OPEN ACCESS Freely available online

ISSN: 2472-114X
International Journal of Accounting Research

Perspective

Blockchain Powered Federated Systems in Digital Market

Jani Shah*

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

DESCRIPTION

An integrated identity is a consolidated identify that allows users to access several corporate services from a single network. Among the risks and threats are identity theft, centralized management, auditing limits, and lengthy breach investigation processes. This study describes a strategy for developing a blockchain-based, integrated identity system in a marketplace by automating and decentralizing the development and auditing of robust and secure attributes. Those that trade on the open market act as nodes in a distributed blockchain network, which aids in the growth of federated identities.

Members of this network can use a single federated identity to access all of the partner companies' offerings. IoT sensors and wearables can automate this process by logging real-time data, detecting patterns, and highlighting issues. Because every blockchain transaction is totally visible, participants and users can see which services they're accessing and how their identities are being used. To put the proposed architecture to the test, it was implemented on both a permissioned blockchain and a public blockchain.

A requestor can be identified using unique identifiers and granted access to a service or place. Personal data, biometric data, and personal papers are all examples of data that is typically included in this category. Identity theft occurs when someone uses their personal information, such as financial account information, computer information, or physical location information, to gain access to things. Documents, smart cards, and digital identities are just a few examples of digital identities. Governments and corporations are always working to safeguard identities and secure them against loss, fraud, and theft in order to preserve these identities and avert serious harm.

To deliver robust and secure identities while minimizing the potential costs of breaches, new technologies are required. Because they allow users to connect to online services quickly, remotely, and economically, digital identities have become increasingly significant as the usage of the internet and mobile devices has risen. Identity authentication technology is just as authentic as traditional identification, which is provided and approved by an identification source outside of the cloud. People are becoming increasingly anxious about their identities in the digital era. Many people, in particular, are concerned that their identities may be misused, such as through fraud or theft, causing financial and reputational loss.

A federated identity is a single identity constructed with the objective of having access to many service providers' platforms. Users can use a federated identity to access apps from many organizations. There is a potential that the various market segments will separate or merge. The healthcare sector, which includes insurance companies, medical facilities, and hospitals, is a good example of this. Customers can use an integrated identification system to access all of their services with a single identity. Using this identity, Single Sign-On (SSO) might be built for the marketplace.

Future federated systems, on the other hand, should have the technology to do so, as the federated systems that currently enable these marketplaces are incapable of providing access to services and data, let alone monitoring and recording all ongoing transactions. By establishing unbroken chains of evidence, auditing facilities can help strengthen the overall security of organizations in the marketplace. The collective identification of a federated system, like the distributed ID paradigm, faces various issues, including an evaluation of breach security, identity leakage, and centralization. New technologies must be studied in order to aid in the development of a more powerful federated identity system.

Because of its decentralization and security, blockchain technology is an excellent choice for this task. A blockchain, or distributed ledger system, uses encryption to record transactions and other data in an immutable digital format. Smart contracts are computer programs that enable for the implementation of business logic and transactions on the blockchain network. Many modern identity management systems have lately included blockchain technology. Blockchain has been used sparingly in identity management due to its immutability and encrypted transactions.

Correspondence to: Jani Shah, Department of Computer Science and Engineering, Western University, Richmond St, Canada, E-mail: Janishah@yahoo.com

Received: 22-Nov-2023, Manuscript No. IJAR-23-24146; **Editor assigned:** 24-Nov-2023, Pre QC No. IJAR-23-24146 (PQ); **Reviewed:** 08-Dec-2023, QC No. IJAR-23-24146; **Revised:** 15-Dec-2023, Manuscript No. IJAR-23-24146 (R); **Published:** 25-Dec-2023, DOI: 10.35248/2472-114X.23.11.357

Citation: Shah J (2023) Blockchain Powered Federated Systems in Digital Market. Int J Account Res. 11:357.

Copyright: © 2023 Shah J. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.