EMPOWERED DATA OWNERSHIP WITH DECENTRALIZED COOKIE MANAGEMENT APPLICATION

K. Nithisha[1], M.D Sandhiy[2], S. Siva Sree[3]

Department of Information Technology, Panimalar Institute of Technology, Tamil Nadu, Chennai, India

[1,2,3]UG Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, Tamil Nadu, India

[1]nithisha.k30@gmail.com, [2] mdsandhiya20803@gmail.com [3]suba15062000@gmail.com

ABSTRACT

A decentralized cookie management application is a software application that allows users to manage their online cookies in a way that is not controlled by any single entity. This means that users can decide which cookies they want to allow, block, or delete, and they can do so without having to rely on a third party intermediary. It typically uses blockchain technology to store and manage user preferences. Blockchain is a distributed ledger that is secure and transparent, so users can be confident that their preferences are being followed. While decentralized cookie management applications empower data ownership through user controlled preferences stored securely on blockchain, they come with both advantages and limitations. On the positive side, users gain increased privacy, reduced tracking, transparency into website cookies, and enhanced security thanks to blockchain's immutability. However, challenges include potential complexity for users, limited website compatibility due to their relatively new existence, and lack of widespread awareness about their benefits. Despite these hurdles, decentralized cookie management has the potential to revolutionize online privacy as the technology matures and adoption increases.

Keywords: Blockchain, Cookie Commander, Remix IDE, Identity Based Encryption

1. INTRODUCTION

In the ever evolving landscape of the internet, where the paradigm is shifting from centralization to the empowering realm of Web3, it becomes increasingly imperative to seize control of our digital identities. The advent of Web3, however, promises a transformation where individuals become the custodians of their own data, orchestrating a future where privacy is not a privilege but a fundamental right. Amidst this promising transition, a persistent threat endures – the ubiquitous and seemingly innocuous cookies. These digital trackers surreptitiously accumulate on our devices, constructing detailed profiles that fuel targeted ads and surreptitious data monetization. In this landscape, users often find themselves relegated to the role of passive observers, with their data traded freely, devoid of informed consent. Each click, search query, and purchase incrementally contributes to a digital footprint that can encroach upon your privacy. Now where the man in problem is Ad networks track and store a staggering amount of data, including personally identifiable information, which is the issue. They may gain access to private data, including political affiliation, sexual orientation, gender identity, and medical history, because they set cookies on a wide range of websites. The fact that this data is probably connected to the user's true name is much more concerning.

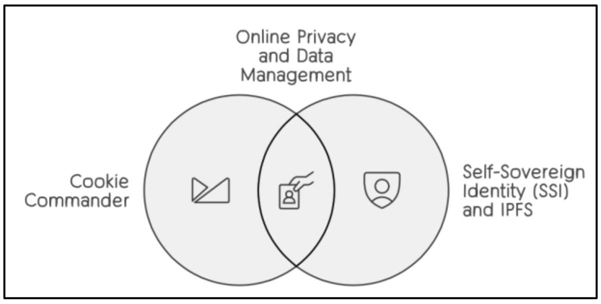
Online Privacy and Data Management
Cookie Commander
Self-Sovereign Identity (SSI) and IPFS

Figure 1: Combined Implementation

Our contribution, the solution. The vision of Cookie Commander, coupled with Self Sovereign Identity (SSI)[1] and the utilization of IPFS[2], represents a significant advancement in the realm of online privacy and data management. By integrating these innovative technologies, users are empowered to reclaim control over their digital identities and safeguard their privacy in an increasingly interconnected online world.

Cookie Commander serves as a robust defense mechanism against intrusive tracking practices, offering users transparency, granular control, and decentralized storage[2] of consent choices. Through its utilization of Web3 technologies[3], Web Extension Development Frameworks, Data Privacy Libraries, Solidity, and smart contracts, Cookie Commander ensures that users can effectively manage their digital preferences while leveraging the security and immutability of blockchain technology.

