”.

7) If you activated, how do you like Brave’s reward program?

I didn’t activate it.

Activated but haven't seen any ad nor made any BAT coin.

Activated, saw ads, but didn't receive any BAT coins.

Activated, didn't see any ads but earned some BAT coins.

Activated, saw some ads, and earned some BAT coins.

8) How was your Cross-site and Cross-platform experience? (Sign in/out processes, remembering your settings/passwords/form inputs/shopping history/etc.)
The options are "Terrible", "Poor", "Average", "Good", and "Excellent".

9) How likely, will you continue to use the Brave browser as your primary browser?
The options are "Extremely unlikely", "Somewhat unlikely", "Average", "Somewhat likely", and "Extremely likely".

10) Do you allow your answers to be used anonymously in research? If yes, please sign.

3.1. Measuring the files:

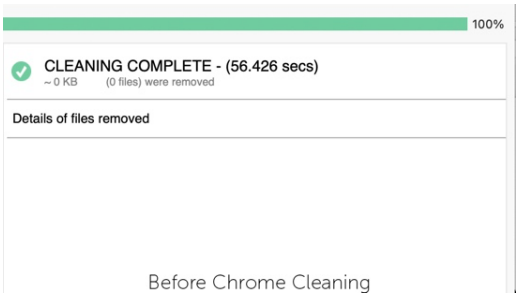
3.1.1. Which websites and why:

The websites used in the research were selected by Ahref and published as the 100 most visited websites on their website (Hardwick). Ahref is a software company founded in 2010 that currently has a database of 12 trillion links and provides SEO tools for marketing professionals such as a site crawler, backlink checker, and keyword research tool. A detailed list of visited websites can be found at the end of the research.

3.1.2. How the data was measured:

The files and cookies left in the computer by visited websites were measured using software called CCleaner. In computing, CCleaner is a utility used to clean operating systems and improve performance. CCleaner removes temporary files, internet history, cookies, and other junk

files that can clog a system and cause the system to run slower. It also has a registry cleaner to fix common problems with registry entries that haven't been used for the research. In order to make an accurate analysis, CCleaner software was used to clean the files and other content left by the websites on the computer before using both browsers.



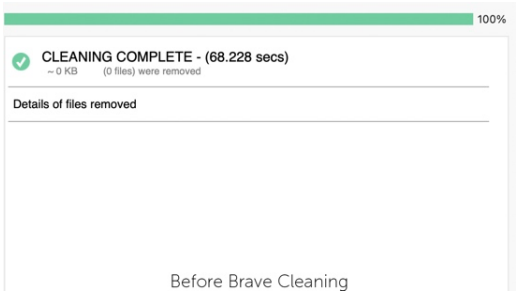


Fig. 5-A: Before using Chrome Browser *Fig.5-B: Before using Brave Browser*

3.1.3. Chrome's results:

After cleaning the operating system (Fig. 5-A), 100 selected websites were visited with Google Chrome and at least 30 seconds were waited for all scripts to be fully loaded and HTTP requests completed. After visiting all sites, Google Chrome was completely disabled, so that it could not block access to the files it created, and CCleaner was run again and the total size and amount of newly created files by the computer were measured. A screenshot of the results, Figure 6, is shared below.

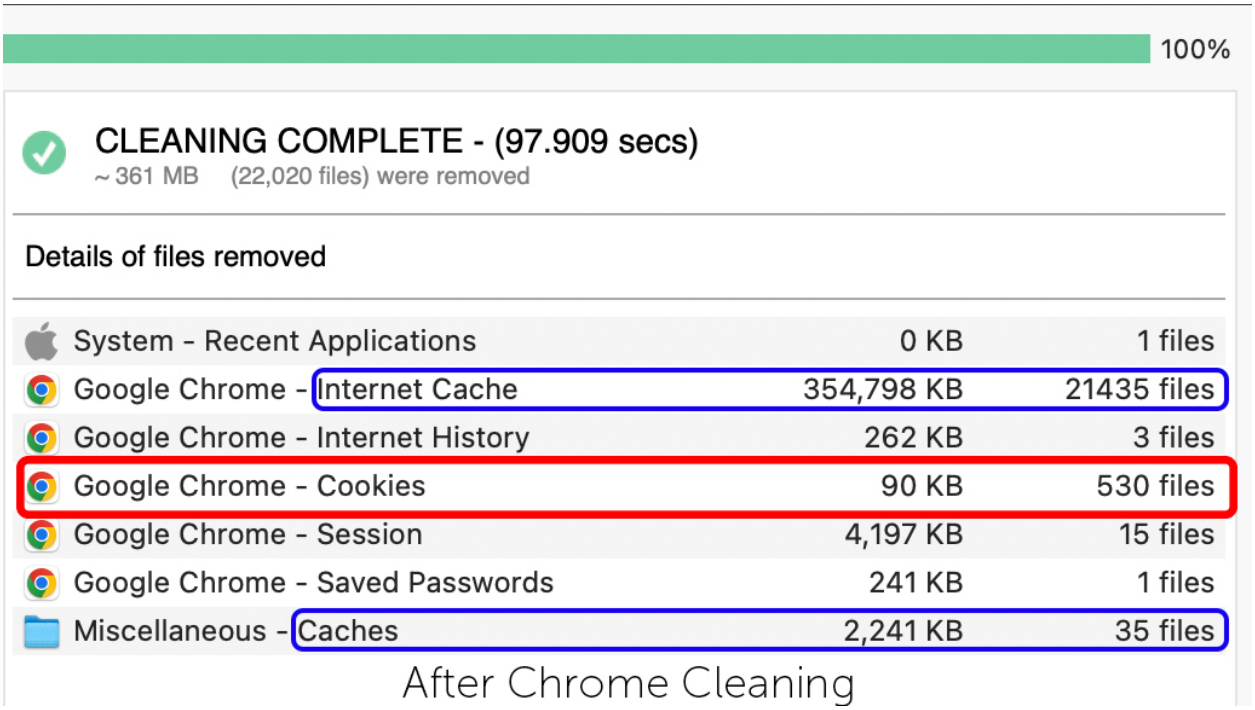


Fig. 6: Chrome Browser Results

As a result of the scan, 22,020 new files with a total size of 361MB were created, according to CCleaner data. Although the majority of these files are cache files, it is seen that a total of 545 third-party cookies, 15 of which are session cookies, are placed on the system. As it can be understood from here, 530 of these cookies are cookies that can provide long-term tracking across platforms and do not expire once the session ended.

3.1.4. Brave's results:

Before using Brave Browser to revisit the 100 selected websites, the operating system was cleaned again using the CCleaner software (Fig. 5-B). The same procedure was applied again, without changing any variables, as before in the Chrome Browser. The 100 selected websites were visited in the same order and waited at least 30 seconds for all scripts to load and HTTP requests to complete. The results can be seen in the screenshot below (Fig. 7).

