NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 6, June. -2021

IDENTITY & ACCESS MANAGEMENT SYSTEM BASED ON BLOCKCHAIN

Ishaq Azhar Mohammed
Sr. Data Scientist & Department of Information Technology, Dubai, UAE
ishaqazhar14@gmail.com

ABSTRACT
This paper discusses the application of identity and access management in Blockchain technology. It is essential in our day-to-day lives that we have effective identity and access management systems. The majority of currently available IAM solutions are centralized, which creates many problems, the most important of which is privacy. The blockchain serves as the foundation of our system, which is by its very nature decentralized and secure [1]. According to our approach, none of the critical identification information about the user is kept on a centralized server; instead, it is stored on the mobile device that has been allocated to that user. This serves two purposes: it protects the user's personal information while also allowing the user to manage his or her identification information. In our increasingly linked and digitalized world, digital identification is becoming more essential. In the case of digital identities, most of us have a number of them, each one connected with a different aspect of our job, our personal life, or another professional activity (ies) [2]. This leads to a rising dependence on identity information management (also known as identity management, identity management and access control, and other terms in the research), which is intended to manage and protect our personal information while also providing appropriate services. Based on blockchain's success, efforts were made to incorporate blockchain into the development of the next wave of identity management systems.

Keywords: Identity and access management, Blockchain, Etherum, cryptocurrency

INTRODUCTION
Revealing our identification is one of the activities that we engage in regularly in our daily lives. The concept Identity and Access Management (IAM) refers to the process by which users get an identity, the process by which a user authenticates themselves using that identity, and the method by which that identity is protected. Our identity and access management solutions have developed over the last several years. From basic usernames and passwords to complex biometrics including the fingerprint and retina [2], there is something for everyone. There is one type of IAM that stands out from the rest: The Self-Sovereign Identity Model [3], which is unique among the different forms of IAM. A paradigm in which the user has complete control over his or her identification and no third party is engaged in the maintenance or restoration of the user's or her identity. The blockchain [3] is the technology that lies at the heart of this approach. Blockchain technology was also used as the foundation for Bitcoin [4]. In computing terms, blockchain is a distributed ledger that is publicly available, which means that anybody may see the ledger and contribute to it. The immutability of the blockchain is one of the most significant characteristics of the technology. That is, once anything is written on this ledger, it can never be deleted or altered. Any illegal modifications made to any block of the chain will also have an impact on the integrity of the whole chain, as previously stated. In recent decades, it has been brought to the public's notice that the problem of Internet security is critical and difficult to resolve. Many people's sensitive personal information is often abused or disclosed, and financial assets are frequently compromised, among other things. These security incidents can directly or indirectly result in economic losses for Internet users, and in certain cases, they may even result in the whole destruction of the Internet transaction environment. As a result, the issue of how to manage one's identity via the Internet becomes a significant issue for both Internet service providers and academic scholars [5]. Many attempts have been made in the search for effective methods to safeguarding the security of personal information. Traditional storage methods for personal data, on the other hand, include a centralized server, which makes it easy for hackers or attackers to accomplish their harmful objectives by stealing, abusing, or altering the data contained on this centralized server [6]. In 2008, Satoshi Nakamoto introduced the idea of Bitcoin [7], which allows individuals to freely trade on the Internet without the need for a reputable or trustworthy third

party to facilitate the transaction. Because of the popularity and rapid growth of Bitcoin, Blockchain, the technology that underpins Bitcoin, has begun to attract the attention of the general public. In other words, Bitcoin heralds the beginning of a new age for Blockchain technology [8], in which it is now feasible to generate and transmit assets on the Internet without the need for a trusted channel [8]. The most important aspect of the Blockchain is its decentralization, which means that all of the nodes in the network are responsible for maintaining the whole database. As long as all of the nodes or a majority of the nodes agree on data generation and change, the mechanism is considered to be in place and effective. This results in the Blockchain exhibiting characteristics such as strong security, difficulty in tampering with, and so on [12]. Because of these characteristics, it has the potential to be an excellent solution for authenticating and safeguarding an identity management system. As a result, users can securely store their personal information in the Blockchain without having to worry about anyone illegally stealing or altering their data, ensuring that their personal information meets the information security requirements of an identity management system [19].