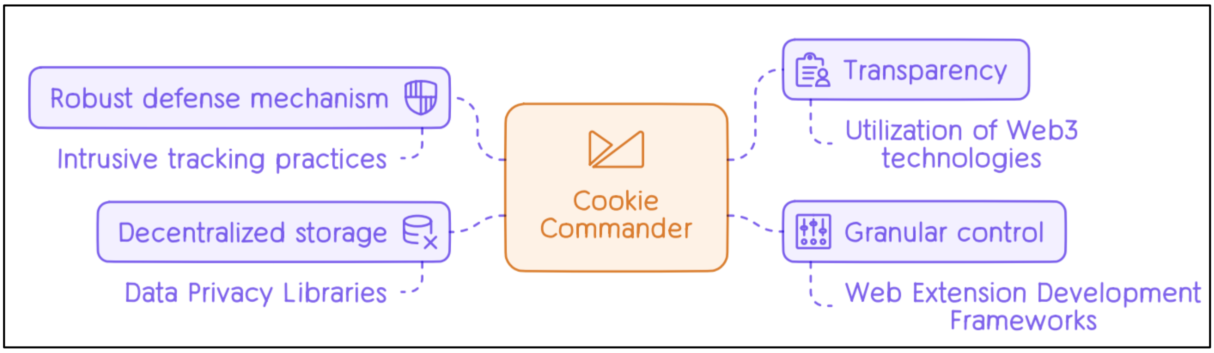

Figure 2: Mechanism of Cookie Commander

Meanwhile, SSI provides individuals with the means to own and manage their digital identities autonomously, storing identity data securely in personal wallets and issuing verifiable credentials as needed. This approach significantly reduces data collection and enhances anonymity, as users have the freedom to selectively share only the information requested by websites.

The integration of IPFS further enhances the decentralization of identity management by leveraging its content addressable nature and Merkle trees for efficient verification and tamper evident logs of credential issuance and usage.

Additionally, the incorporation of TFIM[4] for threat prioritization and assessment, along with other methods such as IDP, IBE[5], DPKG[15], ae privacyend PII[19], strengthens the overall security posture of decentralized identity systems[8], ensuring robust protection against potential threats. Additionally, our solution preserves documents on a decentralised file system by utilising the advantages of IPFS (Inter Planetary File System). The suggested method streamlines the communications that are required between several parties, including approvers and developers. Solidity was used to create the smart contracts, and the Remix IDE (Integrated Development Environment) was used to test their functionality.

Overall, these developments mark a paradigm shift in online privacy and data management, offering users unprecedented control over their digital lives and contributing to a more equitable and sustainable web ecosystem[8]. As these technologies continue to evolve, they hold the promise of further empowering users with greater autonomy and control over their data and privacy in the decentralized web landscape.

2. RELATED WORK

In the dynamic realm of cookie management, prevailing solutions grapple with centralized systems, triggering concerns over data ownership, transparency, and control. Amidst this landscape, Cookie Commander emerges as a trailblazing solution, harnessing the potential of Decentralized Identity (DID) technology[8] to redefine how users interact with and oversee their data. As we navigate through existing technologies and tools, let's illuminate the distinctive contributions that set Cookie Commander apart:

Employing browser extensions or website scripts with fundamental blocking/allowing functionalities. Struggling with transparency, limited control, and dependency on potentially vulnerable centralized servers. Examples include Cookiebot[9], Ghostery[18], Adblock Plus[11]. Incorporating built-in features or addons that obstruct trackers, fingerprinting scripts, and third party cookies. Requiring technical configurations, potential impacts on website functionality, and offering limited data control. Examples include Brave, Firefox with privacy extensions, DuckDuckGo.

Embracing blockchain based protocols for user controlled identity management. Navigating early stages, grappling with limited adoption, and confronting interoperability challenges. Examples include Sovrin[12], Hyperledger Indy[16], Sidetree[20]. Unlike conventional tools, Cookie Commander harnesses DID technology[12], endowing users with ownership and control through selfissued credentials stored securely on a blockchain.

Beyond simplistic blocking/allowing, Cookie Commander empowers users to define access levels for individual data points within a cookie, ensuring meticulous control over shared information.Offering clear insights into requested data, Cookie Commander employs ZeroKnowledge Proofs to maximize privacy, proving compliance without unveiling actual data.

