International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

BLOCKCHAIN BASED PERSONAL IDENTITY SECURITY SYSTEM

Bilali Kalyani[1], Komarasani Hemavathi[2], Siddavatam Ashok Kumar Reddy[3], Tirumala Lakshmi[4], B.Javeed Basha[5]

[5]Guide
Department Of Cse
Tadipatri Engineering College,
Tadipatri.

Abstract:
Identity theft is the unauthorized acquisition of another person's confidential information in order to misuse it. Organizations and individuals should exercise caution when it comes to protecting their identities in order to avoid fraud as a result of identity theft. This information is freely available to attackers in user profiles. Attackers use this information to obtain additional information without raising suspicions about a final attack, identity theft, or fraud. Our block chain based Personal Identity Security System assists in securely storing personal identity data without fear of it being compromised or lost. In this system, the admin can access all the users and verify those accounts. The admin has access to all of the user's documents that have been uploaded to the system. They can view all of the user's activity logs. The admin can view the status and see if any fabrication is taking place. The admin can view the user's complaints. The user can view if logs have been updated or deleted, as well as the status of fabricated document details. If a user discovers a fabrication or an action that they did not perform, they can notify the admin. The user can view all of the details by scanning the QR Code. They can add and verify all the documents with the ledger.

Keyword: Block Chain, Personal, Identity, Security, System, Cryptographic, SHA, AES.

I.INTRODUCTION

Block chain is a decentralized storage device in which records is stored in a series of blocks related with the aid of cryptographic hashing of previous blocks. This undertaking includes HTML, CSS and JavaScript at the front end and ASP.NET on the lower back end. The IDE is Visual Studio and MSSQL Database. Our price-based identification protection system facilitates you securely keep your for my part identifiable data. In this case, the administrator can pick out all users and verify their debts. The administrator has get admission to all user documents uploaded to the gadget. Everything can be carried out by the user. The administrator can view the fame and see if any mistakes have passed off. You can view administrator complaints. To liberate, the user should first sign in; after the administrator has confirmed the account, he or she will be able to unlock the account using the consumer's password. User can replace the profile as according to requirement. Users can control their files by way of adding, adding and deleting them. All documents submitted through the consumer are demonstrated through the administrator. User can test the fame of QR code and product documents.

II.RELATED WORK

A digital identification control device is a key a part of the safety infrastructure for web packages. However, current virtual identification management structures gift various demanding situations, along with move-area authentication and interoperability, trust less ness in identity authentication, and weaknesses in identity statistics safety. Although the development of digital identification gear and blockchain-based structures has

attracted attention inside the field of blockchain technology, these systems do no longer completely deal with the above-cited troubles. To deal with these issues and broaden a relaxed and trustworthy virtual identity device, this paper proposes an powerful research version that integrates identity, oracle technology, and self-carrier blockchain. The purpose of this model is to provide solutions, lay the muse to triumph over the challenges, and create a reliable and secure virtual identity machine [1].

In this contemporary era, with everything evolving and development achieving new heights, the wide variety of frauds and scams is increasing. That is why we ought to be greater cautious now than ever. Today, whether we want to open a bank account or use a monetary app, we first need to do an e-KYC verification. But the trouble is that this e-KYC verification is required in many locations, and we need to do it a couple of times. This article indicates how this hassle may be solved the use of a blockchain-primarily based e-KYC (digital Know Your Customer) system. It may be a unique answer for e-KYC, in which people most effective need to do KYC as soon as after which they are able to use it in multiple establishments. Thanks to blockchain technology, our device may be obvious, decentralized, efficient and cozy. Users can select who to offer electronic KYC facts to, and can send all of the data or popularity facts inside a 2nd. The aim of the e-KYC system is to create a more at ease and comprehensive digital environment that doesn't benefit all people inside the United States of America [2].