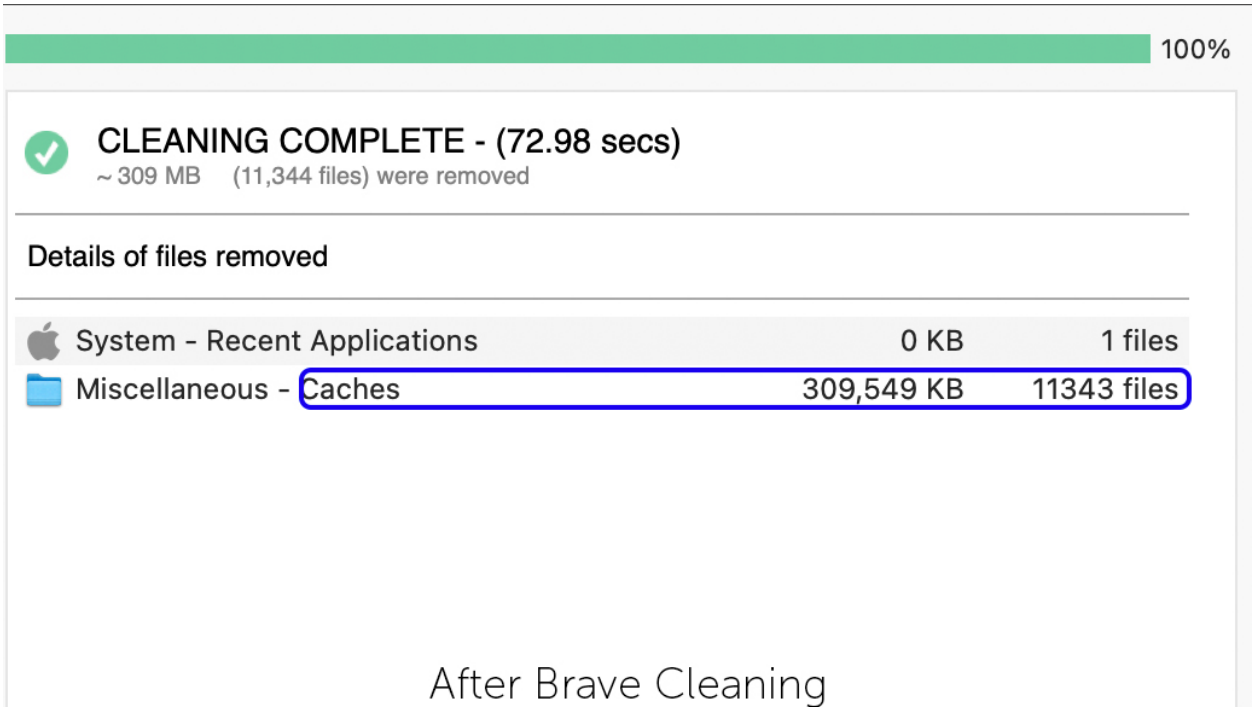


Fig. 7: Brave Browser Results

As a result of the scan, 11,344 files with a total size of 309MB were detected. No cookie files were found among these files. It was observed that the number and size of cache files were lower than scanning done after the Chrome Browser experiment. Although it is thought that the reason for this change is that Brave Browser does not download advertisement files because it blocks platforms such as AdSense along with many pop-ups, this research does not provide definitive information as it was not conducted to determine the reason for this.

3.1.5. What caused this result:

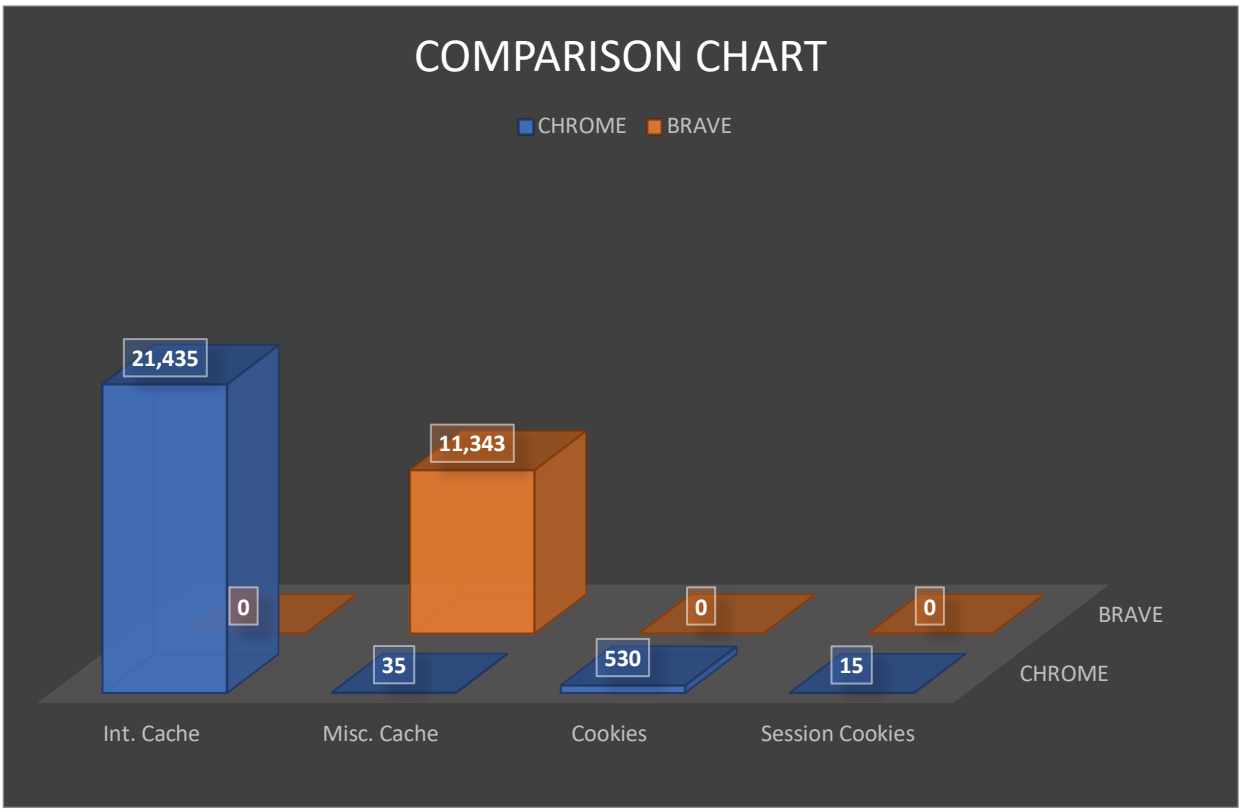


Fig. 8: Chrome vs Brave Comparison Chart

Although both browsers have chromium infrastructure, they are quite different from each other in terms of working principles and the results they are trying to achieve. While Google Chrome's priority is to generate data that can be sold by Google, Brave protects personal information and generates its income from browser-based contextual marketing techniques, as named earlier. Brave browser prevents users from being tracked by blocking all third-party cookies. While it provides a more private experience to its users as it blocks many ads and pop-up messages, it provides a higher loading speed and less data usage as it does not load unnecessary files and stops HTTP requests. This is very useful, especially for users with limited internet access.

3.2. Analyzing Brave Browser:

3.2.1. How the survey was published:

In order to understand the usage and user experience of the Brave browser, surveys were conducted and responses were collected through various methods. The questionnaire was created and distributed over www.qualtrics.com. The survey aimed to collect data on the features and functionality that users found most valuable, and areas for improvement that could be addressed.

The survey was first shared with friends on personal social media accounts to reach the target audience. Unfortunately, the number of responses received was not as high as anticipated. In order to increase the number of responses, the survey was shared on various social media platforms such as Facebook, Instagram, and LinkedIn by joining Brave browser and technology-related groups. The survey was also introduced on blogging platforms such as Reddit and Quora to reach a wider audience. Despite these efforts, the response rate was still unsatisfactory.