With its foundation rooted in DID technology, Cookie Commander ensures seamless integration with upcoming decentralized applications and platforms, embodying a forward looking solution for user data control.

3. PROPOSED MODEL

3.1 Cookie Commander's Core Components:

Utilizes established DID frameworks like Indy and Sidetree for seamless credential issuance, management, and verification. Securely stored on blockchain networks like Ethereum or Polygon, user credentials and consent choices find their vault. Employing ZeroKnowledge Proof libraries such as zkSNARKs facilitates data verification without exposing underlying information. Access control policies, framed through frameworks like XACML, enable granular control over data access. Secure encryption libraries like Charm or PBC ensure that only authorized parties can decrypt data shared with websites[15].

The key difference is Pioneering DID Integration for Cookie Management. In the expansive landscape where diverse solutions grapple with data privacy, Cookie Commander emerges as a trailblazer, pioneering DID technology integration explicitly for cookie management. This groundbreaking approach yields distinct advantages like User Empowerment, Granular Control, Enhanced Privacy, FutureProof Approach.

Users can meticulously define data access levels for each cookie bestowing unmatched flexibility in data management. Zero knowledge proof ensures data verification without compromising personal information and elevating privacy standards. The solid DID foundation positions CookieCommander as a seamless into decentralized web, showcasing a forward-thinking strategy in the ever-evolving realm of user data control.

4. DESIGN OVERVIEW

CookieCommander is a decentralized cookie management application that is designed as an chrome extension that works on both web2.0 and web3.0 Technology[16], which supports complete control over the PII (Personal Information Identity)[19] by being transparent and accountable to the extension users.

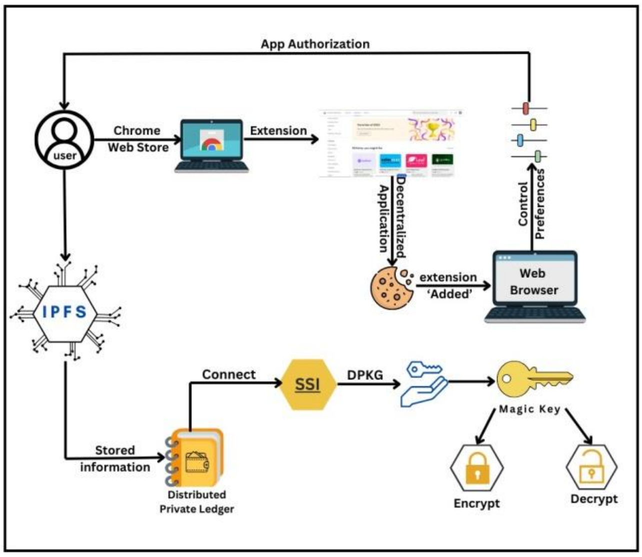

Figure 3: Working of CookieCommander

After adding extension to our browser, the Cookie Commander is logged in based on user information stored in the IPFS(Interplanetary File System)[2] a decentralized data storage. when entering a website for sign in or cookie activation or while accepting privacy policy preferences can be set based on user interest instead of providing accurate results to websites. Then, the IPFS connects to a distributed private ledger for storing, updating and deleting information in the wallet. The schemes such as SSI, IDp[17] and Ibe[5] are used in this application to secure our identity as anonymous IPFS hash IDs. When logged in again on the same website the key generated using DPKG encrypts[15] and decrypts the tokens that contain anonymous information. CookieCommander leverages your IPFS stored information for login, eliminating the need for traditional credentials. Before storing the information the users can encrypt the data for enhanced security. This not only simplifies the process but also enhances security by removing password vulnerabilities. Let's delve into the technical details of its inner workings:

4.1.Decentralized Identity and Storage:

IPFS (Interplanetary File System): Forget traditional servers! CookieCommander utilizes IPFS, a decentralized storage system[2], to securely store your user information[18]. This eliminates single points of failure and empowers you with control over your data. SSI, IDp, and IBe: These cryptographic schemes form the backbone of your anonymous identity. SSI (SelfSovereign Identity) grants you ownership, while IDp (Identity Provider)[17] verifies your credentials without revealing personal information. IBe (IdentityBased Encryption)[5] adds another layer of security by using unique identifiers for encryption and decryption.

