Providing a Secure, Reliable and Decentralized Document Management Solution Using Blockchain by a Virtual Identity Card

Meet Shah, Ankita Aditya, Dhruv Bindra, V. S. Omkar, Aashruti Seervi

Abstract**—**In today's world, we need documents everywhere for a smooth workflow in the identification process or any other security aspects. The current system and techniques which are used for identification need one thing, that is 'proof of existence', which involves valid documents, for example, educational, financial, etc. The main issue with the current identity access management system and digital identification process is that the system is centralized in their network, which makes it inefficient. The paper presents the system which resolves all these cited issues. It is based on 'blockchain' technology, which is a 'decentralized system'. It allows transactions in a decentralized and immutable manner. The primary notion of the model is to 'have everything with nothing'. It involves inter-linking required documents of a person with a single identity card so that a person can go anywhere without having the required documents with him/her. The person just needs to be physically present at a place wherein documents are necessary, and using a fingerprint impression and an iris scan print, the rest of the verification will progress. Furthermore, some technical overheads and advancements are listed. This paper also aims to layout its far-vision scenario of blockchain and its impact on future trends.

Keywords**—**Blockchain, decentralized system, fingerprint impression, identity management, iris scan.

I. Introduction

WE are living in a world where the population has increased at an astronomical rate. Overpopulation has become a major cause of concern and is a deterrent in the development of a nation. With immense modernization in technology, identity management can be linked with digital transformation. The growth rate of the population is 1.14%, out of which, 1.1 billion people are not having an identity [18]. In this age of rapid technological development, individuals still need to carry too many documents when they move to new places. Many countries like India, UK, and African countries are struggling to provide identity to their citizens. Countries like India tried to come up with a solution by creating an Aadhar card, but the system is centralized and trackable by the government [1]. In this regard, emerging technology such as Blockchain could be advantageous. Blockchain is decentralized and secured, which can provide an identity to the aforementioned 1.1 billion people of this world. For instance, Indians have either lost their documents or are not able to manage their records because of a lack of knowledge or technology and due to various other physical and societal reasons [1]. This is where our proposed system shall be a benchmark and aim to provide a solution to these problems.

The proposed system provides a secure, reliable and decentralized document management solution using Blockchain by a virtual identity card. Blockchain is resistant to any unauthorized modification of data. The distributed and decentralized nature of this technology has significant leverage [14]. Being peer to peer, unauthorized crackers and hackers cannot exploit the vulnerability of centralized points, making it more secure. Blockchain has great potential in identity and access management [11]. A virtual identity is assigned to each person that is used in all the major departments such as banking, government, health care, and education [3]. So, a user would have to register once, after which they do not need to manage any of their documents. Their virtual identity acts as a key to unlock the benefits and all the basic needs. Also considering the probability of people who forgets essential passwords and keys, our system would only require the user to remember a single private key for their virtual card, since the verification and validation will be done using voice recognition, retina scanners and fingerprint scanners making the system more reliable. Hence the proposed system solves the problems listed above and finds a better and more unique solution using Blockchain technology.

II. Necessity and Motivation of Research

A. Research

The main requirement for an identity management system is that it should be both secure and reliable. These features are absent in the current identity management systems. The weakest link in the current identity management system is considered to be in government institutes such as banks and credit agencies. In these institutes, third-party involvement without consent is customary, with the private information of the user getting stored at an unknown location and being vulnerable to theft and hacking of data [2]. The industries that suffer from the present identity management system are:

- Government: The time and the cost required to process

Meet Shah is studying in People's Education Society University, Electronic City Campus, Bangalore, Karnataka, India, 560100 (phone: +91-9328243515; e-mail: meet19061999@gmail.com).

Dhruv Bindra, is studying in People's Education Society University, Electronic City Campus, Bangalore, Karnataka, India, 560100 (phone: +91-8511788378; email: ddbindra@gmail.com).

Omkar V.S, Aashruti Seervi, and Ankita Aditya are studying in People's Education Society University, Electronic City Campus, Bangalore, Karnataka, India, 560100 (e-mail: omkarshirigannavar@gmail.com, prinshuchoudary.16@gmail.com, ankita.aditya20@gmail.com).

the verification and authentication is increased as it involves the interaction between several government levels in the form of bureaucracy.