As a final method, paid ads through the Meta platform were used to spread the survey worldwide without any geo-restrictions. This allowed the survey to reach a wider audience and collect more diverse responses. The data collected from the survey is anonymous and although stated in the advertising reports, the geographical location of the volunteers was not taken into consideration.

The results of the survey provide valuable information about the use and user experience of the Brave browser. The data collected from the survey will be used to better understand the factors that influence users' decisions and experiences when using the Brave browser. The survey results will be used to identify the most important features and functions for users and inform the development of the author’s software idea, which aims to address issues related to internet privacy and user experience, as well as areas for improvement.

Gratitude is extended to 122 volunteers who generously shared their time and insights in the survey, which significantly contributed to the development of the research. The feedback received through the survey is immensely valuable, and the effort put forth by each participant is appreciated. Additionally, the platform provided by Qualtrics was instrumental in conducting the survey. Based on the survey's results, further feedback will be gathered and the research will be continuously updated.

3.2.2. What are the overall results:

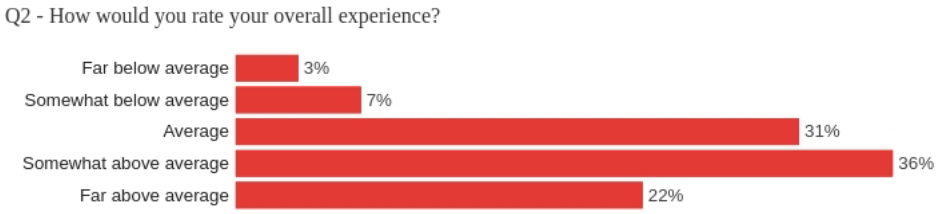


Fig. 9: Overall Experience

According to the answers, it is clear that the Brave browser has advantages and the vast majority of users report a positive experience. However, the results also highlight areas where the browser can be improved. A small percentage of users reported a negative experience, stating that the browser is not perfect and is open to improvement.

Despite its unique features such as privacy protection and a built-in cryptocurrency wallet and rewards system, the Brave browser still faces challenges in providing a seamless user experience. For example, users who rated their experience as "slightly below average" or "well below average" may have encountered issues with the browser's performance, compatibility, or usability. Many of these will be answered in the next survey questions. So, while the Brave browser is a good solution, it's important to acknowledge its limitations and areas for improvement.

3.2.3. What are the device-specific results:

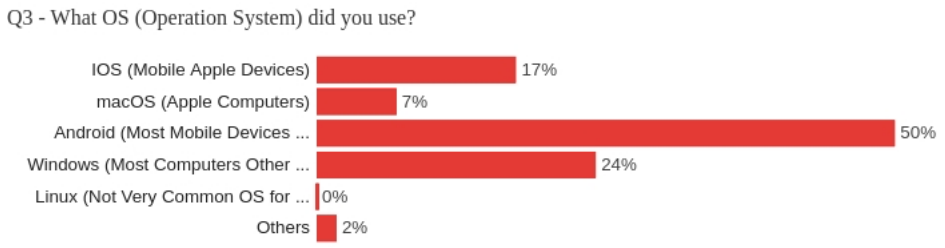


Fig. 10: Device-Specific Results

Looking at the answers on the operating systems used by Brave browser users, it is seen that the browser has a diverse user base. The majority of users in the survey were Android users, representing 50% of the report. Windows users accounted for 24% of the comments, while iOS users represented 17%. Finally, macOS made up only 7% of users and Linux users represented 0%.

A high percentage of Android and IOS users (67%) state that mobile users are more likely to use the Brave browser. This may be because of the browser's data saving and privacy features, which are particularly applicable to mobile users with limited data plans and who may have concerns about online privacy and security. The relatively low percentage of macOS and Linux users indicates that the Brave browser may be gaining more traction among Windows users on devices with larger screens.

3.2.4. What shaped their opinion:

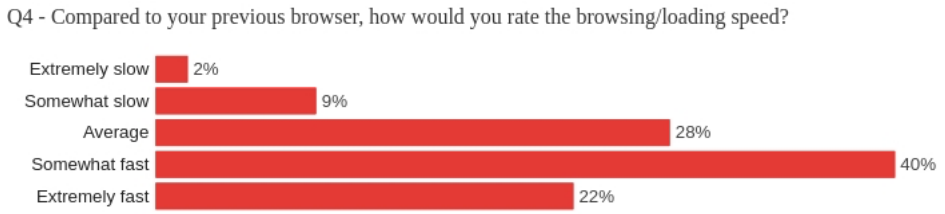


Fig. 11: Browsing/Loading Speed

The answers to Q4 show that the majority of Brave browser users rate the browsing/loading speed positively, with 40% saying it's somewhat fast and 22% thinking extremely fast. However, some users (9%) found it a bit slow and 2% rated it too slow. Overall, positive scores indicate that removed third-party cookies and ads that don't load have a noticeable effect on speed.

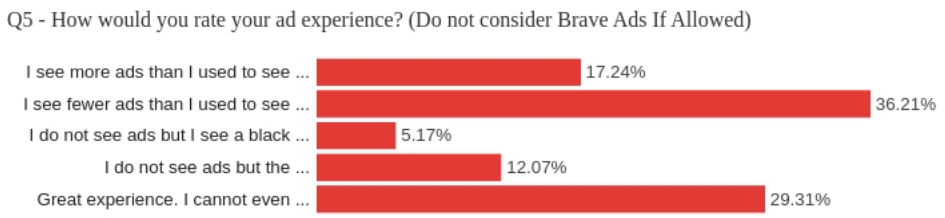


Fig. 12: Ad Experience

The answers suggest that Brave browser's ad-blocking feature is generally well-received by its users. A majority of respondents (65.52%) reported seeing fewer ads or having a great ad experience (29.31%) with the browser. However, a small percentage of users (17.24%) reported seeing more ads than they did with their previous browser. Additionally, a small group of users (17.24%) reported issues with the ad-blocking feature, such as a black screen instead of the ad or a non-seamless experience. Overall, the data suggest that Brave's ad-blocking feature is effective for most users, but there may still be room for improvement to address issues experienced by some users.

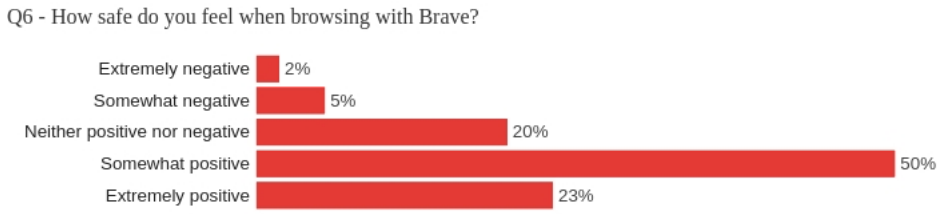


Fig. 13: Feeling Safe

The answers to the question suggest that a majority of Brave browser users feel safe when browsing with the browser. Nearly three-quarters of the respondents (73%) reported

feeling either somewhat positive (50%) or extremely positive (23%) about their safety when browsing with Brave. However, a small percentage of users (7%) reported feeling either somewhat negative (5%) or extremely negative (2%) about their safety when using the browser. These findings suggest that while Brave has made strides in providing a secure browsing experience, some users may still have concerns about their safety when using the browser.

Fig. 14: Reward Program

The answers to the survey question on Brave's reward program indicate that a significant percentage of users have not activated the program, with 31% of respondents indicating that they did not activate it. Among those who activated the program, 11% reported not seeing any ads or earning any BAT coins. This may suggest a need for improved communication or education about the reward program and how it works.