PROBLEM STATEMENT

The main problem that this paper will try to solve is an assessment of how identity and access management works in used in blockchain with particular attention to Ethereum. It is not unexpected that many difficulties exist in the design of blockchain-based identity management systems, given the relatively recent movement in this direction. For example, how can users persuade companies to embrace the characteristics of pseudonymous people with a shaky reputation by presenting them as their own[10] Furthermore, if a transaction is later discovered to be fraudulent or illegal, and the companies involved have not exercised due care in confirming the identities of the individuals engaged, there may be legal and financial ramifications for them.

LITERATURE REVIEW

A. Related Work

Over the years, the use of blockchain technology has been explored in a variety of areas other than cryptocurrency. Identity and access management is an example of an experiment that is noteworthy. Blockchain has the potential to be the catalyst that propels our identification and access management systems towards self-sovereign identity. Some of the more significant works in this field are described in further detail below. It is important to note that a decentralized data management system guarantees that consumers retain ownership and control over their data. Users' data is not maintained by any third parties, which ensures their privacy. In the context of data management, blockchain transactions are utilized to carry out instructions such as saving and accessing data [11]. They also offer the user with fine-grained access control as well as the option to withdraw rights at any time. However, when it comes to data processing, the suggested system does not perform well. A distributed identity and access management system based on blockchain technology for the maintenance of healthcare records [12]. The system is being developed with the help of Hyperledger Fabric. The access to a backend server that contains the patient's health care data is directed via a distributed identity and access management system that is based on the Hyperledger Fabric technology platform. Blockchain may be used to verify an individual's identification and securely communicate the information about that identity. Another benefit of using blockchain is that it makes a system more dispersed, robust to unauthorized intrusions, and tamper-proof. His suggested model is based on a blockchain ID that can be confirmed by any third party and contains certain information about the person, as well as other features. A secured app, which allows users to sign documents and authenticate themselves, is used by him in the implementation of his solution [12]. Interestingly, the use of signatures and hashes is used to provide just the information necessary for identification. A key distribution system called BIBE [9] that combines identity-based encryption with blockchain technology is being developed. The goal of this strategy was to reduce the number of KGC unauthorized intrusions. They claim that the Key Generation Center was created on the blockchain with the assistance of several nodes, particularly three. Additionally, the responsibilities of nodes are rotated regularly to minimize the impact of any assault. In addition, timestamps, random numbers, and hash algorithms are integrated into their architecture to minimize the likelihood of network unauthorized intrusions [13].

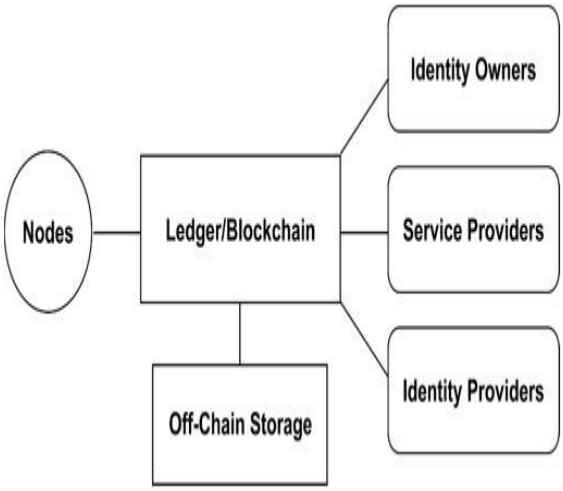

Fig i: Components of Block chain

B. The Fundamental Concepts

To fully comprehend our topic, we must first have a fundamental knowledge of a few ideas. This section provides a high-level overview of the fundamental ideas that are necessary for comprehending our model.

1. Blockchain

Satoshi Nakomoto is the creator of blockchain technology. It was first created in 2001 as the core platform behind Bitcoin. Blockchain is a digital ledger that contains data that has been timestamped and is thus incorruptible. No one body is in charge of maintaining it; instead, it is a collection of nodes that make up the network. Blockchain is made up of a series of data blocks that are linked together. Each block contains a record of the hash of the preceding block, as well as its hash, making it very impossible to alter this ledger in the future. If someone attempts to maliciously alter the contents of a block, the whole chain will lose its integrity and will no longer be deemed legitimate, according to the rules [13,14]. This is because each block contains the hash of the preceding block. It is necessary to get the approval of more than 50% of the nodes in the network to add a new block to the blockchain. This is accomplished via the use of a consensus algorithm [14]. Several different consensus methods may be employed, with proof-of-work being the most commonly used. Ethereum, Hyperledger Fabric, and IBM Blockchain are just a few of the blockchain systems that are now accessible.

