IDENTITY MANAGEMENT USING BLOCKCHAIN

[1] Madhu M Pandurangi, [2] Bharath B R, [3] Koppresh P, [4] Chandan M, [5] Sangeetha V,
[1,2,3,4] Undergraduate student, Computer Science Engineering, K S Institute of Technology,
[5] Associate Professor, Department of CSE, K S Institute of Technology

Abstract: In the present interconnected world, digital IDs are used to demonstrate identity. These IDs prove to be related to the service being accessed and requires us to apply a significant amount of privacy. The current systems possess number of problems such as proxies, vulnerable to data theft but blockchain proves to be the solution for this type of Identity related problem. In this paper, we describe a decentralized identity management system that ensures users own and control their data by using blockchain technologies. The main objective is to maintain a decentralized system to store identity of a person and protect individual identities and massively reduce fraudulent activities.

Indexed Terms - ReactJS, Blockchain, BigChainDB, Hash.

I. INTRODUCTION

In recent years, Blockchain technology has got more attention in the security field. In past we used to store data in a centralized database which is not that efficient, if the database is breached or if someone has knowledge on security features of it, data inside it can be easily be amended or misused. By using Blockchain the system that could run only under authority, can now run between strangers even they are not trust worthy and that too without any middle-men. This can achieved by using Blockchain, because it uses decentralized technique for storing data and can expect same performance as in centralized fashion, which was not possible earlier using centralized system. Blockchain has been our choice to develop the project, Blockchain holds blocks linked together. Each block in a blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is immutable, meaning the data can only be asserted to the chain and no existing data can be modified. The blockchain is also transparent, meaning any public address transactions and holding are open for viewing. The system is also decentralized; hence the servers won't be overloaded with requests. The system is hence resistant to tampering while being transparent to public.

II. RELATED WORK

We live in the age where nearly everything about our own identity can be found on the web. Our online information impressions are broad, consolidating every little thing about us from our name, age, money related history, work history, locations and social records. The Aftermath 2008 report published by Identity Theft Resource Centre [1] has shown that financial identity theft crimes was reported by 73% of the respondents while 5% reported criminal cases only, and 2% reported governmental issues only. The rest were combination cases: financial and criminal (6%), financial and governmental (9%), and a combination of all three types (5%). By combining the blockchain decentralized principle with identity verification, a digital ID can be made that would act as a digital watermark which can be assigned to every online transaction. The solution can help the organizations to check the identity on every transaction in real time, hence, eliminating rate of fraud[2]. Finding an effective method to protect users from identity theft and in this way protecting consumers and society as a whole is of urgent importance to maintain a healthy economy and stable social environment. The main idea here is to provide the solution for identity theft and Identity management using blockchain tries to overcome the identity theft problems.

III. DESIGN

A design document, also known as a technical spec, is a description of how you plan to solve a problem. While building an identity management application using blockchain, the software must be versatile, reusable, and scalable.

