International Journal of Reliable and Quality E-Healthcare
Volume 12 • Issue 1

Decentralized Blockchain-Enabled Employee Authentication System

Bipin Kumar Rai, ABES Institute of Technology, India*
https://orcid.org/0000-0002-9834-8093

Pranjal Sharma, ABES Institute of Technology, India

Sagar Singhal, ABES Institute of Technology, India

Basavaraj S. Paruti, Ambo University, Ethiopia

ABSTRACT

In recent years, there have been many attempts to introduce blockchain-based identity management solutions, which allow the user to take over control of his/her own identity. In this paper, the authors have reviewed in-depth existing blockchain-based identity management papers and patents published online. Based on that analysis of the literature, a system will be implemented which will come up with the current issues and try to minimize them. Being transparent, immutable, and decentralized in nature, blockchain mechanism is found to be a better technology which can reduce the corruption in the experimental scenario. The objective is to develop a decentralized system which can be used for the verification of the employees in an organization. This is done to stop or reduce the cases of identity theft and data leakage in recent time. This system will be using Ethereum blockchain platform for monitoring the information and smart contract for authentication.

KEYWORDS

Authentication, Blockchain, decentralised, Ethereum, Hyperledger

INTRODUCTION

Authentication is a security process through which proof of identity or ownership is required. It allows a user owning an account login credentials to log in to their account while denying access to others. In most cases, the user's login information is stored on a server. Therefore, the authentication process is an interaction between the user and a server. Since this can access sensitive data, the server in which login credentials are stored must be secured. Authentication based on blockchain is kept in review to lower malicious activity and increase the security of the authentication process. Identity Theft is when a person contacts you pretending to be an employee of that organization, providing you with all the documents to gain your trust. Authentication as to the person contacting is the one who he is claiming to be. Virtual identity is the information of a/an user/entity used by the system

DOI: 10.4018/IJRQEH.323570 *Corresponding Author

to represent an external agent. They may be a person, company or any application or device. The information in a virtual identity allows for the assessment and authentication of the user interacting with a business system on the web without the involvement of human operations. Virtual identity allows our access to computers and their services to be automated, making it possible for computers to mediate relationships.

Blockchain uses the key pair for the users to register their identity. Personal information is stored in hashes, which can be used for identity-related attributes like name, unique identity number or social security number, fingerprint, or other biometric information. After that, the user can request a recognized party to verify the hashes by authenticating that the information provided on the blockchain is accurate. So now, whenever someone requires a user's identity for any authentication or identification mechanism, they can use the hashes of the block pre-verified by the trusted, recognized party. As all the data is stored in the form of hashes, each block consists of a unique key pair, making it difficult to crack the information. Also, we are implementing an IDS/IPS to prevent the data from being compromised. Whenever a considerable amount of traffic is exposed to a server, there are chances of crashing. What we are going to do is host the server using blockchain technology. It will reduce the chances of server failure as now the server will be hosted in different blocks for which we can direct the traffic to other blocks rather than referring it to a single server. It will also allow us to engage more traffic as the server crashing chances will be minimum.

There will be a block for every employee working there. As all the employee information is saved in the form of hashes, a unique identification number will be given to each block which can be used or considered the employee ID. To verify the employee, the client or user must enter the employee id into the organization's portal. However, the challenge in such cases is that it involves a high level of trust between the parties. Another challenge that the authentication of identity by blockchain faces is the involvement of different independent participants in calculating the blockchain to make it trustworthy and decentralized.

Our research objective is to develop a decentralized system that can be used to verify the employees in an organization. This is done to stop or reduce the recent cases of identity theft and Data leakage. This system will use Ethereum blockchain to monitor the information and smart contract for authentication.

REASON TO FOCUS ON DIGITAL IDENTITY

Let us first discuss the reason for the significance of digital identity. Digital Identity has become an integral part of our lives with the rapid expansion of technology. We need to have an account for accessing social media profiles where we have already mentioned all our personal information, such as name, address, phone number, date of birth, mail id, etc. Digital Identity allows us to interact with and use different services available through the internet, such as banking services.

The need to reflect on blockchain identity management benefits emerges from the lack of security generally expected from identity management systems. The shifting of each and everything into the digital age has also created new approaches to identity theft. Therefore, hackers, Fraudsters, and other malicious agents are leveraging the latest identity theft tricks to rob people of their money—moreover, the conventional identity management systems relying on paper-based evidence present concerns such as misappropriation of identity.

Advantages of Blockchain Identity Management

Blockchain identity management is more of a necessity than a technical privilege in the existing environment. How it changes conventional identity management and resolves the current identity issues draws attention to blockchain identity management benefits. Here are some of the benefits that can be availed with blockchain-based identity management solutions.