4.2.Seamless Interaction with Websites:

Distributed Private Ledger: Imagine a secure, shared database[19]. This is where CookieCommander stores your cookie preferences and website interactions. Whenever you encounter a signin, cookie activation, or privacy policy acceptance prompt, the IPFS connects to this distributed ledger, ensuring your preferences are applied seamlessly across websites.

DPKG (Distributed Private Key Generation): For added security, CookieCommander utilizes DPKG[15] to generate unique encryption keys. These keys are crucial for encrypting and decrypting tokens containing your anonymous information, further safeguarding your privacy.

4.3.The Login Process:

No Passwords Required: Forget the hassle of remembering passwords! CookieCommander leverages your IPFSstored information for login, eliminating the need for traditional credentials. This not only simplifies the process but also enhances security by removing password vulnerabilities.

4.4.Website Recognition and Anonymity:

TokenBased Interactions: When you revisit a website, CookieCommander retrieves the relevant token containing your encrypted preferences from the distributed ledger. This token acts as your anonymous identity, allowing the website to recognize you while maintaining your privacy.

4.5.DPKG Magic:

The DPKGgenerated key unlocks the power of these tokens[15]. It decrypts the website specific information, enabling the website to adhere to your cookie preferences without compromising your anonymity.

Overall, CookieCommander empowers you with control over your online identity and cookie management. By leveraging the power of decentralization, cryptography, and innovative technologies, it offers a secure and user friendly solution for navigating the ever evolving web landscape[18].

5. ALGORITHMIC STRUCTURE

The implementation of the CookieCommander extension is based on a modular architecture leveraging Ethereum, Solidity, and React. Smart contracts written in Solidity are deployed on the Ethereum blockchain to handle decentralized identity management[8] and preferences storage. User interactions and preferences are managed through intuitive React components, providing a seamless browsing experience. Cryptographic techniques such as Self Sovereign Identity (SSI) and Identity Based Encryption (IBE) are incorporated to ensure the security and privacy of user data. Additionally, the extension utilizes IPFS for decentralized data storage, further enhancing resilience and privacy. Through careful integration of these technologies, CookieCommander empowers users with control over their data while maintaining security in a decentralized web environment.

i) Installation and Initialization:

- Users install the CookieCommander Chrome extension from the Chrome Web Store.
- Upon installation, the extension generates a unique Ethereum wallet address for the user using the web3.js library.
- The extension interacts with the Ethereum blockchain to deploy a smart contract that will handle user preferences and interactions.

ii) Decentralized Identity Management:

- User information, such as preferences related to signins, cookie activations, and privacy policy acceptances, is stored in the Ethereum smart contract.
- Solidity smart contracts define the structure and functions to manage user preferences and store them securely on the Ethereum blockchain.
- IPFS is utilized to store larger data sets such as encrypted user data or preferences that exceed the Ethereum gas limit.

iii) Cryptographic Security:

- Cryptographic schemes like Self Sovereign Identity (SSI)[1], Identity Provider (IDp)[17], and Identity Based Encryption (IBe)[5] are implemented within the smart contract to ensure secure and anonymous user identities.
- Users have the option to encrypt their data before storing it on IPFS[2], utilizing encryption libraries such as CryptoJS or Web3.js encryption functions.

iv) Seamless Website Interactions:

- When users navigate websites, the CookieCommander extension prompts them for preferences based on stored data or new interactions.
- React components within the extension handle the user interface for displaying prompts and capturing user preferences.
- Web3.js library facilitates interactions between the extension and the Ethereum smart contract to retrieve and update user preferences seamlessly.

v) Distributed Private Key Generation (DPKG):

- When revisiting a website, CookieCommander utilizes the Ethereum wallet's private key for authentication.
- DPKG process generates a temporary key[15] for encrypting and decrypting tokens containing anonymous information, ensuring secure login without traditional credentials.
- Solidity smart contracts define the logic for generating and validating temporary keys within the Ethereum blockchain.