A digital identity represents any external entity, be it someone, commercial enterprise, account, or item, and is the idea for having access to computer offerings and personal interactions. Despite years of research, the query of reliable Internet connectivity for virtual identities stays unresolved. In this paper, we propose a blockchain-primarily based solution for digital identities in situations of mutual mistrust. Unlike contemporary identity management structures that rely upon centralized storage, our thought is a blockchain-based totally self-service identity (SSI) platform wherein the actual identification of the client/user is saved in their personal net software the use of decentralized garage. Identity facts is validated the usage of the 0-information evidence (ZKP) method furnished by means of SSI-based totally systems, which ensures privacy and protection. The technique proposed on this paper acts as a digital identity wallet that allows customers to affirm their identity the usage of blockchain and SSI-based access technology, resulting in a decentralized, demonstrated ZKP and immutable identification. By addressing the statistics immutability, traceability, and crucial control troubles associated with traditional identity systems, the proposed approach offers a legitimate and public model of authenticated statistics that can be confirmed by using outside sources. Various implementations of file era and validation are offered under the subsequent implementation demonstration [3].

When it involves virtual identities, privateness and safety are most important concerns, especially in centralized structures wherein information can be without difficulty stolen or humans can engage in identity fraud. Blockchain technology can assist cope with these problems, as it allows decentralized virtual identities to be applied in a cozy and verifiable way. This take a look at uses the Kaggle dataset to compare record transactions and associated devices, comparing how blockchain can enhance privacy and protection. Essentially, various device gaining knowledge of algorithms are used to investigate blockchain packages, and the consequences display that blockchain systems drastically increase transaction accept as true with and reduce fraudulent sports. Therefore, the study argues that an identification management system primarily based on blockchain overcomes the shortcomings of a centralized version via improving information possession and fraud prevention. Further evaluation has broadened the discussion of scalability, interoperability, and the evolution of utility algorithms for blockchain, and it'll fundamentally trade how a few industries, mainly identity management, which might be on the heart of relied on answers and cozy blockchain [4], work with their clients.

Personal authentication is a crucial a part of statistics security principle. A not unusual hassle occurs when a username and password are sent in clear textual content over the community and then returned to an authenticated character. The security is susceptible and it's miles liable to brute force and dictionary assaults. Although dynamic password authentication is very at ease, if there may be a problem at some point of synchronization between the server and the client, the person will no longer be able to log in for a long time. Furthermore, a dynamic password remains unchanged for a positive period of time and might additionally be liable to replay assaults. Therefore, a decentralized blockchain-based totally dynamic identification authentication device isn't always proposed. By the usage of a public key + nonce (an integer growing from zero) to open, it now not only solves the trouble of centralized identification authentication, however also solves replay attacks. Improved safety of the identity authentication process [5].

Identity documents (IDs) are situation to various forms of theft and hacking. Government groups, banks, and credit institutions are susceptible factors in a current identification system. The modern centralized gadget is neither reliable nor at ease. Identity must be supplied using a couple of authorities-approved identifiers at every degree. The not unusual use of a couple of identifiers increases privacy and records confidentiality troubles. We endorse a blockchain technique to comfortable pinnacle-level identity via a decentralized network, which gives privacy where identity files are relaxed, authenticated, and most effective authenticated members can get right of entry to the documents. The proposed answer incorporates a brand new safety architecture and addresses security vulnerabilities bobbing up from the usage of advanced communique technology - steganography and cryptographic technologies [6].

In today's healthcare system, traditional centralized identity management infrastructures are facing demanding situations that jeopardize the security and privacy of patient statistics. The foremost issue is the vulnerability of those centralized structures, which creates the danger of records leakage, unauthorized get right of entry to, and tampering with sensitive scientific information. This poses a threat to the privateness of sufferers and the general integrity of scientific information. Having recognized these flaws, research has been carried out to develop a decentralized identification management solution to triumph over the generation barriers. By removing the want for dispensed ledgers to manipulate identification and immutability, the proposed technique pursuits to get rid of unmarried points of failure and the dangers associated with unauthorized access to records. The innovation of the proposed solution is the convergence trend. This paradigm shift guarantees that affected person facts is relaxed, unaltered, and reachable most effective to authorized people. Unlike traditional structures, the proposed decentralized method offers patients with the capability to use cryptographic keys to control their identities [7].

