International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Modeling Identity Management System Based on Blockchain Technology

Manish Verma[a]*

[a]*Scientist D, DMSRDE, Kanpur, India*

A B S T R A C T

An identity management system (IDMS) described to verification and validation for their record of an entity. The framework oversees computerized personalities, which are computerized objects that contain traits utilized for the recognizable proof of people and different substances in an IT framework and for making character claims. The character objects are encoded and cryptographically typified. Personality the executives conventions incorporate the formation of characters, the approval of their authoritative to true substances, what's more, their safe and solid stockpiling, security, distribution, verification, updates, and use..

Keywords: Blockchain, Distributed ledger, Emerging Intelligence based application, identity management and its application, Peer-to-peer network

1. INTRODUCTION

The identity of nearly 1.2 billion people is not known and 1.5 million people identity theft have occurred in past years. We need digital identifier that individuals can own independently like mail Id, mobile number to access Apps and website. We are at mercy of service providers that can block these identifiers. A new type of distributed digital identifier with verifiable credentials is the need of hour. It should be more trustworthy and respect privacy of individual. Therefore, the identity of any individual is very important for their behavioral and financial needs.

The user centric design for digital and real-time verification of identity without revealing the information can be implemented via blockchain technology. While the main adaptation of Blockchain was presented by the Bitcoin convention as a type of "distributed electronic money," the innovation has suggestions a long ways past budgetary exchanges. Honestly, if you have significant data you need to guarantee, Blockchain might be the best approach to guarding it against security perils and ensuring its uprightness.

2. BLOCKCHAIN

The technology of Blockchain was first financially used in the paper on bitcoin crypto-currency implementation by unknown identity person named Sathoshi Nakamoto in 2008 while uploading bitcoin mining software online in 2009, with mining the first bitcoin. Blockchain is a decentralized, dispersed electronic database shared over an open or private system. Each exchange in a Blockchain database are shared among various clients, every one confirming that the database is exact and keeping unapproved exchanges from being finished.

Blockchain is a case of disseminated record innovation, in which autonomous hubs record exchanges and come to agreement about a common state without a concentrated power. The name Blockchain alludes to a specific sort of information structure where each block speaks to a gathering of advanced exchanges and the "chain" alludes to how each block is connected to guarantee that exchanges are recorded in a particular, unalterable request as in figure 1.

* *Corresponding author.* Tel.: 7571094407; fax: +0-000-000-0000.
E-mail address: dmsz11196@gmail.com

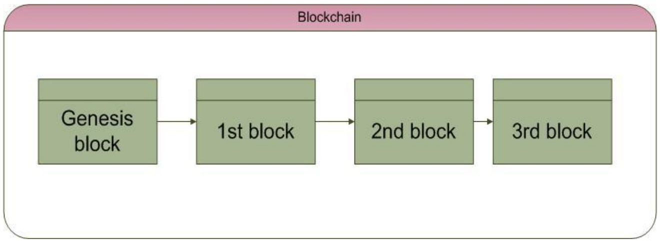

Figure 1: Blockchain architecture with genesis block

A Blockchain "arrange" works as a decentralized database that comprises of a system of PCs or gadgets that go to a concession to a solitary form of a mutual record. In permission less, open Blockchain like Bitcoin, that Blockchain system could comprise of thousands of PCs or gadgets — possibly even millions — working as hubs. In a permission chain, just a couple of believed hubs would work a system between associations.

Each time somebody needs to make an exchange (say, an online buy), an exchange is proposed to the system, which contains the subtleties of the exchange, including what resources changed hands, and a computerized mark of the individual or element directing the exchange. These proposed exchanges are accumulated into deters by the PCs working the Blockchain orchestrate. One PC (or hub) in the framework will be picked to propose a square of exchanges as another development to the record. On the off chance, that the remainder of the hubs concur that this hub is approved to propose a square and the square of exchanges is legitimate, the framework will come to understanding, and the trades in that square will be added to the record.

Besides, each square fuses a cryptographic pointer back to the past square in the Blockchain record, associating the squares together. With each square, another gathering of exchanges is added to the record, and the chain of squares develops ceaselessly in this design.

In any case, here is the place the genuine estimation of this innovation becomes possibly the most important factor. When the squares are affixed, the information in earlier squares cannot be modified or erased by anybody without exhausting an unrealistic measure of registering assets. The structure of Blockchain makes an essentially sealed chain of information. All the while, it makes an unquestionable ordered history of exchanges that anybody inside the Blockchain system can see. You can think once again into the past and see each exchange precisely as it happened.

3. IDENTITY MANAGEMENT SYSTEM BASED ON BLOCKCHAIN

Identity has an issue. On the off chance that it's paper-based, for example, birth declarations sitting inactively in a storm cellar of a town lobby, it is dependent upon misfortune, burglary of extortion. An advanced character diminishes the degree of administration and speeds up forms inside associations by taking into account a more noteworthy interoperability among offices and different establishments. However, on the off chance that this advanced character is put away on a concentrated server, it turns into a honeypot for programmers. Since 2016, in excess of 900 million individual subtleties –, for example, locations or charge card numbers – have been hacked, spilled or penetrated from associations.