Relief From Typical Paper-Based Identity Management

Blockchain identity management solutions can help users obtain duplicate ID proof if they lose their original documents. People who lose or misplace their original ID-proof documents might have to go through specific processes to return them.

For example, they may have to visit the related government department and undergo a time-consuming process to get duplicate ID proof. Government authorities generally have a large piece of information while depending on manual processes, thereby creating delays in issuing identical IDs (basically, it is time-consuming). In such cases, people living away from government service centres, some shifted to other cities, and people from underprivileged societies experience the most difficulty accessing a duplicated ID proof.

Blockchain identity management benefits such as ensuring that records are permanent and tamper-proof resolve such issues. Government authorities could store the ID proof of individuals on a blockchain with the assurance of safety and reliability. In addition, blockchain security ensures that the ID-proof record is permanent.

Easier ID Verification

Identity management solutions could experience the burden of complexity due to various pre-existing manual processes. On the other hand, blockchain technology can power up identity management solutions to overcome these setback issues. The benefits of blockchain identity management for identity verification are visible in examples of identity management solutions.

Self-Sovereign Identity (SSI)

The digital world has opened many opportunities while setting many challenges over time. However, it also has many corners that come to public light occasionally. The Facebook/Cambridge Analytics data scandal clearly shows the darker side of how tech giants can control and manage the digital identity of users. Such incidents require further emphasis on understanding the risks of digital identity management.

As discussed, conventional identity management presents complexities and difficulties for users in managing their digital identity. In this case, self-Sovereign Identity or SSI can serve as a good answer with blockchain identity management benefits. First, users get complete ownership and control over their digital identity.

The consent of the primary user is essential for other parties to access their identity information. SSI is inherently trustless by design, thereby avoiding the need for trusted 3rd party providers. The most common example of using blockchain for obtaining SSI is Hyperledger Indy. The enterprise blockchain framework by the Hyperledger Consortium is the proven answer for digital identity use cases.

Non-Custodial Login Solutions

Internet users must trust third parties while logging into internet-based services or signing into their employer's networks for their ID and password safety. Generally, the service provider or employer maintains central servers to secure user credentials. Such solutions are called 'Custodial Login Solutions', and just like any other centralized solution, they are highly vulnerable to hacking.

Centralized systems serve as appealing targets for hackers. However, the benefits of blockchain identity management can completely change the scenario with decentralization and improved security features. Blockchain identity management solutions leverage public-private critical pairs for login, thereby ensuring the safety of login credentials.

Decentralized Digital Identity Solutions

Blockchain identity management benefits also provide identity management for the decentralized web—different third-party services, such as internet service providers, track users' online activity.

So, internet users are turning towards a decentralized web where they don't need to provide personal information to access services.

However, users must have one digital identity to validate their credentials anywhere on the decentralized web, and blockchain can help. Users could place their digital ID on a blockchain, and internet-based services could access it for verification objectives.

Better Safeguards for Critical Systems/Assets

The significance of better security in digital identity management is not limited to logging our accounts into social media platforms. Many of the systems/assets, whether physical or virtual, such as grids and power plants, are still possibly affected by password protection. Identity management systems implemented using blockchain technology could offer more advantages than security and personal convenience. Employees working in the ecosystem can only access the essential control systems, ensuring the limited potential for attacks on critical infrastructure.

BACKGROUND

Claudia Antal et al. (2021) suggested smart contracts and what data needs to be there. Yang Liu et al. (2020) proposed algorithms for managing identities digitally and for the same authentication. Yousif Abuidris et al. (2020) proposed how to handle extensive data using the blockchain. Zwitter et al. (2020) proposed Innovations in the digital domain, which are increasingly shaping the daily processes and interactions of individuals, educational institutions, companies, and governmental organizations. Tarkhanov et al. (2020) propose a new data synchronization method between public blockchain networks and local machines. Jihyeon Song et al. (2020) gave a solution for detecting the malicious PowerShell script by statically analyzing the scripts and pre-processing tokens using an abstract syntax tree. S. El Haddouti et al. (2019) use algorithms to manage identities digitally and authenticate the same. Rai, B.K.(2022), Rai, B.K.(2023) and R. Chaudhary et al. (2019) proposed a solution to introduce blockchain technologies, including their benefits, pitfalls, and the latest applications. Dirk Van Bokkem et al. (2019) concludes that blockchain technology is not explicitly required for a Self-Sovereign Identity solution. Still, it is an excellent foundation to build on due to blockchain's various technical advantages.

