OPEN ACCESS Freely available online

ISSN: 2472-114X
International Journal of Accounting Research

Commentary

Enhancing Security: Blockchain in Integrated Identity Systems

Tanki Shanav*

Department of Computer Science and Engineering, Western University, Richmond St, Canada

DESCRIPTION

An unified identifier known as an integrated identity allows users to access many corporate services from a single network. The dangers and threats include identity theft, centralised administration, auditing limitations, and lengthy breach investigation processes. The article provides a strategy for developing marketplace's blockchain-based, integrated identity system by automating and decentralising the development and auditing of robust and secure characteristics. Those that trade on the open market act as nodes in a distributed blockchain network, allowing federated identities to expand. Members of this network get access to all of the partner companies' services through a single federated identity.

IoT sensors and wearables can automatically log real-time data, identify patterns, and flag issues. Because every blockchain transaction is totally visible, participants can see which services they're using, and users can keep track of how their identities are used. Implementation on a permissioned blockchain and a public blockchain was done to test the proposed architecture.

A requestor can be recognised using unique identifiers, granting them access to a service or place. Personal information, biometric information, and personal papers are all examples of data that frequently falls into this category. Identity theft occurs when someone uses their personal information such as financial account information, computer information, or information from physical locations to get access to anything. Digital identities can take several forms, such as documents, smart cards, and digital identities.

Governments and corporations are always working to secure identities and guard against loss, fraud, and theft in order to preserve these identities and avoid serious harm. New technologies are required to deliver durable and secure identities while reducing the potential costs of breaches. As the internet and mobile devices have risen in popularity, digital identities have become increasingly significant because they allow consumers to connect to online services quickly, remotely, and economically. The technology utilised for identity authentication is equally as authentic as traditional identification, which is provided and approved by an identification provider outside the cloud.

People are growing increasingly concerned about their digital identities. Many people are particularly concerned that their identities may be used unlawfully, such as through fraud or theft, causing financial and reputational loss. The governments of the United States of America and Canada have issued data that are similar, research and strategy shown that identity theft is increasing year by year.

It would be difficult to develop a digital identity management system without substantial technological challenges. The majority of victims of identity fraud or theft are not immediately notified of the crime, and it may take years to realise its full consequences. Identity breaches are common among firms that use strong encryption to safeguard their customers' identities.

A federated identity is a single identity generated to obtain access to the platforms of multiple service providers. Users can use a federated identity to access multiple organisations' apps. There is a potential that the many market sectors will split up or merge into one. This concept is effectively demonstrated by the healthcare industry, which includes insurance companies, medical facilities, and hospitals. Customers can access all of their services with a single identity by utilising an integrated identification system. This identity could be used to implement Single Sign-On (SSO) in the marketplace.

Future federated systems, however, should have the technology to do so, as the federated systems that currently serve these marketplaces are incapable of providing access to services and data, let alone monitoring and recording all ongoing transactions. Auditing facilities may help to improve the overall security of businesses in the marketplace by establishing unbroken chains of evidence. Similar to the distributed ID paradigm, the collective identification of a federated system confronts various issues, including an investigation to breach security, identity leakage, and centralization. To establish a more powerful federated identity system, new technologies must be investigated to help with these issues.

Correspondence to: Tanki Shanav, Department of Computer Science and Engineering, Western University, Richmond St, Canada, E-mail: tankishanav@gmail.com

Received: 12-Mar-2024, Manuscript No. IJAR-24-25178; **Editor assigned:** 15-Mar-2024, Pre QC No. IJAR-24-25178 (PQ); **Reviewed:** 29-Mar-2024, QC No. IJAR-24-25178; **Revised:** 05-Apr-2024, Manuscript No. IJAR-24-25178 (R); **Published:** 09-Apr-2024, DOI: 10.35248/2472-114X. 24.12.369

Citation: Shanav T (2024) Enhancing Security: Blockchain in Integrated Identity Systems. Int J Account Res. 12:369.

Blockchain technology is an excellent choice for this purpose due to its decentralisation and security features. A distributed ledger system, or blockchain, uses cryptography to record transactions and other data in an immutable digital format. Smart contracts are computer programmes that facilitate business logic and transaction execution on the blockchain network. Numerous current identity management systems have lately adopted blockchain technology. Because of its immutability and encrypted transactions, blockchain has been utilised sparingly in identity management.