- Bank: Banking becomes less secure as it requires to log in details such as a password for verification.
- Hospital: High-quality healthcare facilities are not accessible to all. The interoperability among the hospital staff and space for verification and other process delays the treatment and causes ineffective healthcare.
- Education: Thousands of fake academic certificates are sold. Therefore, it gets challenging to verify and authenticate them.

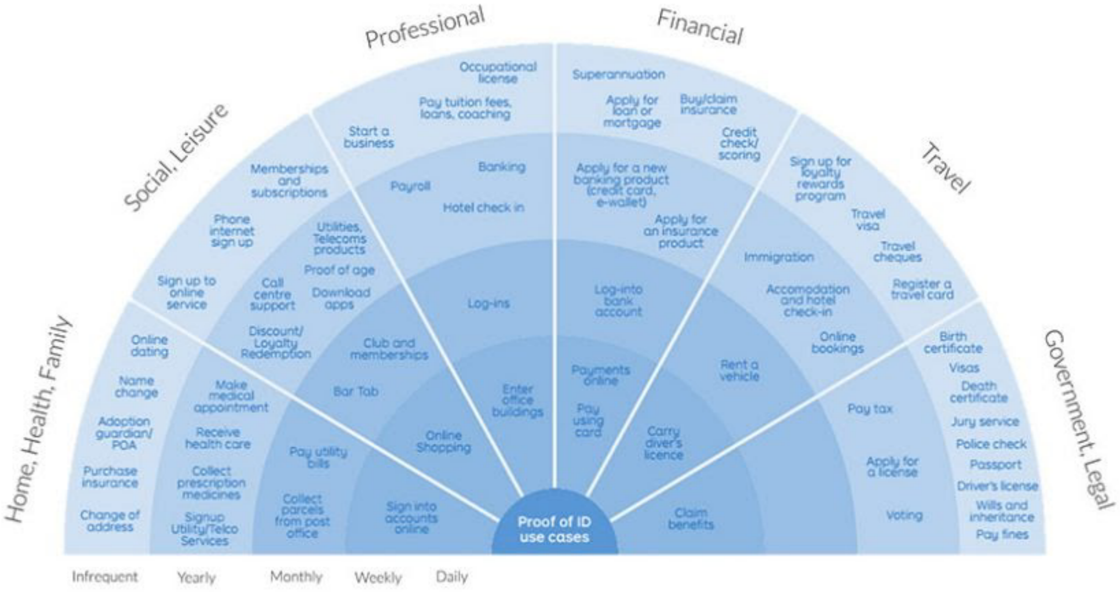

Fig. 1 Activities in various fields that involve identity verification

Portability and verifiability are the two most essential qualities of identity. Along with being portable and verifiable, IDs need to be private and secure, which can be achieved by digitization [4].

Identity management with blockchain can aid in minimizing governmental bureaucracy, building a better healthcare system, detecting academic fraud or duplicity, and forming an effective banking organization [4].

The key challenges faced in these departments under identity management are classified as:

- Identity Theft: Online applications work on centralized servers for storing data; hacking and stealing private information gets very easy for hackers. Information shared online can result in putting an individual's identity documents in danger. Stolen records have always been a major issue and a major threat if it falls in the hands of unauthorized organizations. The breach level index is the proof for the same [2]. A lot of people have lost their identity documents or complained about the cases of identity theft.
- Hassle of remembering multiple usernames and passwords: Users have to sign up and create a unique username and password for each time they access an online platform. It is hard to remember the combinations of username-password and involves high risks of being hacked.
- Know Your Customer: Three stakeholders involved in the present process are users, verifying companies, and third parties that check the identity of the user. The complete system is expensive globally for all the stakeholders. Know Your Customer companies are expensive because of its verification procedure. Furthermore, the process takes a significant amount of time, and third parties have to make onboard customers wait. The global annual spend on Know Your Customer challenges is way too high with figure crossing more than 45 million US dollars per year [2].
- Control: At present, a user has no control over their personally identifiable information (PII). They are neither aware of how many times their PII is shared or used without their permission, nor do they have an idea of where their data is stored. It is crucial that the users have authority on who can access their information.