Wenbo Jiang (2019) emphasizes that blockchain has numerous desirable properties, such as its decentralized nature, cryptographic technology, and unalterable transaction record; these properties make it a potential tool for building a decentralized blockchain-based PKI. Feifei Wang et al. (2019) discovered that their scheme suffers from severe weaknesses, such as session key disclosure attacks, desynchronization attacks, sensor node impersonation attacks, and session-specific temporary information attacks, and does not provide forward secrecy. Tiago M. Fernández-Caramés et al. (2018) provide a thorough review of how to adapt blockchain to the specific needs of IoT to develop Blockchain-based IoT (BIoT) applications. Kumar Rai, B. et al.(2021) emphasized the use of emerging technologies for solving the societal issues. Rai, B. K. et al. (2021) discussed the use of OSINT technologies for gathering of significant data. T.-T. Kuo et al. (2017) proposed a solution for how to use Hyperledger to manage the data. Qi Jiang et al. (2016) claimed that the scheme achieves mutual authentication and withstands all major security threats. However, we identify that their scheme fails to perform mutual authentication because it is vulnerable to the service provider impersonation attack. R O Sinnott et al. (2008) discuss two main possibilities based on a centralized or decentralized approach to role management. We present the advantages and disadvantages of the centralized and decentralized role models and describe how we have implemented them in a range of security-focused e-Research domains.

THE DECENTRALIZED BLOCKCHAIN-ENABLED EMPLOYEE AUTHENTICATION SYSTEM (DBEAS)

The Decentralized blockchain-enabled employee authentication system (DBEAS) will work so that the employee first needs to fill in the information into the form provided by the contract owner. After filling in the details, the employee must verify them by uploading the employee ID, Aadhar card, Driving license, and biometric information. After uploading these documents, the contract owner or the role owner of that organization will verify the documents, authenticate the employee, and provide the hash to the employee, which will further be used for verification, as shown in figure 1.

Whereas if we talk about the user end, the user will input the hash provided by the employee in the dashboard, and then it will fetch the information from the block, verify it side by side, and inform the contract owner. Then if the data exists in the database, it will fetch the information and inform the user who was checking that the employee is authenticated; otherwise, it will give the output of verification as failed or employee not authenticated.

Our workflow works on the client and employee sides, as shown in figure 2 and figure 3, respectively.

Firstly, on the employee side, the employees log into the company's authentication portal with the help of credentials given by the company. After that, the employee must upload all the required

