International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Based Decentralized User Identity Verification System

Kavita A. Sultanpure[1], Subham Gangurde[2], Sudarshan Gawale3 , Harshal Walunj[4], Gauri Shivsharan[5]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: Privacy is a fundamental consumer right, and the data provided by users is handled by only a few of the large centralized entities that control the majority of the internet. Thus, transferring this data to a decentralized entity such as a blockchain would be an excellent solution. Blockchain stores data in a decentralized and highly secure manner, ensuring data security and integrity. Users will also have authority and control over their data which provides a more effective solution to the current problem. As a result, user authentication via blockchain could be a significant fundamental building block for the next generation of the web (Web 3.0).

Keywords*- Blockchain, Decentralized identity, Web 3.0*

1. Introduction

Authentication ensures that only authorized users have access to a system by preventing unauthorized users from gaining access and potentially causing system damage, stealing information, or causing other problems. Almost all human-to-computer interactions, except guest and automatically logged-in accounts, require user authentication. It gives users access to networked and internet-connected systems and resources via wired and wireless networks. User authentication verifies a user's identity by authorizing the transfer of credentials from a human to a machine during network interactions. There aren't many legitimate official identification documents that can be used to prove your identity. However, this is only true for physical identification, the real concern is digital identity. We require a system that can reliably and globally identify a person online. We need digital IDs that people can own without the assistance of any entities, organizations, or institutions. Currently, no global digital identifiers can be used to express, exchange, or verify our identity. Digital identifiers can be anything from phone numbers to email addresses, but they are still the property of service providers, who can revoke ownership at any time. We need digital IDs that people can own without the assistance of any entities, organizations, or institutions. Currently, no global digital identifiers can be used to express, exchange, or verify our identity. Digital identifiers can be anything, but they are still the property of service providers, who can revoke ownership at any time.

2. Literature Survey

Self-Sovereign Identity (SSI) has the potential to give its users control over identity ownership and personal data. Nitin Naik et al. proposed a thorough examination of the Sovrin Network, an emerging SSI service utility that enables self-sovereign identity for all [1]. The most widely used user authentication mechanism on the Internet is abstract password authentication. The server operator is positioned as a trusted party with complete control over the user's identity, so their authentication security is low. Zhao Yun et al. presented a blockchain-based decentralized identity and password authentication system (DIA). [2]. Before you can use many Internet services, you must first create an account. Friebe S et al. brought up DecentID, a Decentralized and Privacy-Preserving Identity Storage System Using Smart Contracts, which is a completely decentralized identity storage system in which users are not identified by a centralized third party. [3]. The rapid increase in reported incidents of spying and security breaches endangering users' privacy calls into question the current paradigm, in which third parties gather and handle massive amounts of personal data. Bitcoin has demonstrated in the financial sector that reliable, auditable computing is possible by utilizing a decentralized network of peers supported by a public ledger. Zyskind G et al. created a method for converting a blockchain into an automated access-control manager that does not rely on trust in a third party. [4] Interactions between patients, medical physicians, nurses, and other healthcare practitioners must be secure and efficient in any interconnected healthcare system (for example, those that are part of a smart city). To reduce security and privacy breaches within a network, for example, all members must be authenticated and securely interconnected. Yet, implementing security and privacy-protecting solutions can cause delays in processing and other associated services, potentially endangering patients' lives in crucial situations. A. Yazdinejad et al. proposed a decentralized authentication of patients in a distributed healthcare network using