B. Current Scenario

An identity card of any country is issued and authorized by its government. Identity cards have been made compulsory in around 100 countries, where not having an identity card is illegal [5]. These IDs are verified while travelling and making transactions. Few countries like Armenia, Mexico, Fiji do not enact laws on compulsory identity, with a national ID being optional. Acceptable alternative proof of identity in several countries such as Andorra, New Zealand, and Turkmenistan is a passport, driving license or any other official government documents [16]. Here, national identity cards have not been issued by the government authorities yet, but the other official documents (e.g. driving license, passport) serve the same purpose. Apart from these countries where IDs are not compulsory, in countries like India, a lot of people, with a majority of them being below the poverty line, do not have identity documents.

All the scenarios as mentioned earlier and limitations in the current identity management system were the key factors behind the research, which led to the design of the methodology of the proposed system.

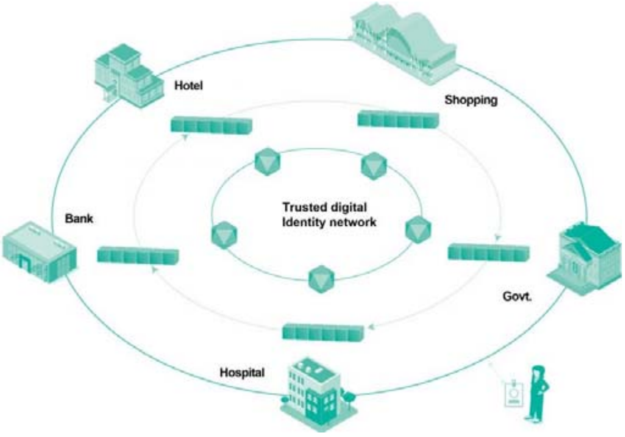

Fig. 2 Major fields that require identity proof

III. Methodology

Our proposed system (Fig. 3) uses asymmetric cryptography [7]. In this kind of cryptography, there are two keys: the public key which is available to all the users and a private key, a unique key that a specific user has. The private key that each user has is restricted to that particular user [12]. A person's basic requirements are categorized into three broad categories: Banking, Government and Other organizations which include education and healthcare (Fig. 2).

Firstly, the users will get registered with the system. The information about the user will get encrypted by two keys: an organization's private and then by the user's public key [13]. Every user's retina scan, fingerprint impression, and voice sample will be mapped to their respective organizations, with the retina scan mapped to banking institutes, fingerprint impression will be mapped to government organizations, and voice sample will be mapped to other organizations which include healthcare and education [9].

The preliminary encryption of the user's data is done by the organization's private key, after which the user's public key is used [17]. Before the data are encrypted by the user's public key, the system will require a retina scan, fingerprint impression or voice sample according to the organization. For example, if a user is getting registered with a banking organization, the user will be asked for the retina scan before encrypting data with a user's public key [13].

When the user visits an organization, the user will only require his/her private key and retina scan, fingerprint impression or voice sample, depending on the organization that he/she visits. The data will be get decrypted first by the user's private key, then by the user's retina scan, fingerprint impression or voice sample and then finally by the organization's public key. Biometric devices will be implemented at every government or non-government facility for the scanning procedure. Considering the direction in which the current technology is moving, these devices may soon not be required since mobile phones are already implementing biometrics for identification of an individual, which can aid the verification and make the process straightforward. This system will provide authenticity, integrity, non-repudiation, and confidentiality. The user can easily extract the documents wherever and whenever needed [10].

IV. Advantages

William Mougayar, the author of the book- The Business Blockchain, has said that the old question "Is it in the database?" shall be replaced by "Is it on Blockchain?" [19]. Inspired by this great Blockchain mentor, the proposed system works with Blockchain as its backbone. Its advantages are:

A. Distributed and Decentralized System

Since data are stored in blocks on a distributed network, the decentralized system gives the convenience not to have a single point failure. Blockchain data are often stored in many devices on a distributed and decentralized network of nodes, so the system and the data are highly resistant to technical failures and malicious attacks. Each network node can replicate and store a copy of the database and, because of this, a single node going offline does not affect the availability or security of the network [15].