Figure 1. DBEAS authentication architecture

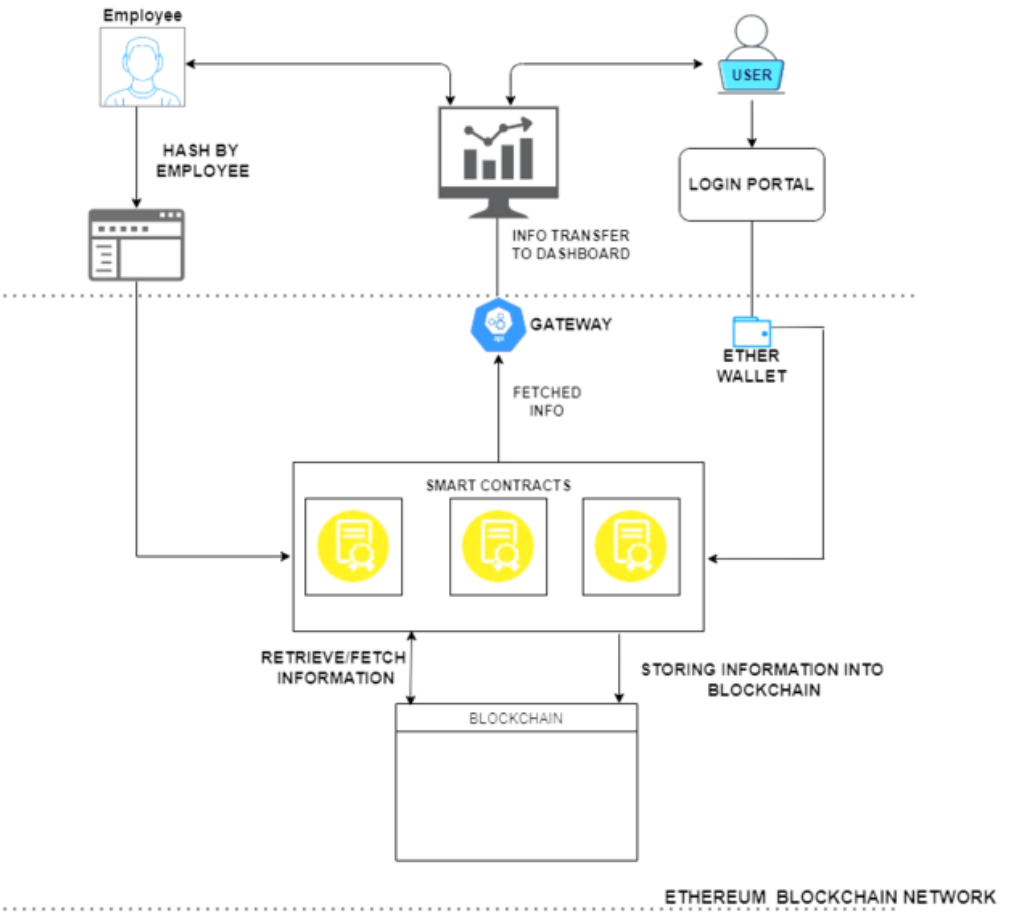


Figure 2. Employee authentication architecture

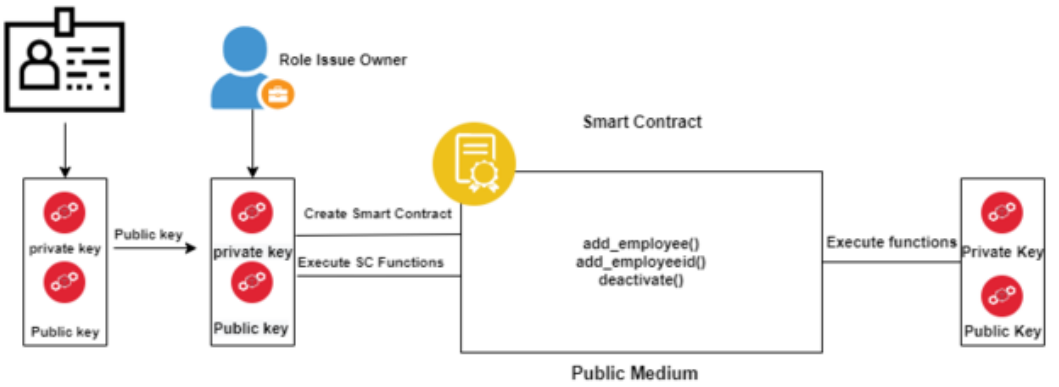
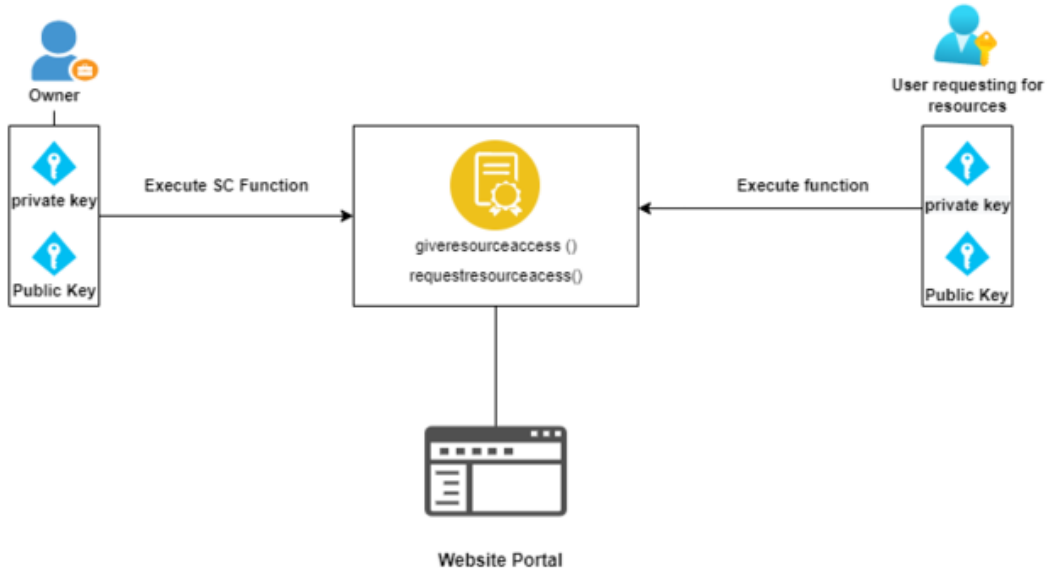


Figure 3. User-end architecture



documents into the portal. Then all the info will store in a blockchain, and a hash is produced for that block id. On the client side, the employee will provide the hash to the user, and the user must input that hash into the portal to verify the user. The info will retrieve if it exists and can confirm whether the employee is actual or fraudulent.

In this, we are considering the role issue owner (company analyst), which will create an Ethereum smart contract where the role issue owner makes the employee account. Creating intelligent contracts generates a pair of keys and a hash of the public key in which there are several options for employees, such as uploading documents, etc. The role of the public key is to store the key pairs, digital certificates, digital signatures, and hashes.