2. Hashing

Hashing is essentially the process of deriving a value from an unstructured string or piece of text. In its most basic form, a hashing function accepts an input string of arbitrary length and produces an output string of a predetermined size. In an ideal situation, the output string should be distinct from the input string, which means that no other text should generate the same hash. Data is protected against manipulation via the use of hashing [14]. Any minor modification to the data will result in a significant change in the hash value. Specifically, cryptographic hash functions are a subset of hash functions that have certain unique characteristics that make them particularly well suited for use in the area of cryptography. Hashing is used in blockchain technology to guarantee that the chain is untampered with. Every block contains both the hash of the preceding block and its hash. As the root of the Merkle tree, each block contains a hash that is unique to it [15].

3. Proof-of-Work

When a block is added to the blockchain, consensus algorithms are employed to achieve consensus. Proof-of-Work (PoW) is the consensus algorithm that is most frequently employed. Proof-of-work is used by both Ethereum [15, 116] and Bitcoin, with notable variations in how they are implemented. This method grants the privilege of adding a new block to the chain to a node that is the first to answer a difficult mathematical problem in a short period. It is the miners that compete with one another to solve this difficult issue, which is

why they are termed nodes in the chain. The workload is considered a safety net by PoW. The blockchain can only be compromised if someone has access to more than 50% of the processing power available across all nodes in the network.

4. Smart Contracts

Smart contracts are nothing more than a piece of code that is self-executing, self-verifying, and tamper-resistant, and they are becoming more popular. To carry out certain activities, smart contracts will include logic, and once they are put on the blockchain, no one will be able to alter the nature of the operations [16]. A smart contract that has the logic to give cinema tickets when a specific amount of money is paid, for example, maybe created and implemented on the blockchain, making it impossible for anybody to get a movie ticket without first paying for it. Important to note is that you do not need the assistance of a central authority to ensure that you have paid the required amount of money and that you will get movie tickets if you have made the appropriate payment. The characteristics of blockchain and smart contracts are combined to accomplish this elimination of the need for a third-party intermediary. A unique address will be linked with each smart contract that is put on the blockchain, which will allow anybody to activate the contract. Solidity is the programming language that smart contracts are created in the most often.

5. The Concept of Self-Sovereign Identity

This is a concept that essentially says that the user must own their identity and be fully controlled. In contrast to the traditional identity model, the self-sovereign identity model does not rely on third-party servers to store the user's passwords or other sensitive identification information. One of the most significant benefits of this single modification is the security of the user's personal information, which is the most essential benefit of all. This is because identification information is no longer centralized, and the user is now in complete control of his or her information. Now it is up to the user to decide what should be done with his information. Moreover, it substantially minimizes the impact of assaults carried out by a hostile user to steal user credentials. It is also possible to eliminate the operating and maintenance costs associated with a centralized server [116,17].

C. Architecture

Blockchain applications are increasingly being developed on Ethereum, which was the first framework that offers Turing complete smart contracts. Ethereum is now one of the most popular blockchain applications. As a result, we'll utilize Ethereum to demonstrate the blockchain configurations. The database system is the bedrock upon which all other services, such as data storage and security assurance, are built [17]. Data storage is accomplished via blocks and chains. To guarantee data durability, the Merkle tree is used. The security guarantee is based on the data layer's hash function, digital certificates, and other cryptographic technologies, which together ensure the account and transaction's security. The Elliptic Curve Digital Signature Algorithm (ECDSA) signature technique and the SHA3 hash function are used to generate the core certificate and hash value. When it comes to networking, a peer-to-peer (P2P) system is used to implement this layer [17]. In peer-to-peer networking, there is no central system, so each user is a node that may perform server-related functions. This layer incorporates the concepts of decentralization and network resilience. The consensus layer is committed to ensuring that nodes in the network agree on records and information, and it is comprised of two consensus methods. To promote the fast discovery of ethers (ETHs), the proof of work (PoW) consensus method is implemented in the beginning to ensure that there are enough ETHs available. When the total number of ETHs reaches a critical mass, the proof of stake (PoS) method will be used to verify transactions. One such strategy may successfully prevent the incomplete distribution of a single node in the network. The incentive layer is in charge of the creation and deployment of Ethereum tokens (ETHs) [17,18]. ETHs may be used to pay for maintenance, execute digital signatures, and for other purposes. They are generated via mining, with a credit of a few ETHs for each block mined. In the smart contract layer, the operating smart contract must be supported by a corresponding virtual machine, such as the Ethereum virtual machine (EVM) in the case of Ethereum, which is used to manage the underpinning smart contract. While at the same time, the decentralized application (DAPP) includes an interactive interface, which makes it easier for users to engage with smart contracts [18].

