OPEN ACCESS Freely available online

ISSN: 2472-114X
International Journal of Accounting Research

Commentary

Blockchain-Based Integrated Identification and Auditing Management

Trevor Christie*

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

DESCRIPTION

A consolidated identifier known as an integrated identity enables users to access numerous corporate services from a single network. Identity theft, centralized administration, constraints on auditing, and protracted breach investigation processes are among the risks and threats. By automating and decentralizing the production and auditing of robust and secure qualities, the article describes a method for building a blockchain-based, integrated identification system in a marketplace. Those that deal on the open market serve as nodes in a distributed blockchain network, which helps federated identities grow. Members of this network get access to all of the partner companies' services using a single federated identity. IoT sensors and wearables can do this for you automatically by logging real-time data, finding patterns, and highlighting issues. Because every blockchain transaction is completely transparent, participants can see which services they're using, and users can monitor how their identities are being used. Implementation on a permissioned blockchain and a public blockchain was done to test the suggested architecture [1].

A requestor can be recognized with the help of unique identifiers, allowing them to gain access to a service or location. Personal information, biometric information, and personal papers are all examples of the kind of data that is frequently included in this category. Identity theft happens when someone utilizes our personal information—such as financial account information, information from computers, or information from physical locations—to get access to things we own or use. Digital identities can exist in a variety of forms, including documents, smart cards, and digital identities. Governments and businesses continuously work to protect identities and guard against loss, fraud, and theft in order to maintain these identities and prevent serious harm. New technologies are needed to provide resilient and secure identities while also lowering the potential costs of breaches. Digital identities have become more important as the use of the internet and mobile devices has grown because they enable users to quickly, remotely, and affordably connect with online services. Technology used for identity authentication is just as authentic as traditional identification, which is given and validated by an identification provider outside of the cloud. In the digital age, people are becoming increasingly concerned about their identities. Particularly, many people worry that their identities might be used inappropriately, such as through fraud or theft, which could cause harm to their finances and reputations. The governments of the United States and Canada have released findings that are similar, and research and strategy revealed that identity theft is rising year [2].

It would be nearly hard to create a digital identity management system without significant technological problems. The majority of victims of identity fraud or theft don't receive instant notification of the crime, and it may take those years to realize its full effects. Identity breaches frequently happen to companies that use robust encryption to protect their customers' identities [3].

A federated identity is a single identity created with the goal of gaining access to the platforms of numerous service providers. A federated identity can be used by users to access apps from many companies. There is a chance that the many market sectors will split apart or combine into one. This idea is well illustrated by the healthcare sector, which includes insurance providers, medical facilities, and hospitals. Here, customers can access all of their services with a single identity by using an integrated identification system. Single Sign-on (SSO) could be implemented for the marketplace using this identity. Future federated systems, however, should have technology capable of doing so, as the federated systems that currently support these marketplaces are unable to provide access to services and data, let alone monitor and record all ongoing transactions. Auditing facilities may help increase the general security of businesses in the marketplace by providing unbroken chains of evidence. Similar to the distributed ID paradigm, the collective identification of a federated system faces numerous challenges, including an examination of breach security, identity leakage, and centralization. In order to create a more potent federated identification system, new technologies must be investigated in order to aid with these challenges [4].

Correspondence to: Trevor Christie, Department of Computer Science and Engineering, Western University, Richmond St, Canada, E-mail: christietrevor@gmail.com

Received: 27-Jan-2023, Manuscript No. IJAR-23-20137; **Editor assigned:** 30-Jan-2023, Pre QC No. IJAR-23-20137 (PQ); **Reviewed:** 17-Feb-2023, QC No. IJAR-23-20137; **Revised:** 24-Feb-2023, Manuscript No. IJAR-23-20137 (R); **Published:** 02-Mar-2023, DOI: 10.35248/2472-114X.23.11.311

Citation: Christie T (2023) Blockchain-Based Integrated Identification and Auditing Management. Int J Account Res. 11:311.

Blockchain technology is a fantastic option for this task because to its decentralization and security qualities. A distributed ledger system, also known as a blockchain, leverages cryptography to store transactions and other data in an immutable digital format. Smart contracts are computer programmes that allow business logic and transaction execution on the blockchain network. There are numerous modern identity management systems that have recently included blockchain technology. Because to its immutability and encrypted transactions, blockchain has so far only been used sparingly in identity management [5].

REFERENCES

1. Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, et.al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew Sustain Energy Rev. 2019;100:143-174.
2. Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec. Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) .2016; 25-30.
3. William P, Gupta A, Darwante NK, Gondkar SS, Verma A, Verma V. Applications of Internet of Things in Smart Grid Intelligent Systems. In2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) . 2022; 1175-1179.
4. William P, Shrivastava A, Chauhan H, Nagpal P, Singh P. Framework for Intelligent Smart City Deployment *via* Artificial Intelligence Software Networking. In2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). 2022;455-460.
5. William P, Yogeesh N, Vimala S, Gite P. Blockchain Technology for Data Privacy using Contract Mechanism for 5G Networks. In2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). 2022;461-465.