In the user mechanism, the user fills the hash code into the portal, and then the smart contract executes the function and matches the public key with the help of Custom API. The information will only be fetched from the blockchain if the public key is correct.

Otherwise, it will return an error.

The user will request the resource owner for the information as the request gets received, and the role issue owner smart contract will fetch the data from the database and publish it to the website or portal.

IMPLEMENTATION

The technology used to implement this proposed work is shown in figure 4. We implemented our model using the Ethereum wallet. The smart contract and role issue owner is written in solidity language. Now, in which the smart contract is compiled using Ethereum virtual machine (EVM). EVM is an execution environment for deploying smart contracts and generates the byte code after compilation. We have deployed and tested our smart contract using the test Ethereum from the Ropsten and Rinkeby test networks. Figure 5 shows the process flow of the application, and Figure 6 represents the authentication workflow.

Figure 4. Technology used

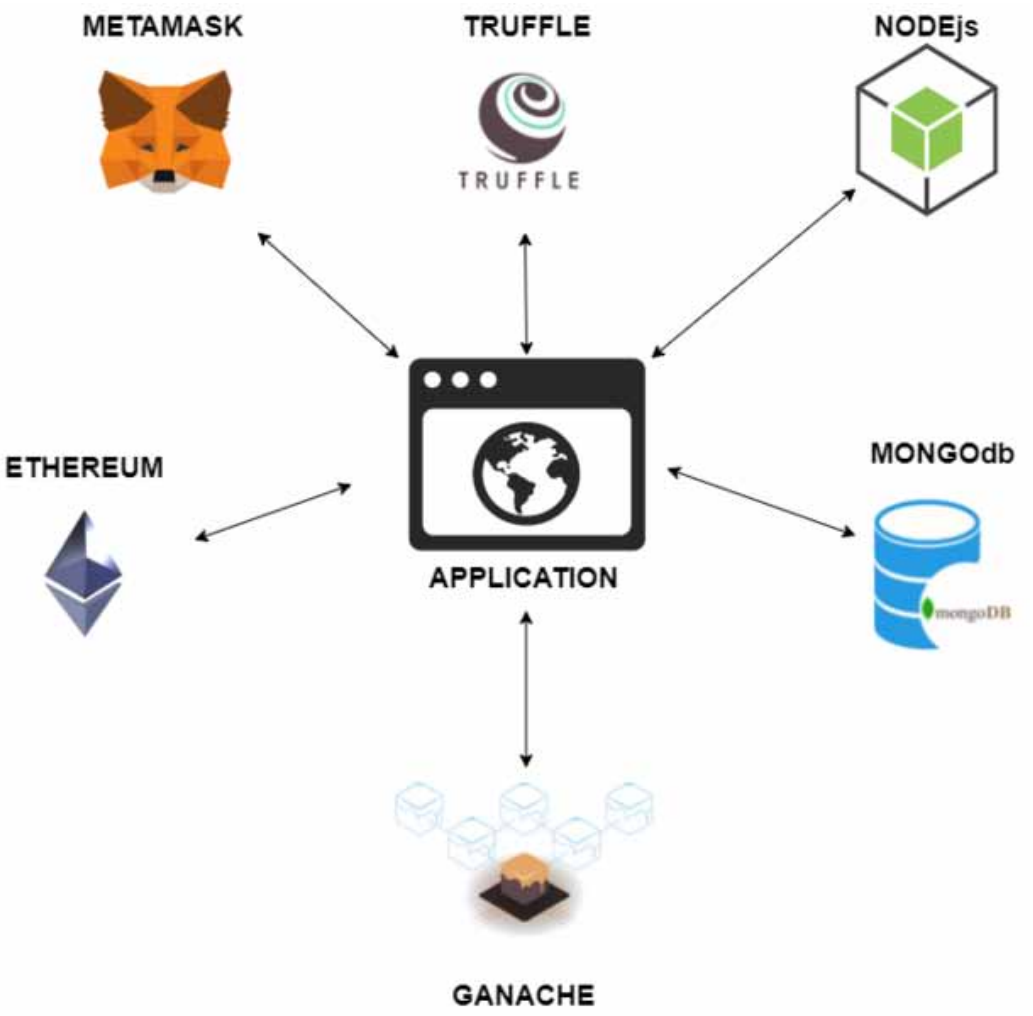
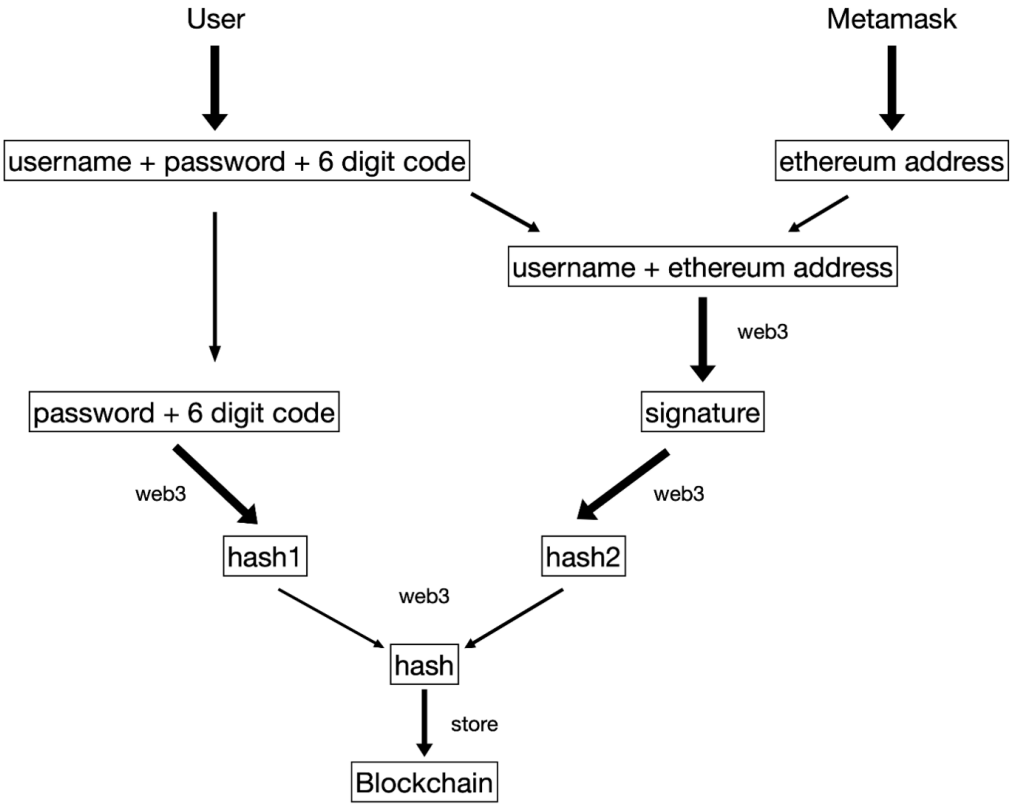