Interestingly, 13% of users who activated the program reported earning BAT coins even though they did not see any ads. This could mean the reward program also offers BAT tokens for simply using the browser, regardless of ad viewing. However, 24% of respondents reported seeing ads but not receiving any BAT coins, indicating a possible issue with the reward system.

Overall, the results suggest that while the reward program may be appealing to some users, there is still room for improvement in terms of user education and reward distribution. There are also some technical issues that exist in the system.

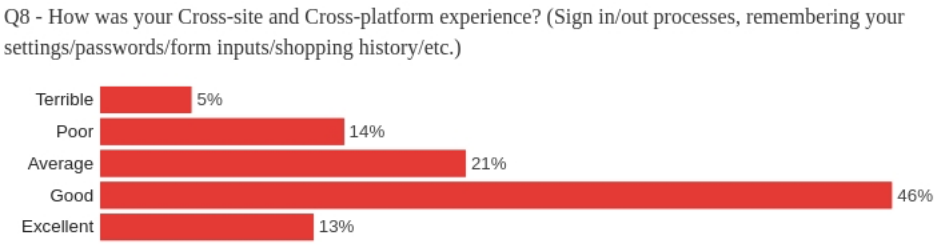


Fig. 15: Cross-site & Cross-Platform Experience

The results suggest that the majority of Brave browser users reported a positive experience with cross-site and cross-platform functionalities. More than half of the respondents (59%) rated their experience as either good (46%) or excellent (13%). However, a notable percentage of users (19%) rated their experience as either terrible (5%) or poor (14%), indicating that there may be room for improvement in terms of cross-site and cross-platform functionalities. Users who rated their experience as poor or terrible may have encountered issues with sign-in/out processes, remembering settings, passwords, form inputs, or shopping history, among other things. These findings suggest that there may be areas where Brave browser could benefit from improvements to ensure a more seamless and user-friendly experience for all users.

3.3. Analyze the data:

A recent study analyzed the performance and user experience of two popular browsers, Google Chrome and Brave, with a focus on privacy and data tracking. The study used CCleaner software to measure the amount of data and newly created files on the operating system after visiting 100 selected websites with each browser. The results showed a significant difference in the amount and type of data generated by the two browsers.

The scan of the operating system after using Google Chrome showed the creation of 22,020 new files, with a total size of 361MB, and 545 third-party cookies were placed on the system, with only 15 being session cookies. Furthermore, 530 of these cookies were long-term

tracking cookies, which can provide tracking across multiple platforms and do not expire once the session ends. In contrast, the scan of the operating system after using Brave Browser showed only 11,344 files with a total size of 309MB, with no cookie files found among these files. The results suggest that Google Chrome prioritizes generating data that can be sold by Google, while Brave focuses on protecting personal information and generating its income from browser-based contextual marketing techniques.

Based on the survey results, it is clear that the Brave browser is generally well-liked by its users, with the vast majority reporting a positive experience. The browser's unique features such as ad blocking and privacy protection, a built-in cryptocurrency wallet, and a rewards system have proven to be popular among users, particularly those on mobile devices. However, the results also indicate areas where the browser can be improved, such as browsing and loading speed, cross-site and cross-platform functionalities, and the reward program.

The browsing and loading speed results show that while the majority of users rate the speed positively, some users still find it slow. This may suggest that there is room for improvement in terms of optimizing the browser's performance and compatibility, particularly for users who have encountered issues.

The ad experience results suggest that the Brave browser's ad-blocking feature is generally well-received by users, with a majority reporting a better ad experience. However, a small percentage of users reported issues with the ad-blocking feature, indicating that there is room for improvement in terms of providing a seamless experience for all users.

The feeling-safe results show that a majority of Brave browser users feel safe when browsing with the browser, but some users still have concerns about their safety. This may

indicate that there is a need for improved communication about the browser's security features to address user concerns.

The reward program results suggest that while the program may be appealing to some users, there are many problems in terms of user education and reward distribution. Some users have reported technical issues with the reward system, and a significant percentage of users have not activated the program at all. This may be due to the complexity of activating the rewards, the inadequacy of the rewards, or the insufficient information given to the users about the rewards.

Finally, the cross-site and cross-platform experience results show that while the majority of users rate the experience positively, there are still some users who have encountered issues. The research findings suggest that users may not be fully aware of their security levels and outcomes when using the Brave browser. This could be attributed to the varying information deletion settings across different browsing scenarios, such as the deletion of data only when the browser is closed versus every time a window is closed. Moreover, the study's observation that users have a seamless cross-platform and cross-site experience without relying on third-party cookies raises questions about how Brave manages and transfers user data. While secure cloud-based transfers are feasible between platforms, the mechanism for cross-site data migration, which involves tracking user behavior across unrelated websites, may require further investigation. Survey results highlight the need for greater transparency and understanding of Brave's data management practices to ensure users' privacy and security.

Overall, the study and the survey results provide valuable insights into the Brave browser's strengths and areas for improvement. While the browser has proven to be a good solution for users looking for privacy protection and a built-in cryptocurrency wallet and rewards system, it

is important to acknowledge its limitations and areas for improvement. By addressing these areas, the Brave browser can continue to improve and provide a better user experience for all.

3.3.1. Is the problem real?

Web browsers pose significant challenges to user privacy, data tracking, and user experience, as revealed by a study and survey conducted in this research. Specifically, the study focused on two popular browsers, Google Chrome and Brave, and compared their performance and user experiences in terms of privacy and data monitoring.

The study found that Google Chrome generates a significant amount of data that can be used/sold by Google, while Brave prioritizes protecting personal information and monetizing its browser-based contextual marketing techniques. However, despite being better than some alternatives, the study identified several areas where the Brave browser could be improved, such as working, browsing, and loading speed, cross-site and cross-platform functionalities, and the rewards program.

It is worth noting that the study found that Brave browsers' privacy protection methods may cause more significant issues with user experience than privacy itself. This may be due to the fact that these methods often lead to lower cross-site and cross-platform experiences.

Both browsers can provide good enough cross-platform experiences whereas Chrome can also provide a very good cross-site experience but transferring data between websites (for Brave only) and browsers can be challenging, with cross-browser transfers being particularly difficult for both. While solutions like Brave browser may be helpful, they may not fully address these issues. One of the main challenges is that browsers have limited access to other browsers' history files and settings, making it difficult to implement the cross-browser UX technique without third-party software support. Even with this support, the technique can only be applied to a single device and

cannot be synchronized across different browsers on different devices. Additionally, without blockchain technology, transferring data between devices cannot guarantee complete security during and after the transfer even if it is made possible.

Ongoing efforts are needed to address privacy and data tracking concerns in web browsers. While the Brave browser and other privacy-focused solutions do offer some level of protection, they may not be perfect and cannot solve all the issues related to user privacy and data tracking. Therefore, it is crucial to continue identifying areas for improvement and developing new solutions that can effectively address these concerns. However, these solutions may still have limitations in terms of providing seamless data transfer between different browsers on different devices, which is an issue that has possibly not been addressed in any other previous research.