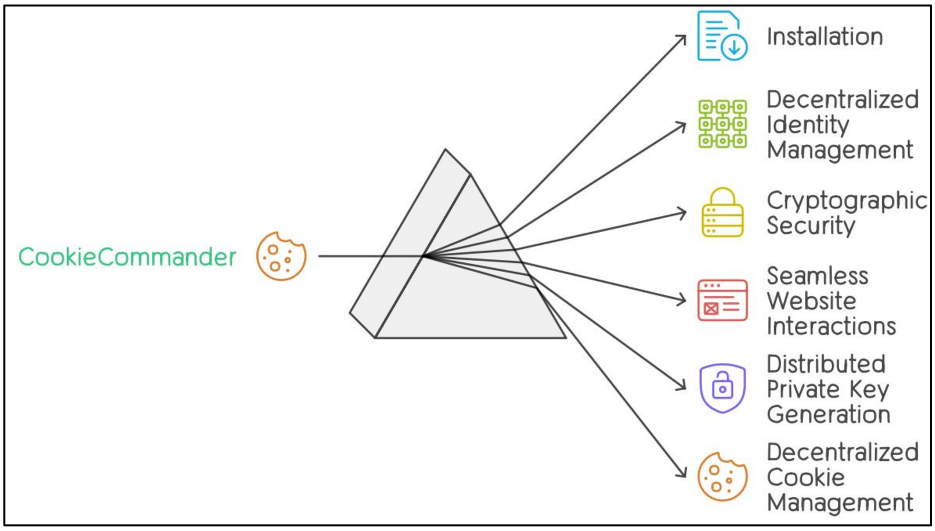
CookieCommander
Installation
Decentralized Identity Management
Cryptographic Security
Seamless Website Interactions
Distributed Private Key Generation
Decentralized Cookie Management

Figure 5: Algorithmic Flow of the Decentralized Cookie Management Application

vi) Decentralized Cookie Management:

- CookieCommander extension manages cookies and user data locally, providing users with control over their Personally Identifiable Information (PII)[19].
- Smart contracts handle interactions related to cookie management, ensuring transparency and security through blockchain immutability and cryptographic verification.

vii) User Interface and Experience:

- React.js is used to develop the user interface of the extension, providing a seamless and intuitive experience for users.
- User interactions, preferences, and notifications are managed through React components, enhancing usability and accessibility.

6. CONCLUSION

In the dynamic shift from centralization to the liberating realm of Web3, the imperative to control our digital identities becomes paramount. Web3 promises a future where individuals stand as custodians of their own data, transforming privacy from a privilege to a fundamental right. Yet, amidst this promising shift, the relentless challenge of cookies persists.Against the backdrop of ad networks tracking and storing personally identifiable information, our contribution emerges – "Cookie Commander." This decentralized weapon against tracking demystifies the intricate web of tracking, granting users unprecedented control. Users become gatekeepers, dictating what information remains private, fortifying privacy against evolving data practices. Powered by revolutionary Web3 technology, Cookie Commander eliminates third-party tracking, offers granular control, ensures transparency, and decentralizes storage on the blockchain[20]. Cutting-edge tools and technologies collaborate seamlessly beneath the surface. In convergence with SSI, IPFS[2], and innovative solutions, Cookie Commander represents a significant leap forward, offering users unparalleled control over their digital identities and privacy. As we conclude, Cookie Commander stands as a beacon of empowerment, harmonizing with Web3 principles and setting the stage for a user-centric, privacy-oriented digital era. In this ever-evolving web landscape, Cookie Commander beckons users to embrace a future where control over online identities is a powerful reality.

REFERENCES

[1] Ma B, Zheng X, Zhao C, Wang Y, Wang D, Meng B. A secure and decentralized SSI authentication protocol with privacy protection and finegrained access control based on federated blockchain. PLoS One. 2022 Sep 23;17(9):e0274748. doi: 10.1371/journal.pone.0274748. PMID: 36149857; PMCID: PMC9506630.