Recently, because the areas wherein private information is used are numerous, digital identity and safety solutions are being furnished with the improvement of the virtual ecosystem. However, the hassle of private data disclosure arises from the usage of malicious code and software with susceptible security. With the misuse of touchy information including scientific statistics and the economic loss due to unauthorized theft of private records, the ownership and management of your personal information is a critical difficulty. The consciousness is on technologies which can clear up this problem. This article explains the history and shortcomings of present identification authentication structures used in agencies and businesses, and also explains the self-signed identification certificate proposed to conquer them. Next, we present a decentralized model designed to guard non-public information, shop identity and fitness facts on non-public devices, and deploy IPFS with a structure appropriate for blockchain use [8].

This examine examines the implementation of blockchain-primarily based identity management within the Republic of Indonesia and analyses its impact on privateness and safety risks. The methodology selected for this have a look at is a qualitative have a look at the usage of an exploratory methodology. This study proposes six research proposals and an architectural framework for citizen identification control. This have a look at

shows that privateness and protection risks can be decreased if implemented via the Ministry of Home Affairs of the Republic of Indonesia [9]. An identity management system (IDMS) is how customers or people are recognized and authorized to apply a company's systems and services. Although traditional identification management and authentication systems rely heavily on a trusted imperative authority, they cannot mitigate the impact of a unmarried point of failure. As a decentralized and distributed public leader in peer-to-peer (P2P) networking, blockchain (BC) era has attracted tons attention inside the IDMS industry in current years. With self-furnished identities (SSI), users can gain complete manage over their virtual identities. The success implementation of BC-based IDMS will notably enhance the privacy and safety of SSI from the user attitude. However, the combination of BC-based IMDS to offer consumer-pleasant SSI stays an unexplored vicinity of research within the early ranges of development. This paper gives a complete literature overview of modern educational guides and industrial marketplace proposals regarding the applicability of BC-primarily based SSI answers. The early complete development of closed-loop technologies hinders the improvement of a progressive course for IDMS answers [10].

III.EXISTING SYSTEM

An identification control device (IDMS) refers to how customers or individuals are recognized and licensed to use organizational structures and offerings. Because conventional identity control and authentication structures rely heavily on a depended on relevant authority, they cannot mitigate the consequences of individual failure. As a decentralized and allotted public peer-to-peer (P2P) community, block chain (BC) era has attracted full-size attention in the IDMS industry in current years. With Supreme Self Identity (SSI), users can have complete control over their digital identification. Successful implementation of BC-based totally IDMS will considerably improve the privacy and safety of user's SSI. However, integrating BC-based totally IMDS to supply SSI to the user is an area of research that is still within the early levels of development. This article provides a comprehensive review of the current clinical literature and commercial market offerings at the applicability of BC-based totally SSI answers. It additionally offers distinctive introductory records on constructing block technologies and modern roadmap for developing ITMS answers. To offer an effective BC-primarily based IDMS solution for SSI person security, this newsletter describes the 5 key components of a BC-based totally IDMS: authentication, integrity, confidentiality, trust, and simplicity. Furthermore, we conduct a protection analysis that identifies a selection of antagonistic threats that may doubtlessly harm BC-based totally IDMS. Identify and speak related problems and demanding situations by using reviewing several main BC-primarily based IDMS solutions in the medical literature. We additionally highlight ability studies gaps and provide possibilities for destiny research. The disadvantages of the existing system are:

- Time of consumption.
- Low safety.
- Server troubles occur regularly.

REQUIREMENT ANALYSIS

Evaluation of the Rationale and Feasibility of the Proposed System

The fundamental objective of the decentralized device is to guard the non-public records and private facts of each person and drastically reduce fraudulent activities.

IV.PROPOSED SYSTEM

In this case, the administrator can pick out all users and confirm their debts. The administrator has get admission to all person documents uploaded to the gadget. Everything may be finished through the person. The administrator can view the fame and notice if any mistakes have occurred. You can view administrator proceedings.