3.3.2. What is the suggested method by the author?

Considering the data obtained by the author as a result of the research, the problems that need to be solved can be examined under four main headings: ‘Security’, ‘Accessibility’, ‘Privacy’, and ‘User Experience”. Malicious attacks like cross-site scripting, memory overflows, session hijacking, and others, can be prevented by removing cookies from the client side but then DoS and DDoS attacks can affect the server side (Al-Ibrahim et al. 312). Based on the findings, the most suitable infrastructure in which solutions can be applied is the blockchain infrastructure. According to Boukis, even though frameworks such as GDPR that try to guarantee the privacy of user information come into effect in the EU, the data anonymity technology of blockchain has the potential to be the definitive solution to this problem (Boukis 316) since blockchain is distributed, encrypted, and public, that makes blockchain infrastructure extremely highly secure by nature (Chang and Hsieh 29). On the other hand, blockchain technology is also divided into three different levels of privacy. Private Blockchain is the most suitable infrastructure for the solution path that

will be specified here, as it can be configured to give users different levels of access to data (Madhani 10-11).

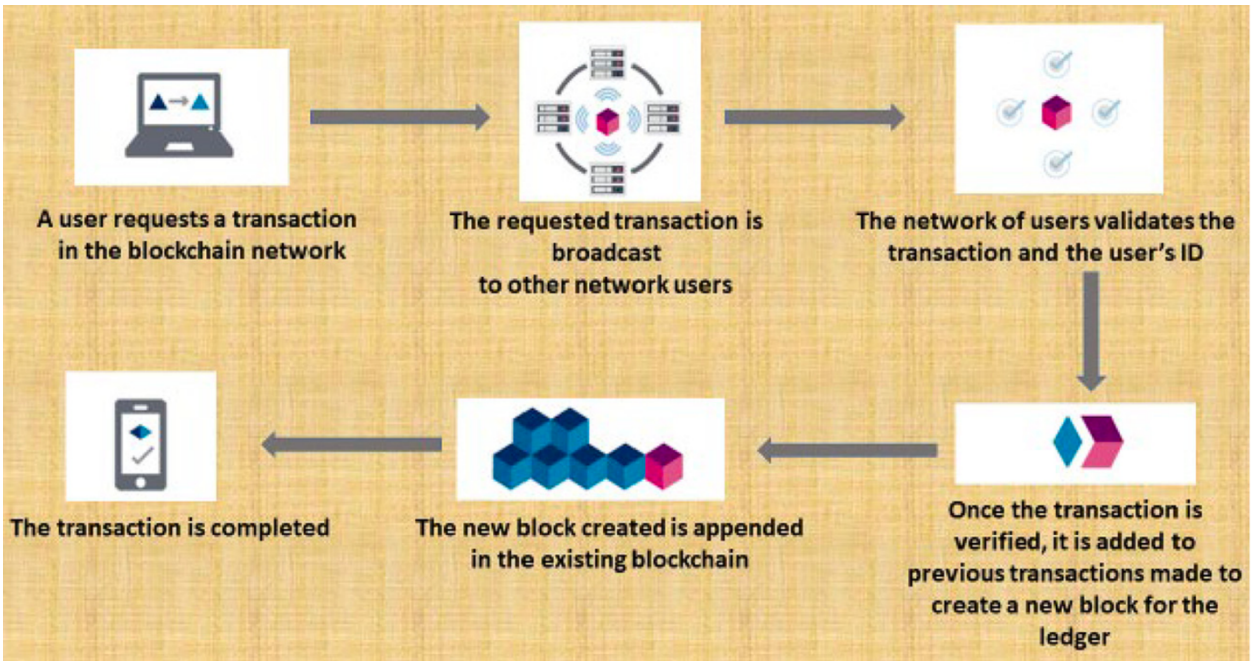


Fig. 16: Boukis, Figure 1, p. 309

The author gives the name "Privacy Wallet" to the technique since the solution is similar to the working principle of a browser-based crypto wallet and is used for managing private keys. One of the most important features of Privacy Wallet is that it will be a dapp (decentralized application) on the PWC (Privacy Wallet Coin) network which needs to be built along with the private blockchain for Privacy Wallet. Thus, it will be free, easily accessible, secure, and quickly adaptable to new developments and changes. Ad buyers will have to cover the transaction cost, known as the gas fee in the Ethereum network, due to the execution of the smart contract, along with the financial or moral values they will provide to the customer every time they want to purchase customer information. Since Privacy Wallet derives its main operating power from the very small processor power that each device donates in exchange for free transactions, these

transaction fees can be used to monetize Privacy Wallet, increase the value of PWC, or invest in it to improve the system by adding more processing power.

In order to solve security issues, a Privacy Wallet should be created using private blockchain technology. At the same time, each device that the Privacy Wallet is being used on will act as a node (device) in the network and host the distributed data blocks of other users to reduce the risk of 51% attacks, provide some storage, and processing power to keep the service free. If attackers can control 51% or more of the network, they can manipulate the blockchain (Wajde et al. 105) but the technique the author suggests very likely solves the problem since the number of devices in the network will be extremely high. As a secondary shield of protection, the blockchain will be set to not allow any account to control more than 49% of the network. So, if the main account, which gets the transaction fees, wants to add processing power to the network, it will have a chance to almost double the power but no one can own the network. The widely distributed database of blockchain prohibits any party from controlling the flow of information and allows other parties to immediately check the transaction partner's records without the need for middlemen (Boukis 309). In other words, while the nodes in the network automatically check the accuracy of the transferred data and ensure its security (Madhani 11), they do not have the authority to change this data. Data contained in the Privacy Wallet can be accessed only via the blockchain network, even if the visited website, web server, or user's computer is hacked, hackers will never be able to access this data. Even if the user password is captured by tracking the user's keyword strokes with software called keyloggers, this captured password will never be able to be used to access the account since recovery phrases will be required for every newly added device.

In order to avoid accessibility problems, unlike Google Privacy Sandbox or Brave Browser, this software created must be compatible with all devices, all operation systems (OS), and all

browsers. To provide this quickly and simply, it will be sufficient to ensure that the software remains open source.

When it comes to privacy issues, since all the user's information, name, last name, address, phone number, age, place of birth, internet history, school attended, credit card information, etc., will be coded separately, the user must decide once and for all which information to give access to every single domain he visits. These permissions will be decentralized into the Privacy Wallet to ensure the continuity of the user's experience on that site on different devices and the data neither saved into the web servers nor the user's devices. In addition, the user will be able to change the privacy settings at any time for any domain. At this stage, users can be granted the right to create ready-made profiles to be easily used on similar sites.

In the solution to UX problems, the fact that the data is stored in the cloud will allow access to this data from any operating system on any device, and even if the browser changes, the UX will never be interrupted unlike the other solutions including Brave Browser. The Privacy Wallet will also be activated with a single password, and from that moment on it will remember all the information on all visited sites. Since the main security is provided with key phrases, the password can be set to be saved in the devices and not be asked every time for a seamless experience. The biggest advantage of this system for UX, for example, is that the history created using the Safari browser on a macOS-based mobile device will continue from where it left off, even if a Mozilla browser is used on a computer running Windows OS.

While it is impossible to manipulate user data in the Privacy Wallet, it is not impossible to ethically access user data for marketers. According to the results of Jayakumar's quantitative research (see Fig. 17), users are not against sharing their data or being monitored. They just want

to decide for themselves whether to share their data and they want to know where and how long the data they shared will be used. They simply want to be in control of their own data.

