e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

USE OF BLOCKCHAIN TO PREVENT IDENTITY THEFT

Shalini Lamba*1, Mayank Singh*2, Ansh Kapoor*3

*1Assistant Professor, Department Of Computer Science, National P.G. College, India.

*2,3Student, Department Of Computer Science, National P.G. College, India.

ABSTRACT

The primary areas of concern in digital identity management are security and privacy. The existing identity management system is neither secure nor trustworthy. Users are required to verify their identity at every step using a variety of government-issued I.D.s such as a voter I.D., passport, or Pan Card. Blockchain Identity Management is a decentralized and secure solution that puts consumers back in control via a distributed trust model. Blockchain has evolved remarkably from the distributed ledger technology created to track bitcoin holdings to replace old systems with a highly trusted mechanism for managing identities. Blockchain can allow people to have greater control over their own identities. Organizations can utilize the information solely with customers' approval, and no central organization would be able to jeopardize a consumer's identity. Blockchain identity management benefits can completely transform the digital landscape. Blockchain applications in digital identity management present viable prospects for improving security, transparency, and control over data. In the long run, improvements in existing identity management systems are inevitable.

Keywords: Decentralized, Blockchain, Security, Distributed Ledger, Identity.

I. INTRODUCTION

A digital identity is an online or interconnected identity created or claimed on the Internet by an individual, organization or electrical device. These users may also create more than one digital identity through different platforms. A digital identity is a set of verified digital attributes and credentials for the virtual world, analogous to a person's identity for the physical world. Usually granted or regulated by a national I.D. scheme, a digital identity identifies a particular person online or offline. Unique identities and use patterns make it easy to detect individuals or their gadgets. Website owners and advertisers typically use this information to identify and track users for personalization and deliver customized content and advertisements.

Because a profile often includes components of a person's true identity, digital identities come with privacy and security threats, including identity theft. Pseudonymous profiles can also reveal individuals identify through cross-site data analysis. While passports and licenses identify individuals in real life, the existence of such personally identifying information (PII) online may create more concerns than benefits for the user. Several authentications and authorization methods have been explored, but no standardized and certified mechanism exists to identify digital identities.

Digital identity is essential for the continued development and viability of our digital economy, and it is fundamental to every segment of society. Identity theft takes a toll on customers and poses a severe threat to online businesses. Cybercriminals deploy many methods, including data breaches, account takeovers, and credit card fraud, to pursue evil purposes.

II. WHAT MAKES UP DIGITAL IDENTITY

The information that defines your digital identity can be classified into two major categories: your digital attributes and your online activities. These pieces of information, either alone or paired together, can be used to identify you. A digital attribute is a piece of personally identifiable information (PII) placed in online records available to private and public sector enterprises and government agencies. These are typically utilized when opening a bank account, paying taxes, applying for a job, or enrolling in universities. Digital activities are virtual behavioural patterns such as your search history, social media activity, mobile phone, and other data your devices track, such as your location.

A digital identity evolves organically from personal information on the Internet and the shadow data created by individuals' online behaviours. A digital identity may be a pseudonymous profile attached to the device's I.P. address, for example, or a randomly-generated unique identity.

Examples of data points that can assist establish a digital identity include:

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

- Username and password
- Purchasing habits or history
- Date of birth
- Social security number
- Online activities, such as electronic transactions
- Medical history

III. TYPES OF IDENTITY THEFT

Identity theft occurs when someone uses your personally identifying information for illicit or illegal activities. Here are some common types of theft that happen to people over the Internet:

1. **Financial Identity Theft:** When someone uses another person's personal information for financial gain, it is called financial identity theft. Financial identity theft is by far the most common form of identity theft. It compromises your existing financial account(s) or establishes new financial accounts in your name by an unwanted third party. Checking and savings accounts, credit and debit cards, loans, medical billing accounts, and insurance are all examples of accounts. Financial identity theft can lead to debt collection and bankruptcy problems for victims.
2. **Medical identity theft:** It might not seem like actual identity theft, but it happens. Medical identity theft is when a thief poses as another individual to receive health care services. Fraudsters may exploit your name and insurance details to Get prescriptions for medications, access medical treatments, from check-ups to pricey operations, and obtain medical devices and supplies, such as wheelchairs or hearing aids. This can result in you having invoices for drugs, services, or equipment you did not require, ask for, or even obtain. These items may have been added to your medical and insurance records. An erroneous medical record can make it difficult for you to get the care you need in the future and possibly affect insurance coverage.
3. **Criminal identity theft:** This identity theft occurs when someone arrested by law enforcement uses another's name instead of their own. By fabricating a fake I.D. or presenting a stolen I.D., such as your driver's license, to the police, they may be able to pass this off as legitimate. It might be challenging to detect this type of fraud until the results are evident, such as receiving a court summons. The court may issue a summons if a criminal uses your I.D. to pay unpaid parking charges. There may also be a bench warrant issued for your arrest. For example, unpaid parking tickets can result in a bench warrant. You may then be taken into custody, even during a regular traffic stop. A background check is issued. Sometimes, authorities will maintain an identity theft victim in their database, identifying it as an alias for the real criminal. This can result in a bogus criminal record on your background check. This can create problems for landlords and employers.
4. **Synthetic Identity Theft:** Synthetic identity theft involves creating new identities by using actual people's information. It is one of the most widely practised forms of financial crime online today. Fraudsters may utilize data like birthdates, residences, and Aadhaar from genuine people, combining them to create a phoney profile. They can then use this persona to seek loans or credit cards or perform other financial crimes—kids and older individuals are likely to be prone to this fraud since they rarely utilize their Aadhaar. The most critical aspect of synthetic identity theft is recognizing the warning signs and acting quickly. Be aware of mail addressed to a different person using your address and phone calls or letters regarding new credit accounts. You can further safeguard yourself by routinely reviewing your credit reports for unusual changes and setting a security freeze.
5. **Child identity theft:** We all want to safeguard our children from evil actors, especially when identity theft. Exploiting a minor's information to commit financial fraud, such as opening a new account or line of credit in the child's name, is known as child identity theft. The thief could even use the child's identity to obtain a driver's license, apply for government aid, or purchase a home. This is generally easier than targeting an adult because most youngsters do not have credit reports or financial accounts, making them a blank slate. Unfortunately, child identity theft is often conducted within the family by a relative who has access to the child's data, such as their birthdate and address. Moreover, many children may not realize they have been targeted until they are adults - for example, they apply for a loan. The problem may have been growing for years at this point. So, it is crucial as a parent to be alert to child identity theft.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

IV. REASONS TO FOCUS ON DIGITAL IDENTITY

With the rapid advancement of technology, digital identity has become a vital aspect of our lives. For your social media profiles, you will need an account where you may enter personal information like your name, address, date of birth, phone number, and other details. The digital identity enables you to communicate with and use various internet-based services, such as banking services.

Due to its crucial role in online financial transactions, digital identity has been under intense examination in recent years. It is critical for expediting the client onboarding process while also assuring accuracy and preventing fraud. Anti-Money Laundering (AML) activities are also hampered by digital identification. Most importantly, digital identity management focuses on citizen service standards and efficiency. As a result, a robust digital identity platform could aid in delivering a variety of services.

The lack of security commonly assumed from identity management drives the need to consider blockchain identity management benefits. The transition to the digital era has ushered in a slew of new identity-theft strategies. As a result, hackers, scammers, and other malevolent actors utilize new identity theft techniques to defraud individuals of their money. Furthermore, traditional identity management systems that rely on paper-based evidence worry about identity theft.

Around 16.7 million people were victims of identity fraud four years ago. According to Javelin Strategy & Research's 2021 Identity Fraud Study, identity fraud scams accounted for about $43 billion of the $56 billion in total fraud losses in 2020. As a result, it is clear that present identity management systems need to be improved, and blockchain could be the most viable solution.

V. THE PROBLEM: CENTRALIZATION

To comprehend how blockchain technology may be used as an identity management solution, it is necessary first to comprehend how the present system's flaws have emerged. In the early days of the Internet, it was a peer-to-peer, decentralized web of connections so that any user could connect with any other user without an intermediary. Third-party intermediaries evolved as the Internet got more privatized, and they became more vital to the Internet's structure.