To free up, the person need to first sign up; after the administrator has confirmed the account, he or she will liberate the account the usage of the person's password. User can replace the profile as according to requirement. Users can control their files by way of adding, adding and deleting them. All documents

uploaded by the person might be managed via the administrator. User can take a look at the fame of QR code and product documents.
User can take a look at whether or not facts have been up to date or deleted and what are the info of the document. If the person reveals any hassle or any movement which he has no longer completed, he can inform the administrator. By scanning the QR code the consumer can see all of the statistics. Add all documents the usage of the registry and click on. The advantages of the proposed system are:

- Rest
- Higher than Ever.
- Always Active.
- Known Problems with the Server

BLOCK DIAGRAM

The safe administration of user identities and documents is guaranteed by the blockchain-based decentralized identity security system. Users register their profiles and upload documents, which administrators oversee and verify. A safe, unchangeable record of all actions, including uploads, updates, and deletions, is offered by blockchain technology. By enabling users to monitor the status and specifics of their documents, QR codes protect confidentiality and openness.

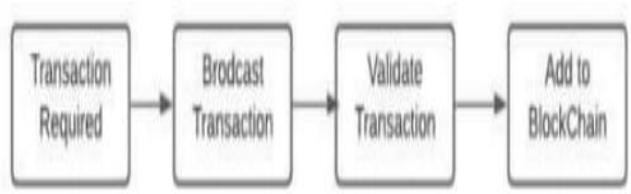

Fig 1: Figure of Block Diagram

ARCHITECTURE DIAGRAM

A description of the general capabilities of this system is associated with the definition Establish excessive-stage machine requirements. Thru architecture Design, various websites and their relationships are diagnosed The key areas of the undertaking to be designated are diagnosed and damaged down Process modules and conceptual data structures, as well as relationships Found among blocks. The following techniques are listed A system is proposed.

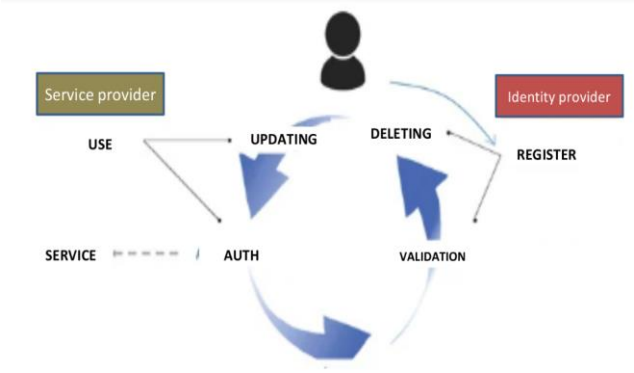

Fig 2: Figure of System Architecture

DATA FLOW

A DFD is also known as a bubble chart. It is a simple graphical illustration of a system in phrases of enter data, the numerous strategies it plays on that statistics, and the output statistics generated with the aid of the device. A facts flow diagram (DFD) is one of the principal modelling gear. It is used for modelling computer components. These additives are organizational methods, records used in the tactics, external entities associated with the employer, and statistics flowing within the business enterprise. A DFD shows how

information actions thru a machine and how it changes via continuous trade. It is a photo artwork that depicts the flow of information and the alterations it makes use of to switch records from enter to output. A DFD is likewise referred to as a bubble chart. A DFD can represent a device at any stage. A DFD may be divided into layers that beautify statistics glide and characteristic.

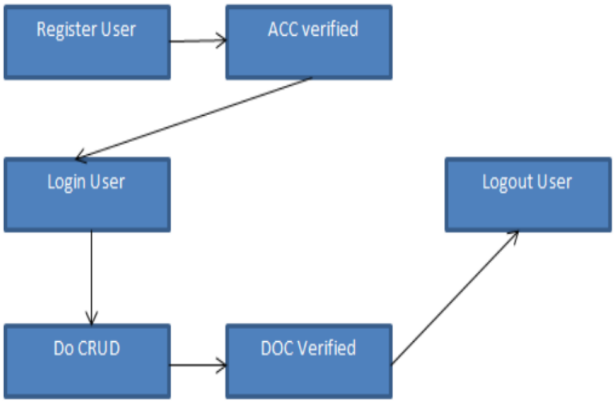

Fig 3: Figure of Data Flow Diagram

V.SYSTEM MODULES

- Admin Module.
- User Module.
- Volume Crude.
- Batch Documentation.