Figure 5. Process flow of the application



Employee Registration

1. State
2. Address_ContractOwner
3. Struct EmployeeInfo(FullName, EmailID, MobileNo.)
4. Struct EmployeeDoc(DL,Passport,Addhar,CompanyID)
5. MAP(Address EmployeeInfo,string inserted)
6. MAP(Address EmployeeDoc,string inserted)
7. Function Adding EmployeeInfo
8. .....
9. Function Adding EmployeeDoc
10. ....
11. INPUT: EmployeeInfo,EmployeeDoc
12. OUTPUT: Employee HASH

In Employee registration, firstly, there is a need to add a contract owner where all the employee details must be stored. Then the structure for the employee information will be created, and employee documents will be uploaded. Then a function is designed for employee input, where the employee must input their details. After that input, the output will come out as HASH. The employee's information can be extracted from the blockchain using that hash.

Smart Contract

In the smart contract for employee authentication, the employee information will be stored in a particular address, and a unique hash id will be generated. Using this, the user will further verify the employee.

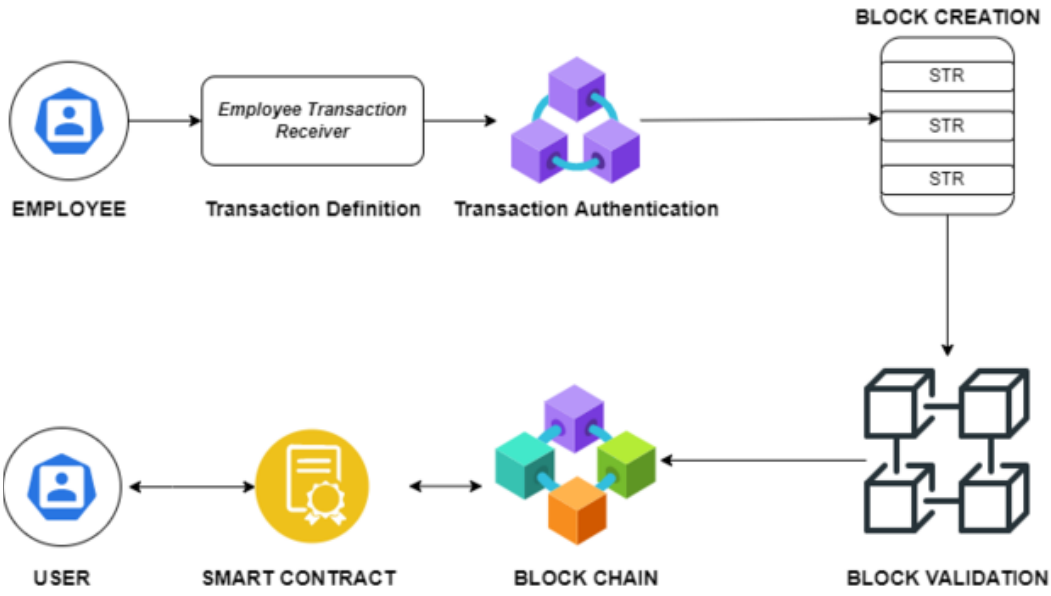
Authentication Algorithm

```
 INPUT: Employee HASH OUTPUT: EmployeeInfo or Invalid Hash
1.  EmployeeAssociated = NULL
2.  for HASH in EmployeeInfo in ContractOwner
     a.  if HASH == EmployeeHASH
     b.  EmployeeAssociated <--- HASH
     c.  if EmployeeAssociated == NULL then
     d.  Not a Company Employee (Verification Failed)
3.  else
     a.  EmployeeAssociated <----- EmployeeInfo
     b.  end if
4.  end if
5.  end for
```

This is the user-side algorithm. USER will put the hash into the portal and extract the employee's information on the user screen.

At first, the hash will be transferred to the employee info, which is present in the contract owner, where the HASH of the employee is also stored. So, it will match the HASH if the hash is the same and verified; then the information will be transferred to the Employee Associated, where a loop would look if the Employee Associated is empty. It will give the output that verification failed, or if the employee associated contains some string or values, it will show it to the USER panel and verify the employee.

Figure 6. Authentication workflow



WORKFLOW DIAGRAM

1. In this, first, the employee must log in to their dashboard and have to add their credentials as well as the proof of being the employee (i.e., name, employee ID, biometric etc.) of the company
2. We have designed a smart contract in which the information is processed and stored in the blockchain as a hash.
3. On the other side, when the user logs into the portal, the hash provided by the employee will be entered by the user in the authentication portal
4. With the help of custom API, we will fetch the employee's information from the blockchain network. The hash provided by the employee will hit the database and match the hash. If the hash is present, it will fetch the information from the blockchain and pass it on to the portal.
5. If the hash is not matched, it will revert that the employee is not of their company.

Contracts compiling: All the contracts are compiled, including the user's authentication and transfer of file data to IPFS (Intra Planetary file system).

RESULTS AND COMPARISON

At last, we reached a point where we can conclude that the identity management system using blockchain technology has been adopted and will be used shortly. We have also compared our proposed solution with the current one, and we came to know that they lag in several points we have taken care of. In our system, the table below briefly compares the main feature we have enabled in our DBEAS.

Below is the comparison with Sovrin, uPort, ShoCard, and our proposed solution named DBEAS. These three are mainly Self-Sovereign Identity management systems that are currently used worldwide and are open source, making this Digital identity concern decentralized, which will help in making it easier for employees as well as the user to maintain the identity and also verify them, which reduces the risk of losing them and re-issuing them.

CONCLUSION

Blockchain identity management system benefits can be incorporated entirely into the digital landscape. The applications/implementation of blockchain in digital identity management presents reasonable prospects for improving security, transparency, and control over data. Overall, improvements over the existing identity management systems were inevitable. However, blockchain presents decentralized solutions for the future of identity management. Presently, the applications of blockchain-based digital identity management solutions are gaining recognition, with a couple of notable examples. In this paper, we developed a decentralized system that can be used to verify the employers in an organization. This is done to stop or reduce recent identity theft and data leakage cases.

Table 1. Comparisons

Feature	Sovrin	uPort	ShoCard	DBEAS
Authentication	✓	✓	✓	✓
Biometric information pre-feed	×	✓	×	✓
Multi Chain Server	×	×	×	✓
Verification through employee id	×	✓	✓	✓

ACKNOWLEDGMENT

Competing Interests

All authors of this article declare there are no competing interest.

Funding Agency

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Funding for this research was covered by the authors of the article.