B. Universal Virtual Identification

Considering India, where a person needs to maintain a passport, Aadhar card, and various other documents just for identity validation and proof of citizenship, the proposed system removes the tedious task of managing digital and physical documents and integrates all the systems to a universal virtual identity card [15].

C.Authenticated and Authorized Access [Server Side]

The authentication and authorization policy of the proposed system sets it apart from the rest. The department gets access to the relevant information required by that particular department and nothing else [15].

No Dependency on Any Physical Environments

If there is a loss of important physical documents due to unforeseen circumstances such as natural causes, there is no significant impact on the system. Bitcoin is a great example and motivation where irrespective of government breakdown or natural calamities there is no such impact on the value of making the system more rational [15].

D.Less Corruption and Fraud

The proposed system is highly transparent in the identification process. It removes the middle layer leading to less corruption and fraud [15].

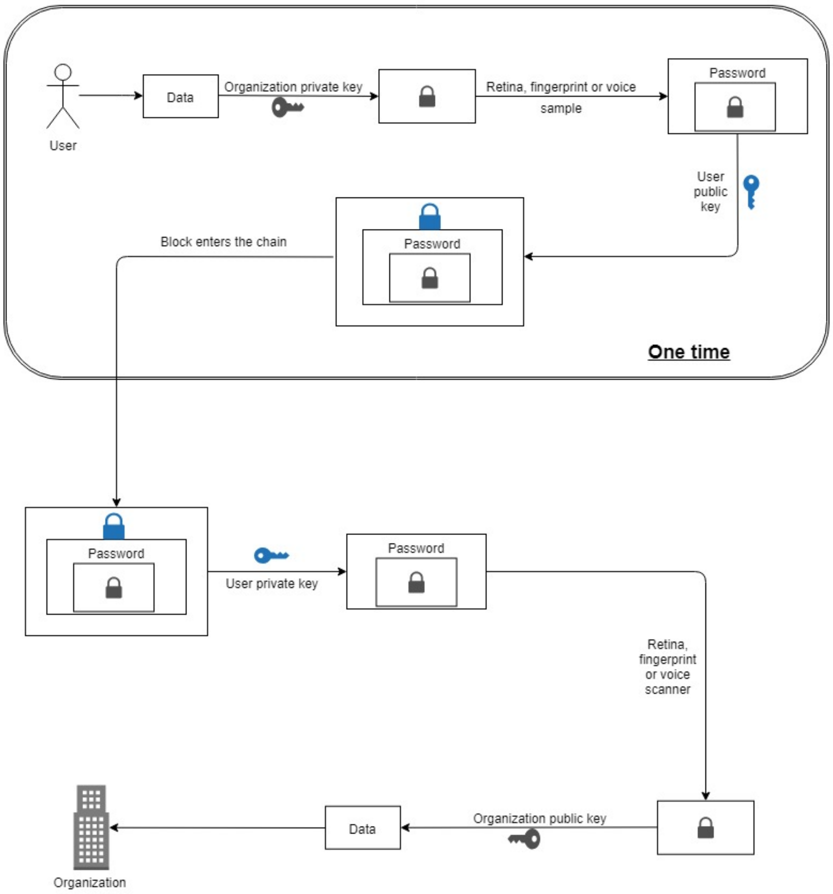

Fig. 3 Flow diagram of the Proposed System

V. Disadvantages

Blockchain evangelists have been successfully able to show the power of Blockchain and its associated technologies. But every technology has its limitations, and so does our proposed system:

- High cost: Biometric devices which consist of fingerprint scanners, iris scanners, and voice recognition systems are expensive and having such systems makes it very costly to operate. Maintaining Blockchain and distributed systems is costly, as well [6].
- High Complexity: It runs on complex algorithms and requires large amounts of computing power. High complexity leads to lesser efficiency and the need for high-speed computational power [6].
- Difficulty in Scalability: It is very difficult to scale a large number of users, resulting in longer throughput. Highly complex encryption-decryption algorithms and extensive rules and regulations to be followed for adding a block to the chain make it challenging to scale [8].
- Conflicts with the government: Issues will arise in the acceptability of this system by the government of all the countries around the world because the proposed system eliminates third party involvement and this might not be an approach that the government would be keen to follow [8].
- Time to adopt the technology: It is difficult for an individual to adapt entirely to the proposed system since it is based on sophisticated technology, and to comprehend it would be an arduous task. Dealing with over a billion people will be a huge task, and the time to adapt the technology may be in years or even decades with the current standards and distribution of education and technology the people possess [8].

VI. Conclusion

Today’s research will drive the technology of tomorrow. Blockchain technology has a great future all around the world, with its impact in the financial sector and identity management serving as proof. A universal identity provided to every individual will make all the documents available at a single place and in a secure way. People shall no longer need to carry any documents while on the move to any location, making the whole process less cumbersome. The proposed system is considered more reliable than the existing identification systems. The feature of integrating all the systems and providing a universal identity for all is itself a boon and shall have a significant impact on the world. The proposed system shall be an innovative way for identity management by providing a reliable, secure and decentralized document management solution with the help of a virtual identity card.

References

[1] India's identity crisis: Between Aadhaar, passport, PAN and NPR, why are we still struggling to prove our identities? URL: https://www.dailymail.co.uk/indiahome/indianews/article2297714/Indias-identity-crisis-Between-Aadhaar -passport-PAN-NPR-struggling-prove-identities.html.

[2] A brief overview and description: Blockchain Identity Management: Enabling control over Identity URL: https://www.leewayhertz.com /blockchain-identity-management/

[3] Open Source Decentralized ID pass solution URL: https://www.idpass.org/

[4] Identity Management with Blockchain: The Definitive Guide (2019 Update) URL: https://tykn.tech/identity-management-blockchain/#How_to_prevent_identity_fraud_and_identity_theft_if_Im_doing_Identity_Management_with_Blockchain

[5] Privacy International – ID Card Frequently Asked Questions URL: https://web.archive.org/web/201109030740 29/https://www.privacyinternational.org/article/id-card-frequently-asked-questions

[6] Article on “The 5 Big Problems With Blockchain Everyone Should Be Aware Of “by Bernard Marr URL: https://www.forbes.com /sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#3594cfff1670

[7] YouTube video on "Blockchain explained in 7 minutes by Simply Explained - Savjee URL: https://www.youtube.com/watch?v=SSo_EIwHSd4&feature=youtu.beY.

[8] 7 Challenges to Blockchain Adoption in 2019 by George Burlakov URL: https://technorely.com /blog/blockchain-adoption-challenges/

[9] A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? URL: https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work

[10] Architecture of the Hyperledger Blockchain Fabric∗ by Christian Cachin, IBM Research - Zurich CH-8803 Ruschlikon, Switzerland

[11] Blockchain for Identity Management by OriJacobovitz, Technical Report #16-02, December 2016

[12] Introduction to Blockchain Applications By Jonathan Reichental URL: https://learning.oreilly.com/learning-paths/learning-path-introduction ‘/9781492029731/

[13] Why Do I Need a Public and Private Key on the Blockchain? - Leon Di URL: https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76

[14] How does a blockchain work - Simply Explained by Savjee URL: https:// www.savjee.be/videos/simply-explained/how-does-a-blockchain-work/

[15] Book on BLOCKCHAIN by Cybrosys Technologies Limited Edition

[16] World Privacy Forum URL: https://www.worldprivacyforum.org/ 2017/07/national-ids-around-the-world/

[17] Blockchain Tutorial for Beginners by Telusko URL: https://www.youtube.com/playlist?list=PLsyeobzWxl7oY6tZmnZ5S7yTDxyu4zDW-

[18] 1.1 Billion people without official identity URL: https://inclusivity.network/en/inclusivity-1-1-billion-people-without-official-identity-id/