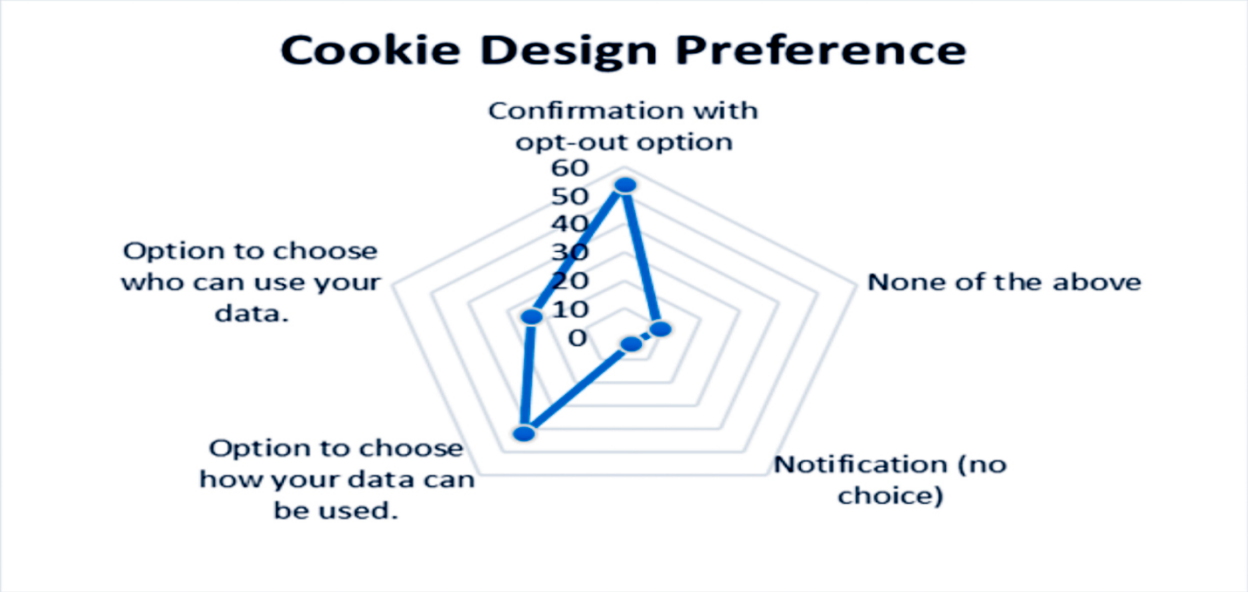


Fig. 17: Jayakumar, Chart 6, p. 37

As mentioned earlier, with Privacy Wallet, the user has the right to share the requested information with companies. Users will voluntarily share the encrypted data with hash algorithms if businesses can make an appropriate offer in exchange for the user's information. This encrypted data-sharing technique can protect users' data from being saved. This is essentially similar to the sales funnel technique commonly used today. This system directs companies to get user information and even statistics and histories using zero-party cookies, which means "no cookies". This system will also naturally eliminate the problems such as click fraud, which is often experienced in PPC (Pay Per Click) campaigns, and will ensure that the ads are much more relevant and result in success.

Also, in the second version of Privacy Wallet, Privacy Wallet can provide unlimited access to the entire internet with a single username and password. When the Privacy Wallet is used as an

account, all websites can be visited with a single wallet account as the Privacy Wallet does not require any user-side or server-side registration or requests. Privacy Wallet, which will be ready for government use with Privacy Wallet V3, can be expanded to a different size by being arranged to store and manage documents such as birth certificates, IDs, passports, social security numbers, etc. to add even better user experience and legal protection.

4. Limitations:

The wallet system proposed in this research aims to enhance the privacy and user experience of digital advertising by employing blockchain technology. However, it is important to acknowledge that this innovative solution is not immune to several limitations, as identified by Wajde et al. (106). One such limitation is the significant amount of storage and high-power usage required, which may pose a challenge for individual users and small businesses. Another potential drawback is the risk of permanent data loss if the recovery keys are lost or stolen, as noted by Wajde et al. (106). Moreover, regulatory compliance may be a hurdle, as the system must adhere to various regulations, as outlined by Wajde et al. (106). Lastly, the system necessitates integration with additional software to allow ad buyers to request and receive encrypted user information with user consent, which may add complexity to the system and demand additional resources and expertise to implement. Thus, while this novel wallet system has the potential to revolutionize digital advertising, its limitations must be carefully considered and addressed to ensure optimal outcomes for users and stakeholders alike.

5. Conclusion:

I. Summary of Findings

The extent to which user experience problems arising from privacy protection methods can be solved with blockchain applications was examined in this research. In the first part of the study, a literature review was conducted on marketing techniques, consumer data collection and use, third-party cookies, decentralized networks, and methods to solve privacy issues.

In the second part of the study, an experiment was carried out to measure the number of files left on users' computers by the world's top 100 most visited websites. Google Chrome and Brave Browser were used for this experiment. Also, 122 people were surveyed to analyze the user experience without third-party cookies and their opinions about web3 marketing techniques.

It was found that the problem of user experience problems arising from privacy protection methods exists and that the removal of third-party cookies is a significant contributor to this problem. It was also discovered that blockchain technology has the potential to provide a decentralized and secure platform for data sharing and protect user privacy.

A proposal was made for the development of a blockchain application that utilizes features such as smart contracts, encryption, and decentralized storage to provide a secure and private browsing experience for users. This application can also provide a platform for web3 marketing techniques that respect user privacy.

Overall, the findings of this research suggest that blockchain technology can offer a viable solution to the user experience problems arising from privacy protection methods and that further research and development in this area can lead to significant improvements in online privacy and user experience.

II. Contributions to the Field

Identification of the problem: The research has contributed to the field by identifying the problem of user experience problems arising from privacy protection methods. This is an important issue that affects the online experience of millions of internet users worldwide.

Evaluation of existing solutions: The research has evaluated the effectiveness of existing solutions to the problem, including the use of third-party cookies and decentralized networks. This evaluation has highlighted the limitations of these solutions and the need for a more effective and secure approach.

Proposal of a blockchain-based solution: The research has proposed a blockchain-based solution that utilizes features such as smart contracts, encryption, and decentralized storage to provide a secure and private browsing experience for users. This proposal has the potential to revolutionize the way online data is shared and protected and can contribute to the development of a more secure and privacy-focused internet.

Overall, the contributions of this research to the field include the identification of a significant problem, the evaluation of existing solutions, and the proposal of a new and innovative solution. These contributions can lead to further research and development in the field of online privacy and user experience and can have a significant impact on the way we interact with the internet.

III. Limitations and Future Research

Limited sample size: The survey was conducted on a limited sample size of 122 people, which may not be representative of the larger population. Therefore, the results may not be generalizable to the entire population of internet users.

Limited scope: The study focused on the use of blockchain as a solution to user experience problems arising from privacy protection methods. However, there may be other potential solutions that were not explored in this research.

Limited time frame: The study was conducted over a limited time frame, and therefore, may not have captured the full extent of the problem or potential solutions.

In terms of future research, there may be a need for more extensive studies to investigate the effectiveness of blockchain-based solutions in providing a secure and private browsing experience for users. Additionally, further research could explore other potential solutions to the problem of user experience problems arising from privacy protection methods, such as the use of artificial intelligence or machine learning algorithms. Furthermore, future research could focus on the ethical implications of online data collection and use, and how to balance privacy concerns with the need for personalized online experiences.

IV. Implications for Practice

Importance of privacy protection: The study highlights the importance of privacy protection for internet users. The findings suggest that many websites leave behind files on users' computers, even after users have left the website, which can compromise their privacy and security. This highlights the need for more effective privacy protection methods and greater transparency from website operators regarding their data collection and use practices.

