Blockchain Based Password Free Authentication

Yashvardhan Singh [*], Sakshi Jain [**], Shubham Rawal [**]

School of computing science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh

DOI: 10.29322/IJSRP.11.04.2021.p11255
http://dx.doi.org/10.29322/IJSRP.11.04.2021.p11255

Abstract- The traditional workflow of authentication uses passwords as the security for any kind of account a person uses on the internet. Passwords are the bane of online existence as they are easy to forget, susceptible to getting stolen and a virtual doorway to one's personal information. Studies have determined that given a choice, most people choose very weak passwords such as birthdays and phone numbers that make them easy to crack. According to Verizon Data Breach Investigations Report, 81% of data breaches are caused due to hacked passwords. This paper proposes a reliable, secure and efficient solution to manage authentication, to enable passwordless authentication by leveraging the power of Decentralised Digital Identity (DDI).
The Internet makes it possible to exchange information between peoples, servers, corporates and Business Enterprises and makes security more and more secure. To truly eliminate all dependencies by using biometric for identification and to access personal and important information, this paper optimizes the standards and build platform using blockchain technology.

I. Introduction

Blockchain can usher in an era of passwordless logins making username and passwords obsolete. A blockchain based authentication solution replaces usernames and passwords with biometric thereby mitigating risks and uses zero trust security. Blockchain technology offers great potential to various sectors with its unique characteristics like decentralisation, immutability and transparency. It stands out from other systems in its exceptional technical architecture, which allows the technology to get adapted for a variety of use cases. The motivation for this work lies in the circumstance that there is currently no systematic review of the blockchain authentication for security. The key topics will be discussed here.

II. Problems in Traditional Methods

The challenges in traditional authentication management methods are grouped as following:

A. Usability: In today's world, people use a combination of username/password in order to log in or to get the permissions to access data and services.. This not only creates hassles but causes pain to remember all the different Login IDs and the password associated with it. Moreover the password reset or recovery procedure is completely dependent on your personal information giving the third party sites or fake sites the opportunity to steal them from you. For remote authentication, in most cases identity owners are obliged to respond to security questions regarding their personal and sensitive information in order to verify their identity. As a result, users pay a price by spending a great deal of time proving their identity, and risking their privacy. A survey report by Centrify in 2014 indicates that even small businesses with 500 employees lose $200,000 annually to employees due to the amount of time spent with password management.

B. Privacy: Identity assets define an individual. Yet, in traditional ways individual's identity assets are stored by third parties. Third parties, whether it is a website, a company or a government, keep silos of identity data. They often require more information than they need in order to verify an individual's identity, as for example, "phone number", "mother's name" and "social security number." Sensitive identity details are often stored in central locations that identity owners are unaware of, shared without their approvals, and exploited for commercial gain.

Security: In traditional ways, each service provider keeps some portion of an individual's identity information for identity verification. Hackers are constantly attacking these systems to steal these information. Any possible breach of identity creates tremendous setbacks both for the identity owner and the businesses. According to Javelin's Identity Fraud Study in 2017 alone, over 16.7 million customers in the U.S. were affected from identity frauds, which costed them a total of $16.8 billion. What is more interesting is that the number of victims affected by identity frauds were increased by 8% comparing to the previous year.

III. Literature Survey

There are very few works that explore the use of blockchain for designing better authentication platforms. The works which in general have tried solving authentication issues using blockchain technology are discussed below.

One proposed a 2FA mechanism to enhance the security of blockchain protocol. The idea is to secure the private key, by splitting the private key into two separate devices so that both the devices are required to be present to perform a transaction.

Ben Cresitello et al, in, explains another way of implementing the 2FA platform. They suggested that instead of using SMS (Short Message Service) of signed tokens for 2FA, we can use a common blockchain that acts as an identity store and has all the required information related to user identity and authorization. The idea is, for any application that requires 2FA, we can interface the application to the blockchain so that, every time a user tries to login using normal credentials, he would be required to submit a signed piece of data to the application.

Bamert et al., in, introduced the idea of a hardware token for Bitcoin. The device having the token communicates using Bluetooth and can perform secure Bitcoin transactions by signing it.

IV. Feasibility Analysis

Biometric authentication will be overlapping with the card based and Login ID based systems market. Biometric not only hides your ID as your biometric is converted into a digital footprint and used to save but also allows you to enjoy hassle free services anywhere.

Benefits of implementation of Blockchain:

a. The blockchain stores the status of process under execution across the involved participants, it creates audit trails. As a result, automated payment can be managed and thus behaves as an active mediator for data transformation or calculation.

b. In order to interact with processes outside the blockchain environment, interfaces or triggers are utilized. They connect process within the blockchain to external world processes i.e. outside the blockchain. To impose security and integrity of contents, smart contracts are not allowed to directly interact with the world outside the blockchain. Triggers are utilized to act as agents of organization.

Secondly, the state of processes is advanced based on the confirming messages

Third, funds and payments can be coded into the process and forth, a changeless ledger maintains a log of transactions,which may not be successful.

References

[1] A Step-by- Step Guide For Beginners, https://blockgeeks.com/guides/ what-is-blockchain-technology/

[2] Know More About Blockchain: Overview, Technology, Application Areas and Usecases,https://letstalkpayments.co-m/an-overview-of-blockchaintechnology/

[3] Deloitte,https://www2.deloitte.com/nl/nl/page s/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

[4] Solidity,https://solidity.readthedocs.io/en/develop/

[5] Ethereum, https://www.ethereum.org/

[6] Datafloq,https://datafloq.com/read/securing-i nternet-of-thingsiot-with-blockchain/

Authors

First Author – Yashvardhan Singh School of computing science & Engineering Galgotias University Greater Noida, Uttar Pradesh akash.yash.singh@gmail.com

Second Author – Sakshi Jain, School of computing science & Engineering, Galgotias University, Greater Noida, Uttar Pradesh sakshi.172015@gmail.com

Third Author – Shubham Rawal School of computing science & Engineering Galgotias University Greater Noida, Uttar Pradesh shubhamrawal4@gmail.com