Admin Module.

In this module, administrator maintains all his account information and all the records specified in his necessities, administrator manages all the users collectively. The administrator will see whether the user has been introduced or now not, and some humans may additionally put together a document for the administrator to approve. And verification of all performance requirements and verification of blocks using a series of blocks.

User Module.

In this module, customers are subjected to authentication and security to get admission to the info supplied in the ontology gadget. Before accessing or querying records, a user should have an account, otherwise they need to first sign up. At a minimum, you'll want to offer an e mail cope with, username, password, show name, and any other fields you decide as wanted. Display call is used whilst the gadget call refers back to the consumer's very own requirement.

Volume Crude

Full shape identification CRUD for method, part, delete and install. Here you may perform all operations and specify your account data effectively.

Batch Documentation

User can test whether or not documents had been updated or deleted and document of particular file document. If a person sees something faux or ridiculous that now not works, they are able to file it to an administrator. By scanning the QR code the consumer can see all the records. In addition to all documents, you could also view bills.

SELECTED METHODODLOGIES

Blockchain is a shared, unchangeable ledger that makes it easier to track assets and record transactions throughout a corporate network. An asset might be intangible (such as intellectual property, patents, copyrights, and brand images) or tangible (such as a home, car, money, or land). On a blockchain community, anything of value may be tracked and sold, lowering risk and costs for all parties. Information is the foundation of business. The higher the speed and accuracy of the records. Blockchain is ideal for providing these statistics

because it provides instantaneous, shareable, and verifiable data that is kept in an unchangeable ledger that only authorized members of the community may access. A blockchain community can adjust production, invoicing, payments, orders, and more. Additionally, because all contributors have the same perspective, you can observe every aspect of a transaction from beginning to end, giving you more self- assurance as well as new skills and opportunities.

A decentralized database or ledger that is shared by all nodes in a laptop community is called a blockchain. They are well-known for playing a crucial part in cryptocurrency architecture to keep a loose and dispersed record of transactions, but they are no longer limited to using cryptocurrencies. Any field can employ block chains to make data immutable, which is a word that refers to the impossibility to exchange facts. Since a block cannot be controlled, it is seen to be the most efficient place for a person or piece of software to submit data. This feature lessens the need for 0.33 events, which are usually auditors or other individuals who make mistakes and increase prices. With the development of several cryptocurrencies, decentralized finance (DeFi) applications, non-fungible tokens (NFTs), and smart contracts, the use of blockchain technology has increased dramatically since the launch of Bitcoin in 2009.

SHA – SECURE HASH ALGORITHM.

Secure hashing algorithms, additionally known as SHA, are a circle of relatives of cryptographic features designed to securely arrange information. It works with the aid of transforming data the usage of a subtraction function: an algorithm such as bitwise operations, modular additions, and summation operations.

AES – ADVANCED ENCRYPTION STANDARD

The AES encryption algorithm (also known as the Reyndahl algorithm) is a symmetric block encryption algorithm with a block/chew size of 128 bits. It converts those character blocks using keys of length 128, 192 and 256 bits.

VI.RESULT AND DISCUSSION

The machine correctly generates a unique digital identifier for every user securely combine them with private statistics. These were virtual identifiers these are stored on a distributed shelf to ensure transparency and immutability. The gadget offers consensus the usage of cryptographic strategies and algorithms security of private facts elevated. Decentralization of generation limits person factors of failure; by reducing access threat or fear of leakage. Users can now keep and hold your non-public data extra at ease. I am approximately to get out of here. Block chain-based non-public information security system lets in users to stay secure Share the unique functions of your virtual identification quantity and what you need to get again detailed documentation of work and verification of the optimization manner. Conventional the verification manner frequently entails time-eating office work Submission and guide methods.

