Enjoy Data Sovereignty by Knowing Where Your Data Go

***Abstract*—This paper introduces certCookie, a blockchain-based system addressing privacy concerns in targeted advertising by ensuring transparent data ownership. In a landscape shaped by regulatory restrictions on third-party cookies, certCookie encourages user data sharing through direct economic incentives. The system employs smart contracts to establish secure data access authorization, enhancing transparency in personalized advertising. Key stakeholders interact within this framework, including users, websites, and marketing agencies. Experimental results on a private Ethereum network suggest practical viability, with plans to evaluate alternative chains for improved efficiency.**

***Index Terms*—Blockchain, Data exchange, Internet**

I. Introduction

Living in an era of easily interconnected internet, it is not uncommon for people to come across social media feeds filled with targeted advertisements. It is surprising to see ads for products or services that align perfectly with one's interests or needs. Targeted ads are everywhere, showing products matching personal interests and preferences. Some people even suspect electronic devices listen to our conversations to gather data. However, the truth is that these ads are made possible by cookie data generated from our interactions with websites.

Targeted advertising plays a crucial role in supporting the online ecosystem, bringing in significant revenue for the Internet market. Personalized advertising, driven by data collected through website cookies, has been found to be more effective than showing generic ads randomly. The impact of a cookie-less environment on marketing companies' revenue is substantial. Google's data collection from May to September 2019 revealed a significant difference in publisher earnings between those exposed to non-personalized ads and those exposed to personalized ads due to some users' deactivation of cookie access. The top 500 publisher companies experienced an average profit decrease of 52%, with a median decrease of 62% [1]. This highlights the crucial role of cookie information or user metadata in the online marketing industry.

However, using cookies has its dual nature. While enhancing user convenience by recommending personalized ads and maintaining information such as a cart, it also raises privacy concerns. As a solution, the EU has restricted third-party cookie usage through the General Data Protection Regulation (GDPR) since May 25, 2018. Safari implemented software updates blocking third-party cookies starting in 2020. Despite efforts to safeguard user privacy, stringent and mandatory regulations impede the cyclical nature of the online market, limiting access to personalized recommendations for users who desire to utilize their data extensively. Additionally, users express greater dissatisfaction with non-personalized ads. When given the option to stop ad displays, there was a 21% increase in users clicking to close non-personalized ads within the group exposed to them.

We propose a new corporate perspective to address the challenge: encouraging user information sharing. Users may choose not to share their data for various reasons. One reason may be that they do not fully understand lengthy cookie access permission messages and only allow necessary cookies or deny all cookies without realizing how their data can benefit various aspects. Furthermore, after users share it, they may not know where their data is being used and who owns it. Ultimately, the primary reason for their reluctance is the lack of direct economic benefits they receive from sharing their data.

This paper introduces the certCookie system using blockchain smart contracts to solve these issues. The proposed system facilitates easy identification of data ownership rights, encouraging data sharing by providing direct benefits to data owners. Moreover, it offers the advantage of allowing users to verify the basis of ad recommendations, leading to interactive adjustments by users.

II. Background

A. Smart Contract

A smart contract [2] is a self-executing contract with the terms of the agreement directly written into code. It operates on a blockchain, a decentralized and distributed digital ledger, and is designed to automatically execute and enforce the terms of a contract when predefined conditions are met. Smart contracts eliminate the need for intermediaries, such as banks or legal entities, by automating and self-verifying the execution of contractual clauses. Smart contracts can be used in a variety of applications, including financial transactions, supply chain management, voting systems, and more. They ensure transparency, security, and efficiency by leveraging the decentralized and tamper-resistant nature of blockchain technology. Once deployed, smart contracts run on the blockchain, and their execution is visible to all participants, providing a trustless and decentralized way of conducting and enforcing agreements.

B. Cookie

Cookies, a technology introduced by in 1994 [3], are small text files, typically 4KB, stored on the client's computer through the browser. They consist of elements such as cookie name and cookie value and may also include optional information like the expiry date, the domain of the server, and the

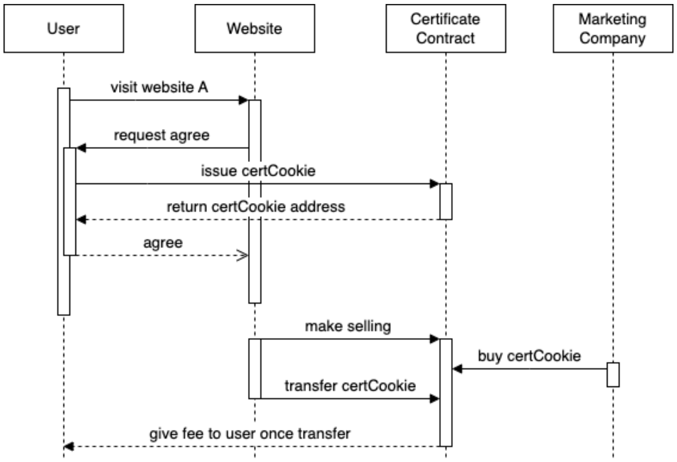

Fig. 1. Sequence Diagram of Some Functions of the System

path. Although the HTTP protocol does not store state, cookies empower web servers to retain browser-related information on the client's computer.