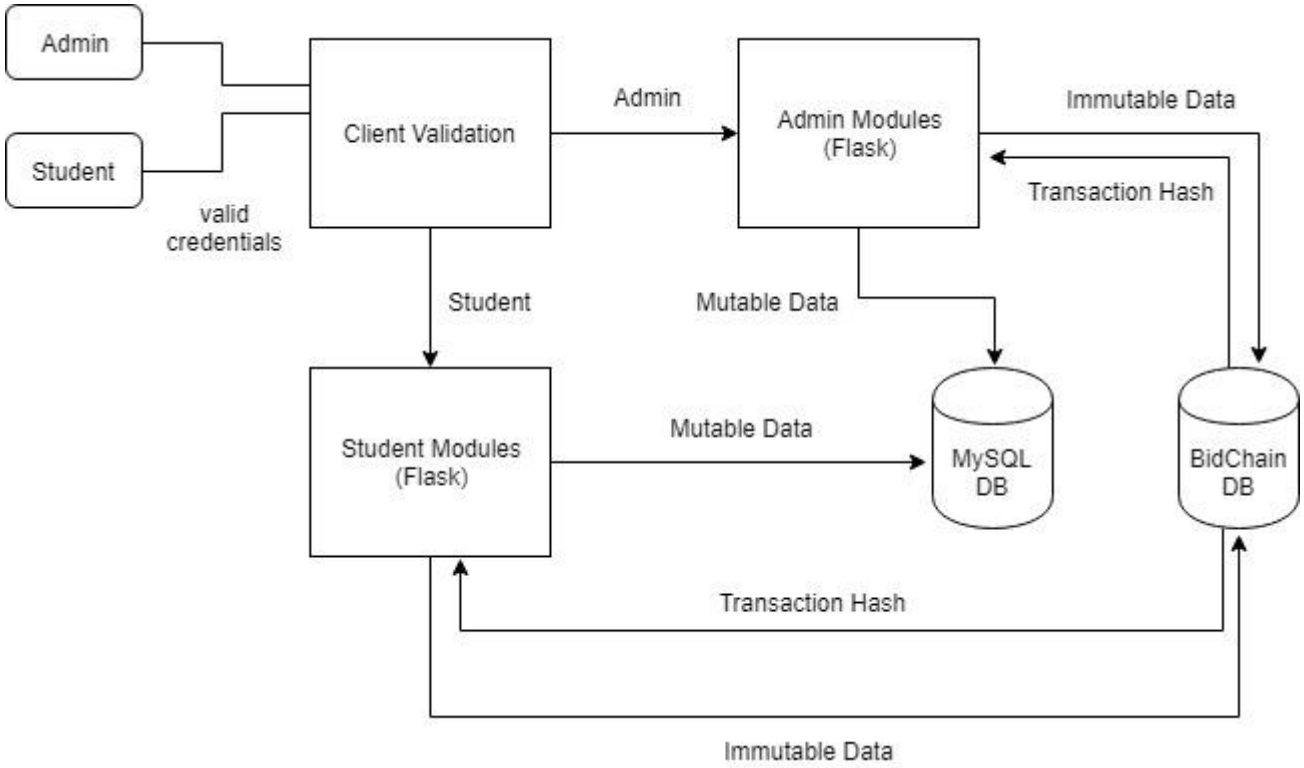

Fig 1. Architectural design of Identity Management using Blockchain.

The Fig 1. depicts the architectural design of Identity Management. In this design we can see mutable and immutable data which are stored in storage entities. As we know Blockchain is immutable, means the data once put away that cannot be changed. Here we are going to feature the Identity Management for college reason, where the student details such as name, student-id, date-of-birth and some of the fields are immutable. This sort of information can be stored in blockchain and the rest of the information such as semester average or CGPA of the student are mutable, such information can be stored in any database and here we utilized MySQL for storing mutable data.

First the college organizational personnel will input the details of the student when the student gets an admission in the college. As shown in the Fig 1. the admin by validating his credentials can enter to the admin module where the authorization is given to keep in touch with the database and to the BigChainDB. He just enters the information, information is automatically divided into mutable and immutable data, and first stored in the BigChainDB, the response sent by the BigChainDB which is the transaction hash will be stored in the MySQL along with the student's alterable information. When the student wants to see his details then he can use the student-id or transaction-id and login to the web-based interface and can see the details. Transaction id is stored in the MySQL database acts as a lookup table to get the individual details from blockchain interface called BigChainDB.

In the same way we can implement the identity management using blockchain in different fields such as vehicle registration, license approval, passport, Aadhar and so on.

IV. TECHNOLOGY STACK

ReactJS: It is a java script library, web interface have been built using ReactJS, which helps the user means the administration faculty to give the inputs such as unique student ID and so on.

BigChainDB: It is a database system with properties of blockchain such decentralization, immutability, assets and tokens, and query. A scalable blockchain database which allows developers and enterprise to deploy blockchain proof-of-concepts, platforms and applications with a scalable blockchain database.

MySQL: The database holds hash values which are present in BigChainDB, hence is used as lookup table when admin of the system queries to perform validation.

Flask Framework: Flask is web framework for python. Using Flask, we have created REST service for backend application.

V. RESULT

The use of identities must be coupled with stronger identity management processes. Identity management was built to provide self-sovereign identity, decentralized approach for storing identity and tamper resistance.
When the system of storing identity becomes decentralized then the people around the world become owners of their own information. Here using our application student's information will be pushed to BigChainDB. The immutability feature of the BigChainDB helps to provide tamper resistance and in case if anyone who is unauthorised tries to change the data will be caught easily.