REFERENCES

Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021, April). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI Journal*, *43*(2), 357–370. doi:10.4218/etrij.2019-0362

Antal, C., Cioara, T., Antal, M., & Anghel, I. (2021, March). Blockchain Platform For COVID-19 Vaccine Supply Management. *IEEE Open Journal of the Computer Society*, *2*, 164–178. doi:10.1109/OJCS.2021.3067450

Chaudhary, R., Jindal, A., Aujla, G. S., Aggarwal, S., Kumar, N., & Choo, K. K. R. (2019, August). BEST: Blockchain based secure energy trading in SDN-enabled intelligent transportation system. *Computers & Security*, *85*, 288–299. doi:10.1016/j.cose.2019.05.006

el Bouanani, F., & the Institute of Electrical and Electronics Engineers. (2019). *International Conference on Advanced Communication Technologies and Networking (CommNet),* Rabat, Morocco.

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 32979–33001. doi:10.1109/ACCESS.2018.2842685

Jiang, Q., Ma, J., & Wei, F. (2018). On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Systems Journal*, *12*(2), 2039–2042. doi:10.1109/JSYST.2016.2574719

Kumar Rai, B., Sharma, S., Kumar, A., & Goyal, A. (2021). Medical Prescription and Report Analyzer. In *2021 Thirteenth International Conference on Contemporary Computing (IC3-2021)* (pp. 286-295). ACM. .10.1145/3474124.3474165

Kuo, T., Kim, H., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6). Oxford University Press. .10.1093/jamia/ocx068

Liu, Y., He, D., Obaidat, S., Kumar, N., Khan, M., & Choo, K. K. (2020). Blockchain- based identity management systems: A review. *Journal of Network and Computer Applications,* (*vol. 166*). Academic Press. .10.1016/j.jnca.2020.102731

Rai, B. K. (2023). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Serv and Outcomes Res Methodolog*, *23*, 80–102. https://doi.org/10.1007/s10742-022-00279-7 doi:10.1007/s10742-021-00268-2 PMID:36438614

Rai, B. K. (2022). Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records. [IJRQEH]. *International Journal of Reliable and Quality E-Healthcare*, *11*(1), 1–15. doi:10.4018/IJRQEH.297076

Rai, B. K., Verma, R., & Tiwari, S. (2021). Using Open Source Intelligence as a Tool for Reliable Web Searching. *SN Computer Science*, *2*(5), 402. doi:10.1007/s42979-021-00777-4

Sinnott, R. O. (2008). Advanced security for virtual organizations: The pros and cons of centralized vs decentralized security models. In *Proceedings CCGRID 2008 - 8th IEEE International Symposium on Cluster Computing and the Grid,* (pp. 106–113). IEEE. doi:10.1109/CCGRID.2008.67

Song, J., Kim, J., Choi, S., Kim, J., & Kim, I. (2021, June). Evaluations of AI-based malicious PowerShell detection with feature optimizations. *ETRI Journal*, *43*(3), 549–560. doi:10.4218/etrij.2020-0215

Tarkhanov, I. (2020). A method of data synchronization with Ethereum blockchain. *Artificial societies, 15*(3). ACM. .10.18254/S207751800010671-7

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*.

Wang, F., Xu, G., & Xu, G. (2019). A Provably Secure Anonymous Biometrics-Based Authentication Scheme for Wireless Sensor Networks Using Chaotic Map. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 101596–101608. doi:10.1109/ACCESS.2019.2930542

Wenbo, J., Hongwei, L., Guowen, X., Mi, W., Guishan, D., & Xiaodong, L. (2019). Privacy-preserving thin client authentication scheme in blockchain-based pki. *Future Generation Computer Systems*, 20.

Zwitter, A., & Hazenberg, J. (2020, March). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain*, *3*, 12. doi:10.3389/fbloc.2020.00012

Bipin Kumar Rai, Ph.D. from Banasthali University, Rajasthan and M.Tech. & B.Tech. in Computer Science and Engineering is working as Professor(IT) in ABESIT Ghaziabad, India. He has more than 17 years of teaching experience in different renowned Institutions. His areas of interest are Cryptography & Information Security, Blockchain, Compiler Construction, and Data Structures. He has published his Ph.D thesis work entitled "Pseudonymization Based Mechanism for Security & Privacy of Healthcare: PcPbEHR Solution for Healthcare" and M. Tech. dissertation work entitled "An Optimized Solution for Certified e-mail with Trusted Third Party". He has published 25 research papers in ESCI/Scopus indexed Journals/Conferences, 4 Books, 6 book chapters in Springer/CRC Press Taylor & Francis Group. He has worked as a Guest Editor/Reviewer of several SCI/Scopus Indexed Journals.

Sagar Singhal has completed his B.Tech. in IT from ABESIT Ghaziabad, India.

Pranjal Sharma has completed his B.Tech. in IT from ABESIT Ghaziabad, India.

Basavaraj S. Paruti, is working as Professor in Ambo University, Ethiopia