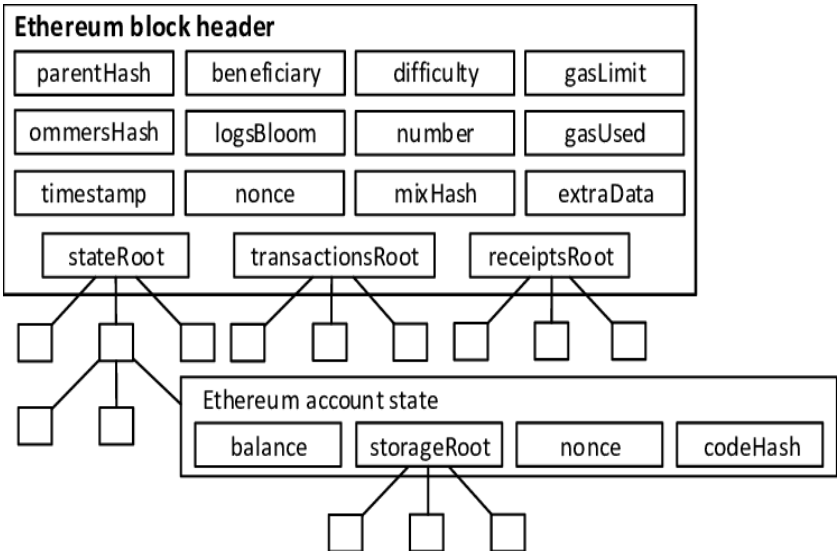

Fig i: Structure of Ethereum

ITS FUTURE

Blockchain technology offers a wide range of potential applications in a wide range of sectors. A variety of applications, including identity management, smart contracts, supply chain analysis, and more, are already being implemented on the blockchain. Probably, the full potential of blockchain technology will not be realized for some time. What is questionable, however, is the role that cryptocurrencies will play in the future. Electronic money has become a thing of the past, with services such as Venmo, Zelle, and digital wallets becoming commonplace [19]. Indeed, bitcoin has seen a Gold Rush-like craze during the past five years, with the top 10 cryptocurrencies all having market capitalizations in the billions of dollars or more. In the United States, there are hundreds of Bitcoin ATMs and Coin Kiosks, and businesses such as Microsoft, Subway, and Overstock currently accept payments in digital currencies, according to the Bitcoin Foundation [19]. In the future, business models that are enabled by blockchain technology will represent a sea change in the way that company is done. Due to the growing digital nature of the international economy and the decentralization of business strategies and stakeholders allowed by blockchain, the technology's effect on business will be game-changing. A new level of invention is waiting to be discovered in this approach. The following are some instances of disruptors who are ahead of the curve [19].

ECONOMIC BENEFITS TO THE U.S

In the United States, blockchain has progressed well beyond its origins in banking and cryptocurrencies. Although Bitcoin's popularity helped show the potential of blockchain technology in the financial sector, entrepreneurs have come to think that the technology has the potential to revolutionize a wide range of sectors. The applications for a transparent and verifiable record of transaction data are almost limitless — particularly considering that blockchains function on a decentralized platform that does not need central supervision, making them highly resistant to fraud [19]. Blockchain and finance are just the beginning of what is possible. Banks, when seen from a macroeconomic viewpoint, function as important value storage and transmission hubs. With the ability to perform the same purpose as traditional ledgers while being digitalized, secure, and tamper-proof, blockchains have the potential to significantly improve accuracy and information exchange in the financial services ecosystem. Credit Suisse, for example, has formed a partnership with New York-based startup Paxos to utilize blockchain technology to settle US stock transactions beginning in March 2020, according to the company. Meanwhile, JPMorgan Chase has launched the JPM Coin, which it plans to use to simplify transactions between institutional accounts [19]. The JPM Coin is the bank's first foray into the blockchain sector. Other institutions, such as Goldman Sachs and Citigroup, have also conducted blockchain trials. The incumbents completed an equity exchange using Axoni's Axcore blockchain, which was developed by Axoni. To improve the efficiency of cross-border payments, blockchain startup Ripple has formed partnerships with over 300 clients, including financial firms

such as Santander and Western Union. Its current solution offers banks a two-way communication protocol that allows them to send and receive messages in real-time, as well as settle transactions in real-time [19].