Servers may (and have) been hacked, and the concentration of personal data in the hands of a limited number of organizations raises the danger of further breaches.

Everything from providing website security certifications to controlling access to the Internet to curating individual online identities was taken over by a tiny handful of firms. Because of this centralized control, these firms accumulated massive amounts of personal data on servers from everyone who uses the Internet. These systems can (and have) been hacked, and the concentration of personal data in the hands of a small handful of firms increases the likelihood of future breaches.

VI. SOLUTION: BLOCKCHAIN DIGITAL IDENTITY MANAGEMENT

People nowadays require a better means to handle their identity than paper-based papers. People will be able to check and confirm their identity using the Blockchain Identity Management app.

Step 1: Download and install the mobile app

To confirm his or her identification, an individual must first download the mobile app from the play store or app store.

A user will create a profile on the app after installing it on their mobile phones.

The user will receive a unique I.D. number once the profile is created, which will allow companies to access the user's identification papers.

Step 2: Uploading the documents

After receiving an I.D. number, the user must upload government-issued I.D.s to the app, which will be kept in IPFS and hashed addresses stored on the blockchain.

The program will extract personal information from these I.D.s in order for the user to self-certify his or her information.

The user will own the data. It assists users in determining which information should be shared with organizations. No data can be shared with identity thieves without the user's permission.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

Step 3: Smart contracts generate the trust score of the person

Assume there is a score that determines a person's trustworthiness.

While creating a self-sovereign identity, smart contracts containing business logic might establish a trust score for a person based on the information they offer.

Step 4: Third-party companies requesting access

A notification will be provided to the persons who hold the identity whenever any organization needs to access specific details of that person for authentication purposes.

Third parties can utilize identifiable information to authenticate a person if the user enables companies to access their details. Individuals would also be able to track how their personal information was used.

The user's data and information are not stored on the blockchain. Instead, only the blockchain will record transactions between identity holders and businesses.

If an immigration authority uses an app to verify a person's identification, the transaction will be added to the blockchain and viewable to all connected nodes.

Let us take a closer look at the example.

Assume Rahul needs to verify his identity to apply for study abroad programs. As a result of the blockchain-enabled identity management tool, the education centre can rapidly verify his identification.

Rahul will give the centre the unique I.D. number, which will allow them to request information access. The education hub can review his documentation when he validates the request, and the transaction will be recorded on the blockchain.

Note that all PII (personally identifiable information) will be encrypted and kept on the phone through IPFS.

Smart contracts, as previously stated, can be used to trigger business rules and establish a trust score for each individual utilizing blockchain identity management. However, what exactly does it imply? How will the trust score function?

We will go through how the trust score can assist an organization in determining the validity of a user.

What is the trust score? What is the mechanism behind it?

The higher the trust score, the more trustworthy an individual will be. Smart Contracts can help enterprises confirm users' identities in real-time by generating a trust score.

By submitting many papers to the app, users can increase their trust score.

It is possible to determine whether a user's account is suspect or authentic based on their trust score. Identity should also be employed frequently to maintain or improve the trust score.

For the first six months after signing up, a user might be deemed a beginner, allowing them to build their trust score. They will have to upload the essential information within that time.

For example, the user's trust score can be checked if Bank of America has to verify a person's genuineness before issuing a loan. It can provide the bank with information on a person's dependability, saving time and money.

The following are three criteria that can aid in the development of a trust score:

Documents can be uploaded.

The higher the number of identities documents a user submits, the higher the trust score. It is the most critical factor for newcomers to consider when calculating their scores.

The data should be consistent.

The system checks to see if fields like name, date of birth, and so on are consistent across all uploaded papers. The trust score will improve as more positive matches are made.

Continual usage

Users may be required to use the system frequently to maintain and improve their trust score.

The following are three things that may cause the trust score to drop:

The trust score suffers when relevant papers are not uploaded to the system.

The trust score will be lowered if a user does not let particular organizations access to verify their identity.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

Regular changes in their personal information may erode confidence, leading to the person being labelled a suspect user.

