E-User verification using Blockchain

Prashanth Gone
Siddhant College of Engineering
Sudumbre, Talegaon Maharashtra
Email : parshya946@gmail.com

Sanket Uday Mane
Siddhant College of Engineering
Sudumbre, Talegaon Maharashtra
Email : sanketx125@gmail.com

Tejas Gorde
Siddhant College of Engineering
Sudumbre, Talegaon Maharashtra
Email : tejasgorde87@gmail.com

Pradeep pandit
Siddhant College of Engineering
Sudumbre, Talegaon Maharashtra
Email : -

Abstract

The process of identification is quite hectic and recurring lots of fake identification are created for fraudulent transactions. Tedious work of carrying and managing all our documents. E-identity verification is the system which is proposed to make the process of identification easier and faster with one time user identification and then identifying the user based on the saved data. The user data will be stored in the blockchain system by a central authority. Which will then be used to identify the user with the user's permission. Blockchain-enabled user identification which reduces fraud user identification

Keywords—Verification, Authentication, Identification.

I. INTRODUCTION

The crime of identity theft, an unauthorized access to a person ‘s particular information, has impacted numerous people especially in recent times and the figures increase yearly. According to Javelin Strategy & Research (1), there were roughly one in 15 people likely to be a victim of identity theft in 2017 just in the United States (US) [1]. Thus, having a system which can help consumers in covering access to private data would be veritably salutary. [2] In this design a system called Blockchain grounded Identity Verification System is proposed whereby it's a system which stores an individual ‘s particular records on the blockchain. [3] This system uses the security features of blockchain to allow everyone to know who has access to their data. stoner will register and upload the stoner data along with biometrics, central garçon will be handed with an Ui or any other method can be decided in order to corroborate the stoner details, this stoner data will be stored in the blockchain network, needed reality can also cost the stoner data from the blockchain network [4]. Blockchain is a decentralized database conforming to blocks connected by a hash number [5]. Each block has an address which records power and is continuously streamlined after being vindicated [6]. Polarize means that blockchain is a distributed tally and the information can be viewed and altered by anyone if it's vindicated by the parties involved [7]. This includes a blockchain-grounded particular library system whereby it erected a decentralized transparent inflexible secure particular library operation and service system via evidence- of- X [8]. There's also exploration using real- world illustration called Aadhaar, a system in India to ameliorate effectiveness in penetrating public identification records of an existent

[9]. One of the oldest papers used for the review bandied regarding a decentralized social network identity confirmation, where the design is grounded on the tendency of social networking operations to cluster its druggies with analogous attributes, either through position, interests, or work [10]. Stoner authentication can also be integrated with blockchain whereby the system is designed to be completely distributed [11]. Smart contracts are also employed in this study to allow social networks to pierce authentication records so that druggies do not have to depend on their cognitive capability to flash back id and word, or calculate on a third party [12]. With respect to identity operation on blockchain, smart contracts are made part of the exploration done by where online individualizes are concerned.

II. LITERATURE REVIEW

User authentication in computer systems requires human cognitive ability and relies on a trusted third party, but this paper designs a fully distributed user authentication framework with blockchain technology. [1]. This paper describes a decentralized personal data management system that turns a block chain into an automated access-control manager that does not require trust in a third party [2]. Medrek is a novel, decentralized record management system to handle EMRs, using blockchain technology. It provides patients with a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Medrek incentivizes

medical stakeholders to participate in the network as blockchain "miners" in return for access to aggregate, anonymized data as mining rewards. The purpose of this short paper is to expose a working prototype through which to analyse and discuss our approach.[3]. This paper explores applications of blockchain technology to the concept of "proof of X" such as identity, property ownership, transaction, college degree, medical records, and academic achievements. It describes a novel approach of building a decentralized transparent immutable secure personal archive management and service system. Stakeholders in a consortium oriented blockchain network serve as verifiers and miners that provide delegated proof of stake. A prototype simulation shows that the system is feasible and immune to ID attacks. [4]. Medrek is a novel, decentralized record management system to handle EMRs, using blockchain technology. It provides patients with a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Medrek incentivizes medical stakeholders to participate in the network as blockchain "miners" in return for access to aggregate, anonymized data as mining rewards. The purpose of this short paper is to expose a working prototype through which to analyse and discuss our approach. [5]. Diva is a novel model that uses mining techniques to extract fine-grained community-aware correlations among user profile attributes, with average improvements up to 50%. It exploits a decentralized learning approach and ensures privacy preservation.[6]. Blockchain systems are decentralized and resistant to alteration, allowing for applications such as banking, digitizing healthcare, and digital voting. Integrating Aadhar with blockchain yields illimitable applications in a decentralized, secure, and transparent manner.[7]. This paper proposes a systematic framework for aggregating online identity and reputation information to provide a holistic approach to personal online behavioural ratings.[8]. Blockchain technology provides a secure distributed data storage with keyword search service, allowing clients to upload their data in encrypted form, distribute it to cloud nodes, and grant permission for others to search [9]. Government implementation in Oman has been improving, but still behind expectations.