[2] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "BlockchainBased, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Internet of Things, pp. 14991506, doi: 10.1109/Cybermatics_2018.2018.00253.

[3] Mazieri, M. (2022). Tokenization, blockchain and web 3.0 technologies as research objects in innovation management. https://www.semanticscholar.org/paper/Tokenization%2Cblockchainandweb3.0technologiesMazieriScafuto/945097cf2193e84c0fe8356375a301eb63bb1508

[4] TFIM-IBM Documentation. (n.d.). https://www.ibm.com/docs/en/sva/7.0.0?topic=sssaj-single-signon-using-tivoli-federated-identity-manager

[5] IBE-Shao, S., Chen, F., Xiao, X., Gu, W., Lu, Y., Wang, S., Tang, W., Liu, S., Wu, F., He, J., Ji, Y., Zhang, K., & Mei, F. (2021, August 12). IBE-BCIOT: an IBE based cross-chain communication mechanism of blockchain in IoT. World Wide Web. https://doi.org/10.1007/s11280-021-00864-9

[6] pii- PII - Glossary | CSRC. (n.d.). https://csrc.nist.gov/glossary/term/IBE#:~:text=Personally%20Identifiable%20Information%3B%20Any%20representation,either%20direct%20or%20indirect%20means.

[7] A. C. -F. Chan, "Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks," in IEEE Wireless Communications Letters, vol. 1, no. 1, pp. 46-48, February 2012, doi: 10.1109/WCL.2012.120211.110130.

[8] Xiong, R. (2023). BDIM: A BlockchainBased Decentralized Identity Management Scheme for Large Scale Internet of Things. https://www.semanticscholar.org/paper/BDIM%3AABlockchainBasedDecentralizedIdentityforXiongRen/0bf05db35592e89dc5efbd22f532394b95eeaf32

[9] GDPR Compliance and ePrivacy CMP Solution - CookiebotTM. (n.d.). Cookiebot. https://www.cookiebot.com

[10] Best Ad Blocker & Privacy Browser. (n.d.). Ghostery. https://www.ghostery.com

[11] Adblock Plus | The world’s #1 free ad blocker. (n.d.). https://adblockplus.org

[12] How DIDs, Keys, Credentials, and Agents Work in Sovrin - Sovrin. (2019, March 10). Sovrin. https://sovrin.org/library/how-dids-keys-credentials-and-agents-work-in-sovrin/

[13] IBMhttps://identity.foundation/working-groups/sidetree.html

[14] Indy. (2023, October 20). https://www.hyperledger.org/projects/hyperledger-indy

[15] Tian, Y. (2023). Efficient identity based multicopy data sharing auditing scheme with decentralized trust management. https://www.semanticscholar.org/paper/82f91676dafdd4518760ef6b97bd26e25c3e293f

[16] H. K. M. AlChalabi, "Evaluation of a MultiParameter Elearning System using Web 3.0 Technologies," 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 2021, pp. 14, doi: 10.1109/ECAI52376.2021.9515191.

[17] S. Michael and Z. J. Anna, "An Identity Provider as a Service platform for the eduGAIN research and education community," 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 2019, pp. 739-740.

[18] Agrawal, K. (2023). Blockchain Based Healthcare System to Secure Health Records. https://www.semanticscholar.org/paper/BlockchainBasedHealthcareSystemtoSecureHealthAgrawalAggarwal/4c9dda653b67ad51ad6cc433a333d1d7090ac199

[19] Hussien, H. M., Yasin, S. M., Udzir, N. I., & Ninggal, M. I. H. (2021, April 2). BlockchainBased Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. Sensors. https://doi.org/10.3390/s21072462

[20] Shaikh, R. (2022). Blockchain Based Cloud Storage of Patients Health Records. https://www.semanticscholar.org/paper/BlockchainBasedCloudStorageofPatientsHealthShaikh/3729b0cf9534e8122d3156e7e285a1c410560cb2

[21] M. R. Asghar, M. Backes and M. Simeonovski, "PRIMA: PrivacyPreserving Identity and Access Management at InternetScale," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 16, doi: 10.1109/ICC.2018.8422732.