[1] *Department of Information Technology, Vishwakarma Institute of Technology, Pune.*
ORCID ID : 0000-0003-1594-0110
[2,3,4,5] *Department of Information Technology, Pune Institute of Computer Technology, Pune*
** Corresponding Author Email:kavita.sultanpure1@vit.edu*

blockchain.[5] Decentralized identity management has attracted great attention in academia and industry in recent years, as traditional centralized identity management systems suffer from security and scalability issues. Yet, as sharing interaction within domains has increased, administration and authentication of decentralized identity have raised higher needs for cross-domain trust and faced numerous practical obstacles. To address these issues, R. Chen et al. presented BIdM, a blockchain-based decentralized cross-domain identity management system. [6] Users in centralized infrastructures are unable to authenticate themselves in systems for identity management outside of their application's domain. Users are compelled to rely on their service providers for authentication and data management. Such solutions have been subjected to large-scale data breaches, and it is difficult for users to remember the passwords for many sites. In addition, users have minimal control over their information. The idea of decentralized identification has given rise to the describe a blockchain-based decentralized identity management system that enables patients and healthcare professionals to identify and authenticate themselves transparently and safely across various eHealth platforms [8]

3. Proposed Mechanism

The status of digital authentication demands a high level of faith in third parties. Users must trust websites or service providers to protect their authentication data because personal information may be gathered for data mining, profiling, and exploitation without the users' knowledge or permission. We aim to improve current systems with DAuth solution for authentication with the following features:

1) Trustless authentication: With a blockchain-based system, any user's authentication must be always verifiable not just by one node but by all participating nodes. Authentication is performed without the need for a centralized authentication provider.
2) Not using passwords for login: The core premise is that it is cryptographically simple to establish account ownership by signing a piece of data with a private key. If you successfully sign a specific piece of data generated by our back end, the back end will recognize you as the owner of that public address. As a result, we may create a message-signing-based authentication system that uses a user's public address as an identification.
3) One account: One DAuth account will allow users to authenticate themselves on any websites that are using DAuth as an authentication service provider. DAuth can be used to bind authentication of online

prospect of better handling these concerns. It enables users to share only the relevant portion of their personally identifiable information with a provider of services for their digital identity to be verified. OrgID, a decentralized identification and user-centric data management platform that includes identity registration and authorization procedures, is proposed.[7] The epidemic of COVID-19 has been a true motivator for remote eHealth technologies such as Telehealth. It makes remote care, diagnosis, and treatment more efficient, accessible, and cost-effective. They do, however, have a centralized identity management system that limits patient and healthcare provider identification interoperability. As a result, users are isolated and unable to authenticate themselves outside of their eHealth application's domain. Furthermore, users of remote eHealth apps must entirely trust their service. People are unable to determine whether their eHealth service providers follow regulations to safeguard the security and privacy of their personal information. Ibrahim Tariq Javed et al.

accounts on social media platforms, e-commerce, and financial websites or verification of identity during a face-to-face meeting.

4) At authentication-required services, no user credential data must be stored: Data loss and infringement threats are irrelevant. On the chain, just authentication transaction records will be recorded.
5) Immutable: The transaction logs created by consensus among the nodes are hashed and added to the blockchain. The data stored in an encrypted form is immutable. Any changes to these logs require building the Merkle tree, which is almost impossible.
6) Flexible and resilient authentication: Users do not have to carry around identifying documents all the time. Users could prove their identity by scanning the QR code which will be generated at the third-party websites from the mobile application.