III. PROBLEM STATEMENT

The process of identification is relatively exciting and recreating. Lots of fake individualities have been created for fraudulent deals. Tedious work of carrying and managing our documents. Lots of paperwork demanded. The reason fraud is so commonplace is because culprits are good at what they do and are continually instituting to find new, better ways to commit fraud. By simply looking at a document, which is how most identification checks are performed, it is easy to be wisecracked into allowing it’s an original and valid document. counting on an individual who is untrained in the complications and rearmost developments in fraud to rightly corroborate identity documents isn't enough. A British passport, for illustration, has eight security features that need to be checked in order to corroborate its authenticity. When you ’re presented with a passport from a foreign country, how do you indeed begin to know how to corroborate its authenticity? Accountants, attorneys or any other largely good fiscal professional just do not retain the necessary chops to corroborate stoner documents to a high enough standard.

IV. PROPOSED SYSTEM ARCHITECTURE

The system consists of User Interface (UI), Nodejs server, MongoDB (database service), Ethereum network (Blockchain). The user can interact with the system through the mobile app which is a cross platform mobile application. The Nodejs server is used to handle the requests from the user and perform the respective transaction in the blockchain network.

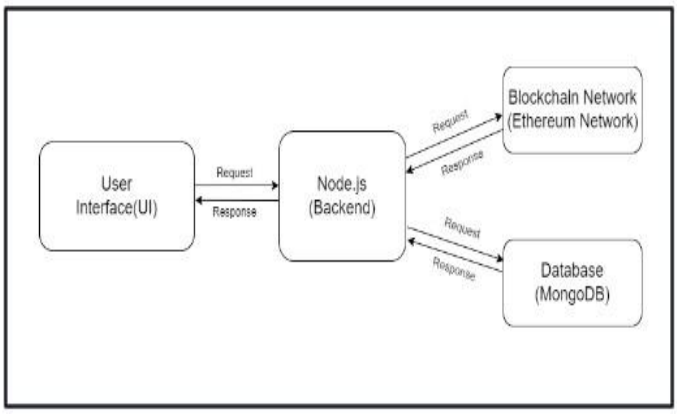


Figure 4.1: System Architecture

V. METHODOLOGY

Agile Methodology

The Agile model is a project management methodology that allows for iterations to minimize mistakes and errors in software development.

The model divides the project into development cycles assigned to each professional on the team, allowing for rapid change and flexibility to accommodate changes throughout the development lifecycle.

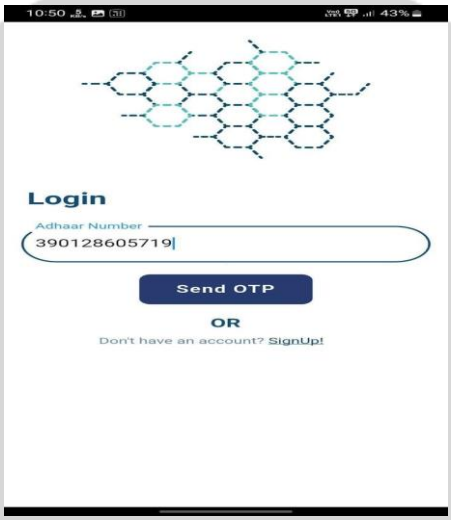
Feature Driven Development (FDD) – Agile is a lightweight and incremental model that focuses on features and requires a high level of design expertise and planning.

Lean software development – Agile and lean manufacturing combine to optimize time and reduce waste, cost and effort.
Scrum – Teamwork, iteration and accountability are essential for successful software development.

VI. RESULT

1) OTP Screen:

This is our login page If the person is already registered, then they can login through their Adhaar number. If the person is not registered then they have to register as a new user.