VII. BENEFITS OF THE BLOCKCHAIN IDENTITY MANAGEMENT SYSTEM

In the wake of the crypto-craze, blockchain technology, the digital ledger system that underpins such currencies, has gained prominence. However, current calls to reclaim personal identity make the decentralized nature of blockchain more enticing. Recent consumer data breaches at Orbitz, Saks Fifth Avenue, and Delta Airlines show that our data is especially vulnerable to fraud when housed in centralized systems. As more global banking and business goes online, the temptation for fraud and theft grows. Decentralization, a significant element of blockchain, may help keep identities safe.

- **Interruption of Identity Data**: To the extent that blockchain can answer the fundamental identification question, "Who am I?" rather than "Am I Who I Say I Am?" These technologies can securely store and make available sensitive data like our financial and health records. The rising internet presence of service providers has increased our need to present this data at the moment of service, sale, or care. We are in a "risk race to the bottom" if we keep up with this desire by presenting every enterprise with a complete profile of our personal and financial lives.
- **Control over our data and its sharing**: Blockchain-based data may be disseminated among an extensive network of people like us, giving us more control over our data. We must own the cryptographic keys that unlock it to own our data. A blockchain is not required for users to have more control over their data. Cryptographic keys, which secure data like long, complex passwords, are crucial. Putting the keys on a blockchain and establishing ownership opens up new possibilities. Rather than directly communicating with an individual or organization, one can check facts on the blockchain ledger. Our data will be shown only when needed as both parties adopt a "presented as needed" methodology for data sharing. This and other blockchain technologies might drastically revolutionize today's know your customer (KYC) operations. Other approaches to alter today's passive, wholesale data-sharing model include segmenting data so only those who need it can access it. Custom permissions can be put up for data storage on the blockchain. For example, your insurance company may access your health data, but not your bank.
- **Raising The Fraud Entry Bar**: Using blockchain in this way would require a cybercriminal to switch identities one at a time, rather than having access to a centralized database of people's bank cards, social security numbers, etc. A centralized architecture provides a large attack surface and a single point of failure for identity, which is undesirable for sensitive data. Decentralization and public-key cryptography (PKI) reduce the scalability of cyberattacks like significant data breaches. It may disrupt the fraud paradigm enough to reduce widespread identity theft. Because the blockchain database is encrypted, only those with the crypto keys can access it. Blockchain technology maintains the line of trust by requiring evidence of credentials, server permission, and network compliance to recognize the request.
- **Pilot Trends and Data Privacy**: Consumers seek more control over their identities, as demonstrated by the emergence of E.U. rules like GDPR and PSD2. Similar regulations may arise in the U.S. following several data breaches and overshares like the Facebook incident. Decentralization and PKI in blockchain technology may enable self-sovereign identity, improving security and confidence in online services. Companies like Nestle, DHL, and Walmart have already adopted and used these networks to meet consumer, vendor, and internal security concerns.

VIII. CONCLUSION

Because a decentralized method removes the target, blockchain technology may help businesses save or reallocate I.T. expenses presently spent defending big pools of targeted data. Companies like Microsoft are forming industry alliances to establish a new digital identification method. Many service providers (banks, e-commerce, brick-and-mortar) possess our data without blockchain. That implies our data is spread over thousands of databases with varying levels of security.

With blockchain technology, consumers regain control of their data, a loss of confidence that hurts businesses and disappoints well-meaning corporate executives. Consumer identity fraud is the root of the problem and maybe addressed with a solution that shows great promise.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

IX. REFERENCES

[1] Blockchain's role in curbing identity theft - https://www.allerin.com/blog/blockchains-role-in-curbing-identity-theft

[2] 5 Common Types of Identity Theft - https://www.mcafee.com/blogs/privacy-identity-protection/5-common-types-of-identity-theft/

[3] Blockchain Identity Management: Enabling Control Over Identity –

[4] https://www.leewayhertz.com/blockchain-identity-management/

[5] digital identity - https://www.techtarget.com/whatis/definition/digital-identity

[6] Can Blockchain Solve Identity Fraud? –
https://www.forbes.com/sites/forbestechcouncil/2018/05/31/can-blockchain-solve-identity-fraud/?sh=143f66c07289

[7] Blockchain Identity Management: The Definitive Guide –
https://tykn.tech/identity-management-blockchain/