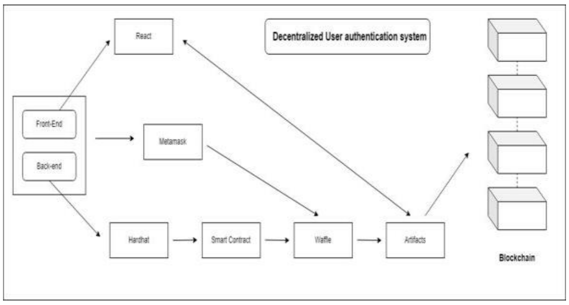

Fig 1 System Architecture

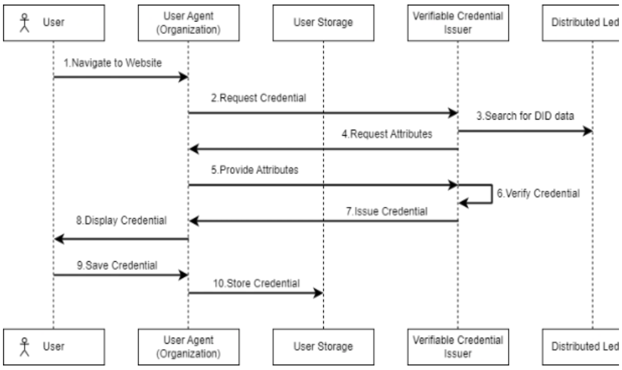

Fig 2 Data Flow Diagram

3.1 Proposed Architecture

The stakeholders in our solution are public users with mobile devices, third-party online services requesting user authentication, and DAuth, the authentication blockchain.

1) Third Party websites or organizations, use our SDK to include the DAuth on their websites.
2) Once the user visits the third-party website, he/she will be able to get the prompt to connect to the MetaMask wallet, after connecting to the MetaMask wallet the user will get two options register and log in.
3) The new user must register to the DAuth, where the public address will be linked to the user data.
4) The user data is hashed using SHA256 and this transaction is recorded on the blockchain.
5) This public address can be used later for authentication purposes.
6) The user can log in to the system by using the MetaMask, the DAuth service will authenticate the user using the public address of MetaMask.
7) If the user information for the public address is present in the blockchain, then the verification data is sent to the third-party website.

3.2 Authentication Algorithm

Our proposed method can authenticate users on the DAuth blockchain from any public platform, give proof of user authentication, and complete any future authentication to any third party at any moment.

Authentication will be done using the following algorithms

1) User registers using the DAuth and the data along with the public address of the metamask is stored onto the blockchain.
2) The third-party websites call createUser() to create a new user, wherein username, email, password, number, and public address will be taken as input. Then the user data is mapped to the public address of the blockchain.
3) The DAuth uses Keccak-256 hash function for hashing the data, H(UserData, Public Address) and publishes to the blockchain.
4) The third-party websites then call isUserOfAddress() wherein they pass the public address of the metamask, and then the function returns a Boolean value for whether or not the data for the particular address exists on the blockchain or not. If the data exists, successful authentication will be sent to the third-party website.
5) If the user chooses to authenticate himself using the username and password method then the third-party websites call validate() wherein the username and password would be hashed using the Keccak-256 hash function and would be matched to the existing data present on the blockchain.

The fundamental defense against these attacks stems from the inability to brute force the incoming data H(UserData, Public Address) into satisfying the authentication hash H. The intruder cannot build a valid pair (UserData, Public Address) since he does not know the private key that the user uses to sign the transaction. Now that a user's authentication has been established, Metamask's Public address can be utilized as an authenticator for user N. This procedure would also enable the creation of a transaction to any public network account. Platform smart contracts will automatically finish the transaction to the Public Address after the receiver's authentication has been completed.

4. Implementation

The proposed methodology has its core implementation in the smart contract which is implemented in solidity and compatible with Ethereum-based blockchains. The smart contract is developed and deployed in such a way that it will be available publically to all users. And only a certain number of resources would be restricted to the admin of the application.

There are 7 methods in the smart contract, out of which two of them are the core of the application, namely createUser and validate.

createUser takes the DTO of the user that is added to the smart contract. Which includes the username and other information. The method thus has vulnerability to attackers as they can create false user accounts, therefore the method is protected with the modifier named only owner which only allows the owner of the smart contract to add users to the database. So admin can have the preferable implementation at their end to authenticate the user’s existence.

Validate Function:

```
function validate(string memory _user,string memory
_password) external view returns (bool)
{
bytes memory b1 = bytes(usersList[_user].password);
bytes memory b2 = bytes(_password);
uint256 l1 = b1.length;
if (l1 != b2.length) return false;
for (uint256 i = 0; i < l1; i++) {
   if (b1[i] != b2[i])
   return false;
  }
  return true;
}
```

As it is not a write function so it will not cost anything to the user.