The potential of blockchain technology: The study suggests that blockchain technology may be a viable solution to user experience problems arising from privacy protection methods. Blockchain technology offers a decentralized and transparent approach to data storage and management, which could help to address some of the privacy and security concerns associated with traditional web browsing.

The need for further research and development: The study also highlights the need for further research and development of blockchain-based solutions for privacy protection. While the findings suggest that blockchain technology may be effective in addressing some of the challenges associated with web browsing, more extensive research is needed to fully explore its potential and limitations.

Implications for marketers and website operators: The study has important implications for marketers and website operators, who must balance the need for personalized advertising and user experience with users' privacy and security concerns. The findings suggest that website operators should be more transparent about their data collection and use practices and that marketers should explore new advertising models that prioritize user privacy and security.

In conclusion, this study investigated the effectiveness of blockchain technology in solving user experience problems arising from privacy protection methods. The research revealed that visiting websites leaves a significant number of files on users' computers, which can compromise their privacy and negatively impact their browsing experience. Furthermore, the study found that blockchain technology, particularly decentralized networks, can offer an effective solution to this problem.

The study contributes to the field by providing insights into the benefits of using blockchain technology and how it can be applied to enhance user experience while maintaining privacy. The research shows that businesses should consider using blockchain technology to enhance consumer trust and loyalty, which can translate into increased sales and revenue.

However, the study also has some limitations that need to be addressed in future research. The sample size used for the survey was relatively small, and the study focused on a specific type

of blockchain application. Future research can expand on this by using a larger sample size and exploring the potential of other types of blockchain applications.

In summary, the study provides valuable insights into the potential of blockchain technology to solve user experience problems arising from privacy protection methods. By addressing the limitations identified in this study, future research can further explore the potential of blockchain technology and its implications for practice.

Top 100 most visited websites in the world (Hardwick):

#	Domain	Monthly search traffic
1	youtube.com	8,184,698,651
2	en.wikipedia.org	2,896,256,261
3	twitter.com	1,970,902,586
4	instagram.com	1,690,557,250
5	amazon.com	941,617,882
6	pinterest.com	834,802,079
7	imdb.com	726,030,044
8	es.wikipedia.org	602,904,595
9	facebook.com	551,954,710
10	fandom.com	527,692,324
11	apple.com	479,853,905
12	ja.wikipedia.org	457,146,037
13	de.wikipedia.org	410,650,975
14	live.com	380,165,003
15	cricbuzz.com	330,655,815
16	fr.wikipedia.org	309,400,383

#	Domain	Monthly search traffic
17	linkedin.com	281,297,942
18	globo.com	265,597,387
19	microsoft.com	252,803,595
20	nytimes.com	251,707,985
21	etsy.com	251,597,151
22	it.wikipedia.org	244,951,362
23	mayoclinic.org	229,542,637
24	healthline.com	228,849,546
25	indiatimes.com	216,057,808
26	amazon.in	207,247,289
27	amazon.de	204,993,642
28	bbc.co.uk	184,907,100
29	ikea.com	184,895,409
30	amazon.co.jp	180,411,677
31	amazon.co.uk	178,254,939
32	indeed.com	177,065,528
33	flipkart.com	172,755,306

#	Domain	Monthly search traffic
34	bbc.com	158,803,824
35	espn.com	156,286,007
36	mail.yahoo.com	155,627,263
37	ebay.com	155,399,761
38	hurriyet.com.tr	149,869,821
39	allegro.pl	143,848,076
40	booking.com	143,655,090
41	mercadolivre.com.br	143,134,791
42	britannica.com	142,397,079
43	google.com	141,297,176
44	kompas.com	139,963,591
45	nih.gov	134,053,666
46	cnn.com	125,779,675
47	merriam-webster.com	121,666,645
48	homedepot.com	118,195,967
49	amazon.fr	112,178,475
50	ar.wikipedia.org	109,840,894

#	Domain	Monthly search traffic
51	detik.com	109,248,806
52	nike.com	108,103,178
53	medlineplus.gov	106,418,617
54	id.wikipedia.org	103,975,885
55	brainly.co.id	102,397,336
56	milliyet.com.tr	99,296,399
57	accuweather.com	98,689,506
58	magazineluiza.com.br	98,598,710
59	marca.com	98,550,894
60	medicalnewstoday.com	97,945,908
61	cdc.gov	97,933,405
62	hepsiburada.com	96,838,668
63	cambridge.org	96,607,060
64	cookpad.com	95,125,602
65	m.wikipedia.org	95,029,693
66	dailymail.co.uk	95,005,731
67	as.com	93,305,939

#	Domain	Monthly search traffic
68	ilovepdf.com	93,243,977
69	gsmarena.com	92,247,265
70	byjus.com	89,725,133
71	amazon.it	88,848,535
72	adobe.com	88,668,874
73	investing.com	88,290,123
74	epfindia.gov.in	87,464,090
75	clevelandclinic.org	87,104,871
76	aliexpress.com	86,167,214
77	espncricinfo.com	86,069,721
78	india.com	85,940,027
79	ndtv.com	84,883,790
80	canva.com	82,990,122
81	amazon.es	81,719,879
82	craigslist.org	80,949,296
83	finance.yahoo.com	80,190,740
84	dailymotion.com	79,367,183

#	Domain	Monthly search traffic
85	indiamart.com	78,155,956
86	kinopoisk.ru	77,694,674
87	nl.wikipedia.org	77,354,382
88	onet.pl	76,383,500
89	omegle.com	76,348,649
90	goal.com	73,866,626
91	americanas.com.br	73,344,240
92	investopedia.com	70,668,903
93	dictionary.com	70,350,892
94	mail.ru	68,176,299
95	ebay.co.uk	66,996,424
96	naver.com	66,784,762
97	hm.com	66,387,888
98	hotstar.com	65,480,184
99	bestbuy.com	64,746,994
100	collinsdictionary.com	64,628,918

Works Cited

Al-Ibrahim, Mohamed, et al. "Cookie-Less Browsing." *International Journal of Computer Engineering and Information Technology*, vol. 9, no. 12, 2017, pp. 308–312. *ProQuest*, https://www.proquest.com/scholarly-journals/cookie-less-browsing/docview/1993348469/se-2. Accessed 9 Aug. 2022.

Aydin Aslaner, Duygu, and Gülşah Aydin. "Dijitali yeniden Okumak: Sosyal Etki Pazarlamasi Ve Influencerler." *Pamukkale University Journal of Social Sciences Institute*, 2020, https://doi.org/10.30794/pausbed.795144. Accessed 2022.

Boukis, Achilleas. "Exploring the Implications of Blockchain Technology for Brand–Consumer Relationships: A Future Research Agenda." *Journal of Product & Brand Management*, vol. 29, no. 3, 2019, pp. 307–320. *ProQuest*, https://doi.org/10.1108/jpbm-03-2018-1780. Accessed 2022.

Chang, Li, and Min Y. Hsieh. "Five Ways to Create Customer Value with Blockchain." *International Journal of Organizational Innovation (Online)*, vol. 14, no. 4, 2022, pp. 25–43. *ProQuest*, https://www.proquest.com/scholarly-journals/five-ways-create-customer-values-with-blockchain/docview/2653588396/se-2. Accessed 9 Aug. 2022.