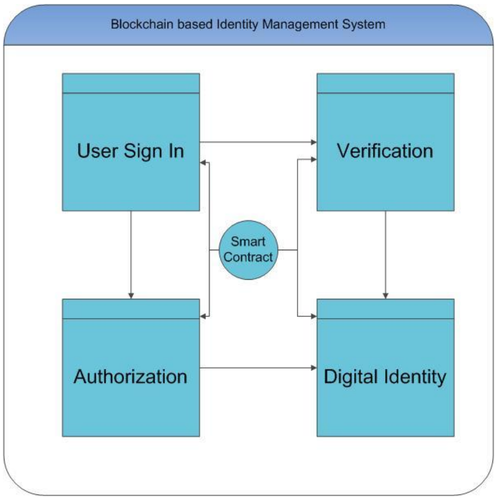

Figure 2: Blockchain based identity management system

A large portion of the current personality the executive's frameworks are feeble and obsolete.

Characters should be convenient and irrefutable all over the place, whenever, and digitization can empower that. However, being advanced is not sufficient. Personalities likewise should be private and secure.

A few enterprises endure the issues of current personality the board frameworks:

– **Government**: The absence of interoperability among offices and government levels incurs significant damage as abundance organization. Which, thus, expands procedures' occasions and expenses.

– **Healthcare**: half of the total populace doesn't approach quality medicinal services. The absence of interoperability between entertainers in the medicinal services space (Hospitals, centers, insurance agencies, specialists, drug stores, and so on) prompts wasteful social insurance and postponed care and disappointment for patients.

– **Education**: It is assessed that 200,000 phony scholarly endorsements are sold every year in the USA alone. The trouble in confirming the legitimacy of these accreditations prompts employing of inadequate experts, brand harm to the colleges and the recruiting organizations.

– **Banking**: the requirement for login subtleties, for example, passwords diminishes the security of banking for clients.

– Businesses when all is said and done: the current need to store customers' and representatives' very own information is a wellspring of risk for organizations. An individual information penetrate may bring about tremendous fines due to GDPR encroachment –, for example, the British Airways case – or just because of client trust misfortune and significant harm to the association's image.

4. CONCLUSION

The Blockchain based model of identity management help in prevention and controlling of fraud as the identity information of individuals cannot be tamper while being auditable with privacy. It could be implementation in any security architecture to improve safety features of system.

Acknowledgements

Author is grateful to Dr. Namburi E. Prasad, Director DMSRDE, Kanpur for permitting this work. The author is thankful to the scientist community of DMSRDE Kanpur for their support in scientific research.

REFERENCES

Bernard, Zoë. "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator." Business Insider. Archived from the original on 15 (2018).

Finley, Klint. "After 10 Years, Bitcoin Has Changed Everything—And Nothing." (2018).

Nakamoto, Satoshi. "Bitcoin whitepaper." URL: https://bitcoin. org/bitcoin. pdf- 17.07. 2019 (2008).

Nakamoto, Satoshi. "Bitcoin v0. 1 released." The Mail Archive 9 (2009).

Dinh, Tien Tuan Anh, et al. "Untangling blockchain: A data processing view of blockchain systems." IEEE Transactions on Knowledge and Data Engineering 30.7 (2018): 1366-1385.

Gupta, Sourav Sen. Blockchain. John Wiley & Sons, Inc, 2017.

Muftic, Sead. "Blockchain identity management system based on public identities ledger." U.S. Patent No. 9,635,000. 25 Apr. 2017.

Jacobovitz, Ori. "Blockchain for identity management." The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva (2016).

Faber, Benedict, et al. "BPDIMS: a blockchain-based personal data and identity management system." Proceedings of the 52nd Hawaii International Conference on System Sciences. 2019.

Lim, Shu Yun, et al. "Blockchain technology the identity management and authentication service disruptor: a survey." International Journal on Advanced Science, Engineering and Information Technology 8.4-2 (2018): 1735-1745.

Liu, Yuan, et al. "An identity management system based on blockchain." 2017 15th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2017.

Dunphy, Paul, and Fabien AP Petitcolas. "A first look at identity management schemes on the blockchain." IEEE Security & Privacy 16.4 (2018): 20-29.

El Haddouti, Samia, and Mohamed Dâfir Ech-Cherif El Kettani. "Analysis of Identity Management Systems Using Blockchain Technology." CommNet. 2019.

Gao, Zhimin, et al. "Blockchain-based identity management with mobile device." Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. 2018.

Nabi, Atif Ghulam. "Comparative study on identity management methods using blockchain." University of Zurich 118 (2017).