Validate is the function that authenticates the user who is logging in to the application. It is a boolean-type function that returns the value of whether the user is authenticated user or not. It simply takes the username and password from the user end and maps the password stored in the smart contract and then compares the existing password to the provided one. As the string in solidity is not comparable directly therefore, we need to compare them byte by byte. To reduce the time complexity of the function we have added the condition if the number of bytes is not the same there returns a false value from the function.

isUserOfAdress is the function that can validate the user just by its address. It is a function that checks if the user from a particular address is in the smart contract array or not. It can be useful to validate the user at the runtime of the application, the website can take the user address from the wallet that is added to it and then can validate the user without having to ask for the password. As the wallets are already very secure the developers can trust the address provided.

Also, there could be several ways that a developer can use these methods in their application as the functions are very generic. There could be a system where a developer can fetch the user credentials with any preferable method and validate them through our application.

There are scripts returned for implementation of the methods which can be included in the node modules to create an SDK for the developer's ease.

5. Conclusion and future scope

As a result, the proposed methodology specifies how we can use blockchain technology to create a decentralized user identity verification system. This gives the user confidence in the process because it is completely decentralized and secure. The user data will not be stored in any database that is controlled by a centralized entity. Rather, it will be encrypted and stored in a decentralized blockchain manner with strong security and a transaction-specific hash value. We will have an application that has all its implementation in front of everyone at the same time making it nearly impossible to change that. That increases transparency in the system without any security threats. This methodology has the potential to be a stepping stone in the Web 3.0 space.

References

[1] N. Naik and P. Jenkins, "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology," 2021 IEEE International Symposium on Systems Engineering (ISSE), 2021, pp. 1-7

[2] Z. Yun, C. Chao, W. Haoling, L. Tao and J. Hefang, "Decentralized Identity and Password Authentication System based on Block Chain," 2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS), 2022, pp. 481-485

[3] Zyskind G, Nathan O, Pentland A "Decentralizing privacy: Using blockchain to protect personal data" Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015 (2015) 180-184

[4] Friebe S, Sobik I, Zitterbart M "DecentID: Decentralized and Privacy-Preserving Identity Storage System Using Smart Contracts" Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 (2018) 37-42

[5] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. -K. R. Choo and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2146-2156, Aug. 2020

[6] D. Zheng, C. Jing, R. Guo, S. Gao and L. Wang, "A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs," in IEEE Access, vol. 7, pp. 117716-117726,2019

[7] R. Chen et al., "BIdM: A Blockchain-Enabled Cross-Domain Identity Management System," in Journal of Communications and Information Networks, vol. 6, no. 1, pp. 44-58, March 2021

[8] K. Gilani, F. Ghaffari, E. Bertin and N. Crespi, "Self-sovereign Identity Management Framework using Smart Contracts," NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium,

Budapest, Hungary, 2022, pp. 1-7

[9] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena and D. Gountia, "DecAuth: Decentralized Authentication Scheme for IoT Device Using Ethereum Blockchain," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 558

[10] Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare. Healthcare 2021

[11] Matloob, Samuel, "Exploring the applicability of blockchain to enhance Single Sign-On (SSO) systems" (2019). UNF Graduate Theses and Dissertations. 931https://digitalcommons.unf.edu/etd/931

[12] Kebande, V.R.; Awaysheh, F.M.; Ikuesan, R.A.; Alawadi, S.A.; Alshehri, M.D. A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles. Sensors 2021

[13] Lim, SY, Fotsing, PT, Musa, O & Almasri, A 2020, 'AuthChain: A decentralized blockchain-based authentication system', International Journal of Engineering Trends and Technology, no. 1, pp. 70-74

[14] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications, 2(2), 100014.