CONCLUSION

This research addresses the application of identity and access management in blockchain technology, with a special emphasis on the Ethereum blockchain. The findings from this analysis show that Identity management systems are typically intended to ease the administration of digital identities and activities such as authentication, according to this study. Blockchain is cryptography by its very nature, and this is what distinguishes it from other technologies. This enables both parties to ensure that the other entity is genuine and to validate that the data provided is essential. We utilize the web3js module to create signatures and verify them. Cryptocurrency network security systems have been proposed recently, allowing users to take responsibility for their own identities (i.e. self-sovereign identity). This study also showed that the technological benefits of the blockchain make the data in the system secure and trustworthy. Smart contracts are used to establish system rules that guarantee user data is reliable.

REFERENCES

1) D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," CoRR, 2015. [Online]. Available: http://arxiv.org/abs/1508.04868
2) P. F. Costa, "Ethereum blockchain as a decentralized and autonomous key server: storing and extracting public keys through smart contracts," Ph.D. dissertation, University of Bologna, 2017. [Online]. Available: http://amslaurea.unibo.it/14306/
3) S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F.Ang, and R. Ismail, "Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey," International Journal
4) on Advanced Science, Engineering and Information Technology, vol. 8, no. 4-2, pp. 1735–1745, 2018.
5) O. Jacobovitz, "Blockchain for Identity Management," Ben-Gurion University, Beer Sheva, Israel, Tech. Rep., 2016. [Online]. Available: https://www.cs.bgu.ac.il/ frankel/TechnicalReports/2016/16-02.pdf
6) Z. W.-O. Danny Yang, Jack Gavigan, "Survey of confidentiality and privacy preserving technologies for blockchains,"R3 Research, Tech. Rep., 2016. [Online]. Available: https://z.cash/static/R3 Confidentiality and Privacy Report.pdf
7) A. Muhle, A. Gruner, T. Gayvoronskaya, and C. Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," 2018.
8) Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," 2018.
9) M. Ahmed and K. Kostiainen, "Identity Aging: Efficient Blockchain Consensus," 2018.
10) P. Dunphy, L. Garratt, and F. Petitcolas, "Decentralizing Digital Identity: Open Challenges for Distributed Ledgers," –, 2018.
11) P. Dunphy and F. A. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," IEEE Security & Privacy, vol. 16, no. 4, p. 20–29, Jul 2018. [Online]. Available: http://dx.doi.org/10.1109/MSP.2018.3111247
12) D. Augot, H. Chabanne, O. Clemot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the Bitcoin blockchain," CoRR, vol. abs/1710.02951, 2017. [Online]. Available: http://arxiv.org/abs/1710.02951
13) D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, "A User-Centric System for Verified Identities on the Bitcoin Blockchain," CoRR, vol. abs/1710.02019, 2017. [Online]. Available: http://arxiv.org/abs/1710.02019
14) M. Schanzenbach, G. Bramm, and J. Schutte, "reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption," CoRR, vol. abs/1805.06253, 2018. [Online]. Available: http://arxiv.org/abs/1805.06253
15) A. Othman and J. Callahan, "The Horcrux Protocol:A Method for Decentralized Biometric-based Self-sovereign Identity," CoRR, vol. abs/1711.07127, 2017. [Online]. Available: http://arxiv.org/abs/1711.07127

16) U. Der, S. Jahnichen, and J. Surmeli, "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution," CoRR, vol. abs/1712.01767, 2017. [Online]. Available: http://arxiv.org/abs/1712.01767
17) 20[60] F. Guggenmos, J. Lockl, A. Rieger, and G. Fridgen, "Challenges and Opportunities of Blockchain-based Platformization of Digital Identities in the Public Sector (Research in Progress)," in., 06 2018.
18) M. Al-Bassam, "SCPKI: A smart contract-based PKI and identitysystem," in Proceedings of the ACM Workshop on Blockchain, Cryp-tocurrencies and Contracts. ACM, 2017, pp. 35–40.
19) D. Baars, "Towards Self-Sovereign Identity using Blockchain Technol-ogy," Master's thesis, University of Twente, 2016.
20) H. Shrobe, D. L. Shrier, and A. Pentland, New Solutions for Cyberse-curity. MIT Press, 2018.