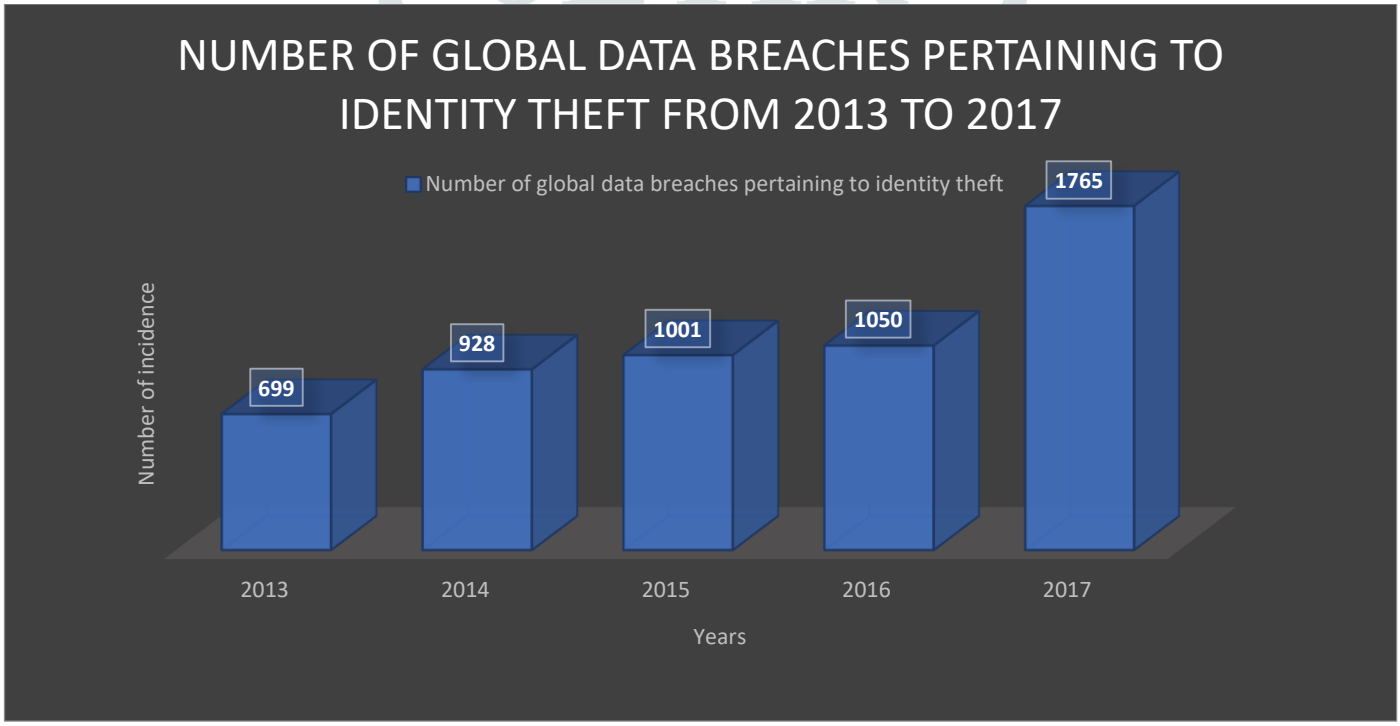

Fig 2. Number of Global Data Breaches Statistics.

The above statistics(Fig 2.) presents a timeline of the number of global data breaches pertaining to identity theft from 2013 to 2018. During the most recently recorded period, the source reported around 609 identity theft attacks worldwide. This statistics will rise awareness in general public and this will make people slowly transform to blockchain technology. Data security and identity management represent use cases well-suited for blockchain technology and areas in desperate need of improvement going forward.

By using decentralized identity management system, people will get the following features:

- **Reduced risk:** This system reduces the risk of tampering the information or the identity of individual.
- **Eliminating security threat:** Eliminated security threat from active accounts that have no valid owner or unapproved configurations.

- **Reduced effort:** Effort is reduced for maintaining security. Blockchain Frame work BigChainDB will handle all the background decentralization process.
- **Fraud and loss prevention:** This is the basic idea to develop the project. Almost all fraudulent activities can be prevented intern preventing loss.

VI. CONCLUSION

Identity Management using Blockchain is a simple concept that can be implemented to prevent tampering of personal identities, which in-turn will be safety. The traditional security parameter is shrinking. Organisations searching for better identity management solutions must take into account the realities of an increasing the decentralization of things and decentralized applications. A robust identity management solution can ease management pains and boost user productivity while lowering costs, reducing demands on IT.

Education institute or any organisation which requires identity management will find good use from the application, blockchain technology implemented to store identity will help the authorities to find any ill activities that might be intruding the system.

VII. ACKNOWLEDGEMENT

The successful project execution would have not been possible without the people who made it possible and whose constant guidance crowned our effort with success. We take this opportunity to express our sincere gratitude to Management K S Institute of Technology, Bengaluru. We would like to express our gratitude to Dr. K.V.A. Balaji C.E.O. K.S. Institute of Technology, Bengaluru, for facilitating us to build and present the project. We would like to extend our gratitude to Dr.T.V.Govindaraju, Principal/Director, K.S. Institute of Technology, Bengaluru, for providing opportunity to publish this paper.

We thank Dr. Rekha.B.Venkatapur, Professor and Head, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for her encouragement.

We would also like to thank, Mr. K. Venkata Rao, Associate Professor, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for his constant guidance and inputs.

We wholeheartedly thank our project mentor Mrs. Sangeetha V, Associate Prof., Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for her support and guidance.

Finally, we would like to thank all the teaching and non-teaching staff of the college for their cooperation.

Moreover, I thank all my family and friends for their invaluable support and cooperation.

VIII. REFERENCES

[1] L. Foley, Sh. Gordon, and ITRC staff, Identity Theft: The Aftermath 2008, ITRC 2008
[2] Blockchain For Identity Management, Ori Jacobovitz, Ben-Gurion University, Beer Sheva, Israel, December 2016
[3] BigchainDB 2.0 The Blockchain Database, BigchainDB GmbH, Berlin, Germany, May 2018