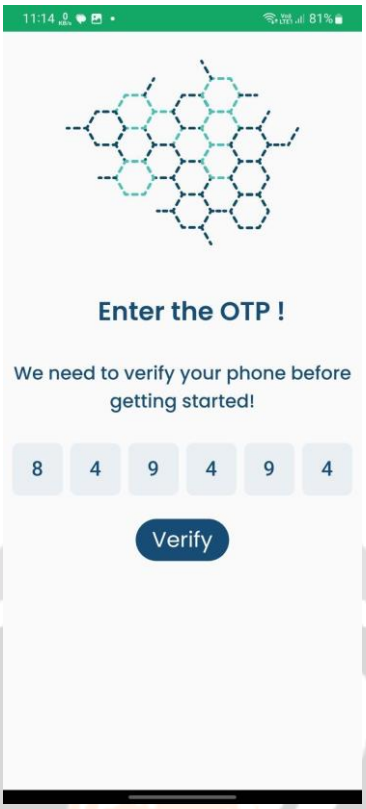


Fig 6.1 OTP Screen

2) Registration Screen:

After clicking on sign up you will be redirected to the registration page where you have to enter all the information related to you. All this information will be sent to the server where central authority will access all the information from the server and check all the data that is uploaded by the user.

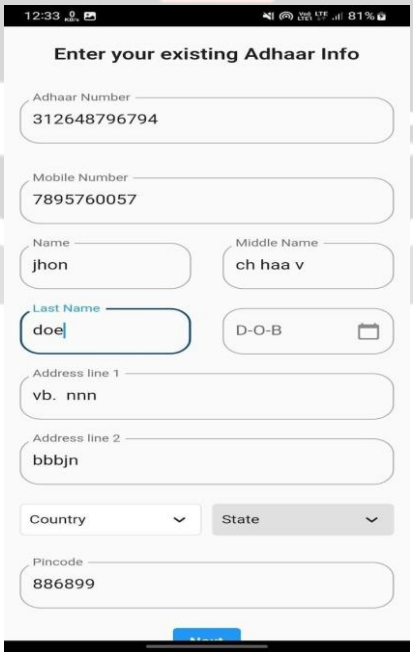


Fig 6.2 Registration Screen

3) Upload Screen:

User has to upload real time photo of all the document and personal photo. central authority can easily check whether the information provided by user is correct or not by using photo which has been upload by user. After verifying all the documents all the information will stored in blockchain network.

Fig 6.3 Upload Screen

VII. CONCLUSION

Identification process can be simplified and the user does not need to carry the documents. Fake identification can be avoided. One time process of identification. The system also describes how a system which enhances the area of blockchain identity is vital in helping the society to gain control of their lives. Since most of the research are focused on the storage system of businesses using blockchain, personal identities of the people should be digitized the blockchain as well.

VIII. REFERENCE

[1] Pascual, A., Marchini, K., Miller, S. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Retrieved from https://www.javelinstrategy.com/coverage-area/2018-identityfraudfraud-enters-new-era-complexity.

[2] Zyskind, G, Nathan, 0., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to ProtectPersonal Data. In 2015 IEEE Security and Privacy Workshops. San Jose, CA: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7163223/

[3] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In 2016 2nd International Conference on Open and Big Data (OBD).Vienna: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7573685/Workshops. San Jose, CA: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7163223/

[4] Chen, Z., & Zhu, Y. (2017). Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging. In 2017 IEEE International Conference on AI & Mobile Services (AIMS). Honolulu, HI: IEEE. Retrieved from https://ieeexplore.ieee.org/document/8027275/

[5] Do, H., & Ng, W. (2017). Blockchain-based System for Secure Data Storage with Private Keyword Search. 2017 IEEE 13Th World Congress on Services. Doi:10.1109/SERVICES.2017.23

[6] Mudliar, K., Parekh, H., & Bhavathankar, P. (2018). A comprehensive integration of national identity with blockchain technology. In 2018 International Conference on Communication information and computing technology (ICCICT).Mumbai:IEEE. Retrieved from https://ieeexp1ore.ieee.org/document/8325891/on Communication

information and computing technology (ICCICT).Mumbai:IEEE. Retrieved from https://ieeexp1ore.ieee.org/document/8325891/

[7] Soliman, A., Bahri, L., Carminati, B., Ferrari, E., & Girdzijauskas, S. (2015). DIVa: Decentralized identity validation for social networks. In 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Paris: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7403568/

[8] Zhang, L., Li, H., Sun, L., Shi, Z., & He, Y. (2017). Poster: Towards Fully Distributed User Authentication with Blockchain. In 2017 IEEE Symposium on Privacy-Aware Computing (PAC). Washington, DC: IEEE. Retrieved from https://ieeexp1ore.ieee.org/document/8166639/?part=1

[9] Chandramouli Subramaniam, Asha A George, Abhilash K A and Meena Karthikeyan. Book on Blockchain Technology.