VII.CONCLUSION

In conclusion, block chain-based totally identification protection systems enhance the security and privacy of personal facts and prevent identity theft and fraud. However, challenges nonetheless stay to be conquer, together with the want for big statistics units and ensuring compatibility with existing systems. It is likewise important to make certain transparency and responsibility in these systems to growth person self-belief. Further studies and development is needed to increase the capacity skills of these systems. Despite the challenges, block chain-based totally identity safety systems offer extensive capability advantages, supporting to create a safer and more accountable digital society and giving human beings more manipulate over their non-public identification. Further studies and improvement is needed to maximise those blessings, inclusive of exploring more advanced contracts, integrating other kinds of facts, and making sure transparency and duty in management structures. Overall, using block chain-based privateness systems can considerably improve the manner non-public records is treated and protected. By helping to create a more at ease and responsible

virtual society, block chain-primarily based systems assist save you losses from identity theft and fraud, at the same time as giving humans extra manage over their non-public identities. Therefore, it is crucial to maintain studies and improvement in this area and enforce those structures in a green and moral manner.

REFERENCES:

[1] S. Srivastava, D. Agarwal and B. Chaurasia, "Secure Decentralized Identity Management using Blockchain," 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom, 2023, pp. 1355-1360, doi: 10.1109/TrustCom60117.2023.00185.

[2] S. Karmoker et al., "Decentralized e-KYC System for Secure Identity Verification in Bangladesh," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-6, doi: 10.1109/ICBDS61829.2024.10837368

[3] A. R. Raipurkar, S. Bobde, A. Tripahi and M. Sahu, "Digital Identity System Using Blockchain-based Self Sovereign Identity & Zero Knowledge Proof," 2023 OITS International Conference on Information Technology (OCIT), Raipur, India, 2023, pp. 611-616, doi: 10.1109/OCIT59427.2023.10430981.

[4] S. Saranya, Monika, K. Manikandan, J. Nagaraju, S. Nagendiran and B. T. Geetha, "Blockchain-Based Identity Management: Enhancing Privacy and Security in Digital Identity System," 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), Greater Noida, India, 2024, pp. 1620-1625, doi: 10.1109/IC3I61595.2024.10829044.

[5] J. Zhu, Y. Wei and X. Shang, "Decentralized Dynamic Identity Authentication System Based on Blockchain," 2021 International Conference on Networking Systems of AI (INSAI), Shanghai, China, 2021, pp. 1-4, doi: 10.1109/INSAI54028.2021.00012.

[6] P. Rede, S. Iyer, S. Sharma and S. Deshmukh, "Blockchain Based Identity Management System Using Cryptography and Steganography," 2023 International Conference on Information Technology (ICIT), Amman, Jordan, 2023, pp. 173-177, doi: 10.1109/ICIT58056.2023.10225957.

[7] P. V. M, S. N. Qurashi, F. Sobia, F. Harahsheh, S. Surendran and S. S. C. Mary, "Decentralized Identity Management Using Blockchain for Healthcare Systems," 2024 IEEE Silchar Subsection Conference (SILCON 2024), Agartala, India, 2024, pp. 1-6, doi: 10.1109/SILCON63976.2024.10910771.

[8] J. Bang and M. -J. Choi, "Design of Personal Data Protection Decentralized Model Using Blockchain and IPFS," 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), Sejong, Korea, Republic of, 2023, pp. 251-254.

[9] O. H. Padmanegara, R. K. Putri, R. Yuliani and E. K. Masli, "Blockchain and The Public Sector: Blockchain-Based Identity Management Systems For Public Services and The Impact on Privacy and Security Risks," 2023 International Conference on Digital Business and Technology Management (ICONDBTM), Lombok, Nusa Tenggara Barat, Indonesia, Indonesia, 2023, pp. 1-6, doi: 10.1109/ICONDBTM59210.2023.10326737.

[10] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643.