Chomiak-Orsa, Iwona, and Konrad Liszczyk. "Digital Marketing as a Digital Revolution in Marketing Communication." *Informatyka Ekonomiczna*, vol. 2020, no. 2, 2020, pp. 9–19., https://doi.org/10.15611/ie.2020.2.01. Accessed 2022.

Ertemel, Adnan V. "Implications of Blockchain Technology on Marketing." *Journal of International Trade, Logistics and Law*, vol. 4, no. 2, 2018. *ProQuest*, https://www.proquest.com/scholarly-journals/implications-blockchain-technology-on-marketing/docview/2194151039/se-2. Accessed 8 Aug. 2022.

Graesch, Jan Philipp, et al. “Information Technology and Marketing: An Important Partnership for Decades.” *Industrial Management & Data Systems*, vol. 121, no. 1, 2020, pp. 123–157. *ProQuest*, https://doi.org/10.1108/imds-08-2020-0510. Accessed 2022.

Graham, Charles, et al. “The Generation Z Audience for in-App Advertising.” *Journal of Indian Business Research*, vol. 13, no. 3, 2021, pp. 343–360., https://doi.org/10.1108/jibr-08-2020-0275. Accessed 8 Aug. 2022.

Hahn, Alexander, et al. “The Blockchain's Impact on Digital Marketing Platforms.” *Marketing Review St. Gallen : Marketingfachzeitschrift Für Theorie & Praxis*, vol. 37, no. 6, 2020, imc.unisg.ch/app/uploads/2021/11/The-Blockchains-Impact-on-Digital-Marketing-Platforms.pdf. Accessed 2022.

Hardwick, Joshua. “Top 100 Most Visited Websites (US and Worldwide).” *SEO Blog by Ahrefs*, 27 July 2022, https://ahrefs.com/blog/most-visited-websites/.

Hawlk, Kali. “Outbound Versus Inbound Marketing: Which Strategy Is Best?” *Journal of Financial Planning*, vol. 31, no. 6, 2018, pp. 30–31. *ProQuest*, www.proquest.com/trade-journals/outbound-versus-inbound-marketing-which-strategy/docview/2063810081/se-2?accountid=12104. Accessed 2022.

Jain, Deepa, et al. “How Is Blockchain Used in Marketing: A Review and Research Agenda.” *International Journal of Information Management Data Insights*, vol. 1, no. 2, 2021, p. 100044., https://doi.org/10.1016/j.jjimei.2021.100044. Accessed 2022.

Jayakumar, Lakshmi Narayanan. “Cookies ‘n’ Consent: An Empirical Study on the Factors Influencing of Website Users’ Attitude towards Cookie Consent in the EU.” *DBS Business Review*, vol. 4, 2021. *ProQuest*, https://doi.org/10.22375/dbr.v4i0.72. Accessed 8 Aug. 2022.

Joseph, Seb. “WTF Is Google's Privacy Sandbox?” *Digiday*, 17 Jan. 2020, https://digiday.com/marketing/wtf-googles-privacy-sandbox/.

Madhani, Pankaj M. “Effective Marketing Strategy with Blockchain Implementation: Enhancing Customer Value Propositions.” *IUP Journal of Business Strategy*, vol. 19, no. 1, 2022, pp. 7–35. *ProQuest*, https://www.proquest.com/scholarly-journals/effective-marketing-strategy-with-blockchain/docview/2672062161/se-2. Accessed 13 Nov. 2022.

Nelissen, Lei, and Mathias Funk. “Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX through Speculative Enactments.” *International Journal of Design*, vol. 16, no. 1, 2022, pp. 77–94. *ProQuest*, https://www.proquest.com/scholarly-journals/rationalizing-dark-patterns-examining-process/docview/2665959361/se-2. Accessed 9 Aug. 2022.

Pantelic, Ognjen, et al. “Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations.” *Sustainability*, vol. 14, no. 9, 2022, p. 5015. *ProQuest*, https://doi.org/10.3390/su14095015. Accessed 8 Aug. 2022.

Parkyn, Jonathan. “Is It Safe to Go Anonymous Online?” *Computer Act!Ve*, vol. 590, Oct. 2020, pp. 62–63. *ProQuest*, https://www.proquest.com/magazines/is-safe-go-anonymous-online/docview/2452517054/se-2. Accessed 6 Oct. 2022.

Patrutiu-Baltes, Loredana. “Inbound Marketing - the Most Important Digital Marketing Strategy.” *Bulletin of the Transylvania University of Brasov Economic Sciences Series V*, vol. 9, no. 2, 2016, pp. 61–68. *ProQuest*, www.proquest.com/scholarly-journals/inbound-marketing-most-important-digital-strategy/docview/1881686958/se-2. Accessed 2022.

Prasad, Abhiram, et al. “Predictive Programmatic Re-Targeting to Improve Website Conversion Rates.” *Journal of Physics: Conference Series*, vol. 1714, no. 1, 2021. *ProQuest*, https://doi.org/10.1088/1742-6596/1714/1/012027. Accessed 9 Aug. 2022.

Presthus, Wanda, and Hanne Sørum. “Consumer Perspectives on Information Privacy Following the Implementation of the GDPR.” *International Journal of Information Systems and Project Management*, vol. 7, no. 3, 2021, pp. 19–34. *ProQuest*, https://doi.org/10.12821/ijispm070302. Accessed 8 Aug. 2022.

Price, Marjorie S. “Internet Privacy, Technology, and Personal Information.” *Ethics and Information Technology*, vol. 22, no. 2, 2020, pp. 163–173. *ProQuest*, https://doi.org/10.1007/s10676-019-09525-y. Accessed 8 Aug. 2022.

Rejeb, Abderahman, et al. “How Blockchain Technology Can Benefit Marketing: Six Pending Research Areas.” *Frontiers in Blockchain*, vol. 3, 2020. *ProQuest*, https://doi.org/10.3389/fbloc.2020.00003. Accessed 2022.

Routray, Janendra K. “Blockchain: How It Is Changing Digital Marketing.” *A Quarterly Peer Reviewed Multi-Disciplinary International Journal." Splint International Journal of Professionals*, vol. 7, no. 3, 2020, pp. 55–64. *ProQuest*, ProQuest, www.proquest.com/scholarly- journals/blockchain-how-is-changing-digital-marketing/docview/2620975779/se- 2?accountid=12104. Accessed 2022.

Sadeghpour, Shadi, and Natalija Vlajic. “Ads and Fraud: A Comprehensive Survey of Fraud in Online Advertising.” *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, 2021, pp. 804–832. *ProQuest*, https://doi.org/10.3390/jcp1040039. Accessed 8 Aug. 2022.

Van Auken, Stuart. “Bot Baseline Report: Fraud in Digital Advertising.” *Bot Baseline Report | Ad Fraud | White Ops*, 2019, http://www.humansecurity.com/botbaseline2019. Accessed 2022.

Van Auken, Stuart. “From Consumer Panels to Big Data: An Overview on Marketing Data Development.” *Journal of Marketing Analytics*, vol. 3, no. 1, 2015, pp. 38–45. *ProQuest*, https://doi.org/10.1057/jma.2015.2. Accessed 2022.

Wajde, Baiod, et al. “Blockchain Technology and Its Applications Across Multiple Domains: A Survey.” *Journal of International Technology and Information Management*, vol. 29, no. 4, ser. 4, 2021. *4*, https://scholarworks.lib.csusb.edu/jitim/vol29/iss4/4. Accessed 30 Oct. 2022.