There are two primary types of cookies: first-party cookies and third-party cookies.

First-Party Cookies These are cookies set by the website domain the user is currently visiting. They are primarily used to enhance the user experience on that specific website. First-party cookies are often used to remember user preferences, maintain user login sessions, and customize content based on user interactions.

Third-Party Cookies In contrast, third-party cookies are set by domains other than the one the user is currently visiting. They are often utilized for cross-site tracking and advertising purposes. Third-party cookies enable advertisers and marketing companies to collect information about a user's online behavior across different websites, allowing them to deliver targeted ads based on the user's interests and activities. This has significantly contributed to the activation of the online marketing industry, as advertisers can tailor their messages to specific audiences, thereby increasing the effectiveness of their campaigns.

III. System Architecture

This system aims to encourage user data sharing by enabling an understanding of who can access user data. The key stakeholders in this system include the user, websites, online marketing agencies, companies seeking advertisements, and third-party cookie collection agencies.

When Alice accesses a Website, the site requests the consent to use cookies. The website includes first-party and third-party cookies requests, all of which require the user's certCookie. If the parties requesting cookie data are unable to find a record of Alice's browsing history, Alice can issue their certCookie and transfer this to these parties. After completing the certCookie issuing process, Alice receives the certCookie's address. This address is transmitted to the Website, indicating permission for cookie access. The received certCookie address is stored as the cookie value on the Website, and the hashed value is additionally stored to prevent malicious alterations. When the same user revisits the Website, the website identifies Alice through the certCookie address stored as a cookie, verifies ownership through a Certificate Contract verification request, and gains access to Alice's cookie.

Even if the website copies and possesses data, it becomes useless if Alice's current association with that data is unknown.

A. *Personalized Advertising*

Marketing companies collect user metadata, such as third-party cookies, to understand preferences and determine efficient advertisements. When a user accesses a website where their data is present, personalized advertisements are displayed. Personalized ads are typically finalized through an auction, where the company bidding the highest price among those interested in advertising gets the opportunity. Advertisers must possess certCookie representing all data about the user, including third-party cookies and first-party cookies. Through the corresponding certCookie, users can understand the basis for the recommended personalized ads.

B. *User Cookie Data Access Authorization*

This subsection explains the process of issuing and selling certCookie that grants access to user cookie data. The certCookie is issued with a timestamp and the initial user's address when initiated. The certCookie can be sold, transferring data access authorization through a function that moves the certCookie to another user's address. Each user contract expects parameters such as the artist's address, fee token address, fee amount, and initialization timestamp. As certCookie representing data access authorization is transferred, the user who initially created the certCookie can expect economic gains.

IV. Evaluation and Future work

Utilizing the Truffle framework [4], we established a private local Ethereum network and conducted experiments with 10 accounts. We deployed smart contracts for certificate authentication and an auction on this network.

Due to the relatively slow block processing speed of Ethereum, it is deemed necessary to practically test and evaluate its use on alternative chains with shorter latencies, such as Sui [5] and Aptos. Future research plans include conducting tests on these chains to assess their suitability for more practical applications.

References

[1] D. Ravichandran, N. Korula, "Effect of disabling third-party cookies on publisher revenue," Google Report, August 2019.

[2] Wood, Gavin and others, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp. 1-32, 2014.

[3] Giannandrea, John and Montulli, Lou. "Persistent Client State: HTTP Cookies," October 1994.

[4] Hartel, Pieter and van Staalduinen, Mark. "Truffle tests for free–Replaying Ethereum smart contracts for transparency," arXiv preprint arXiv:1907.09208, 2019.

[5] Blackshear, Same and Chursin, Andrey and Danezis, George and Kichidis, Anastasios and Kokoris-Kogias, Lefteris and Li, Xun and Logan, Mark and Menon, Ashok and Nowacki, Todd and Sonnino, Alberto and others. "Sui lutris: A blockchain combining broadcast and consensus," arXiv preprint arXiv:2310.18042, 2023.