International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain Technology for Identity Management

Junaida Moidu[1], Jayalekshmi S[2], Nandana S Raj[3], Dr. Solomon Jebaraj[4]

[1,2,3]MCA Scholar, Department of CS & IT, JAIN (Deemed to be University), Bangalore
[4]Professor, HOD OF AI AND ML, Department of CS & IT, JAIN (Deemed to be University), Bangalore

Abstract

Blockchain technology has revolutionized identity management system because of its secure, transparent and decentralized way of storing information. Even though it provides a decentralized solution they face a critical challenge that they don't account for the context in which they are used. As a result, when credentials are issued it can be used in any context. To overcome this shortcoming of traditional blockchain based identity management system, we are proposing a novel methodology. In this paper I am proposing a new methodology Proof-of-contract Identity validation which introduces contextual validation into blockchain based identity management system, so that the credentials can be used only when the predefined, authorized context are met. In this we are integrating contextual constraints like time, location and purpose. By integrating these contextual constraints, it ensures that the credentials are valid when predefined conditions are met. By ensuring that credentials are used in authorized context, it prevents fraudulent and unauthorized use of credentials.

The main components in Proof-of-Context Identity validation are: Contextual identity credentials, which are used to store the context-based validation rules along with identity information; Context Oracle, which provides real-time contextual datalike time, location and usage condition; and then we have PoC smart contract which ensures that the credentials comply with the context before giving access to the resource requested by the user. In addition to this we have a tamper-proof Interaction Log Registry in which all interactions along with the credentials are logged. This provides transparency, accountability of credential usage. This can be used in the field of healthcare, education and government services.

Despite its advantages, there are several challenges including difficulty in managing context rules, scalability issues when dealing with large transactions and users, and for getting real time data we need outside sources like oracle, which could lead to a problem if the data is inaccurate or unavailable. In this paper we are going to discuss possible solutions to these challenges. In this paper we are going to discuss the techniques to protect privacy, using decentralized data sources like oracles to reduce the reliance on a single source, and making the context verification process faster. In this paper we are also going to discuss about legal and regulatory requirements as well as suggest areas which requires further improvement.

KEYWORDS: Blockchain, Digital Identity, Proof-of-Context Identity Validation, Contextual Validation, Decentralized Identity, Privacy, Smart Contracts, Identity Management, Access control, Credential Verification.

1. Introduction

The increasing need for digital identities in various section has highlighted the importance of secure, transparent identity management system. In traditional identity management-system the information is validated and issued by centralised authority which is prone to attacks like unauthorised access.

Blockchain technology is a decentralised, tamper proof and secure identity management system which overcome the challenges of traditional systems by providing self- sovereign identities, which helps the users to manage their identities without the need of any intermediaries. In blockchain based identity system we store our digital identities in special digital ID called Decentralised identifier. This is cryptographically secured and whenever the user wants to prove their identity, they can use this without the need of sharing more of their personal information. Even though this is secure and decentralised way of storing information still it doesn't verify the context in which the credentials are used. For example, if a person receives a digital credential like degree certificate, the person can use it anywhere irrespective of the context. This poses a serious issue since digital credentials can be used by anyone. Sometimes the person might use their credentials in wrong situations or another person who has stolen this credential' s can also use it for malicious purpose.

To address all these limitations, in this paper we propose a novel idea of Proof-of-Context identity validation where contextual validation is also done. In this methodology, not only the credentials but the context in which credentials are used are also verified before giving access to the requested resources. In this we include contextual constraints like time, location and purpose. This provides an extra layer of security to blockchain based identity systems which protects the system from unauthorised access.

Proof-of-Context Identity Validation has three key components:

1. Contextual Identity Credentials: These credentials are issued with predefined constraints which are the special conditions in which this credential can be used. This constraint's include time like it can be used only during the working hours, geographical location which is like the credentials can be used only in a particular country, purpose which is like the credentials can be used only for a particular purpose.
2. Context Oracles: This is the second main component of Proof-of-Context Identity Validation which is used to get the real time context in which the credentials are used. This gives location-based information, time related data and also the context in which the credentials are used. Context Oracles play a very important role in providing real time data to ensure that the credentials are used in valid context.
3. Proof-of-Context Smart Contract Validator: This helps to validate the context in which credentials are used before giving access the resource that has been requested. This validates every possible context we get from oracles which ensures that no misuse of credentials can be performed.
4. Interaction log Registry: In addition to all other components, we have this component to log all the interaction using identity credentials. This provides accountability and traceability of activities using identity credentials.

Proof-of-Context Identity Validation provides an extra layer of security by verifying the context in which credentials are used. This enhances the trust in the integrity of the blockchain based identity systems since it prevents any fraudulent activities. Though Proof-of-Context Identity Validation has lot of advantages, it also has challenges when coming to collecting the real-time data to get context, scalability issues. We are going to discuss about challenges and also provide possible solution to this challenge.

In the remainder of this paper, we are going to review the papers which already exist, propose the methodology with its components and architecture, its applications and challenges, and at last we are going to conclude this paper by providing ideas for future work which will refine Proof-of-Context Identity Validation for large scale uses.

2. Literature Review

Traditional identity management system is often centralized which is more prone to attacks. To overcome this, in recent years we have blockchain technology which provide decentralized, secure and tamper-proof way of storing data. To address limitations of identity management system numerous studies have been explored to integrate blockchain technology for identity management.

In [1] the author is discussing about the blockchain based identity management system which enhances cybersecurity by preventing single point of failure. This study tells us about how decentralized system along with smart contracts, public and private key, distributed ledger enhances security by preventing single point of failure. Similar arguments are also proposed in research paper [2]. Using this type of identity management system helps user to manage their own identity credentials without intermediaries.

In [3] the author discuses about the technical implementation. By adopting SSI and verifiable credentials, the study shows how the user can issue and verify identities without intermediaries.

In Systematic review [4] the author tells us about the blockchain based identity management systems which provide secure, tamper-proof way of storing data. In this author tells us about the benefits like trust, privacy and reduced third party interference. In [5] also the above idea is iterated along with their applications in healthcare and financial sectors. It tells also about how blockchain based identity management provide secure, tamper-proof way of storing data and transactions.

In [6] the author is saying about the benefits of integrating AI into education system which helps in online tutoring. But the researchers are worried about the potential vulnerabilities of sharing personal information online. So, the author is proposing a blockchain based solution for protecting personal information which provides immutability, accountability and transparency. In [7] and [8] also they discuss about the great potentials of blockchain based identity management systems which prevents fraudulent activities. This paper also highlights the need for addressing the scalability and legal frameworks foe widespread adoption of these blockchain based identity management system.

From these studies, it is evident that blockchain based identity management system by adhering to SSI principles has immense potential to provide security, privacy and user control. It also has challenges like scalability issues, adherence to legal frameworks, and the institutions and organizations must be ready to adopt blockchain based identity systems.

3.Proposed methodology

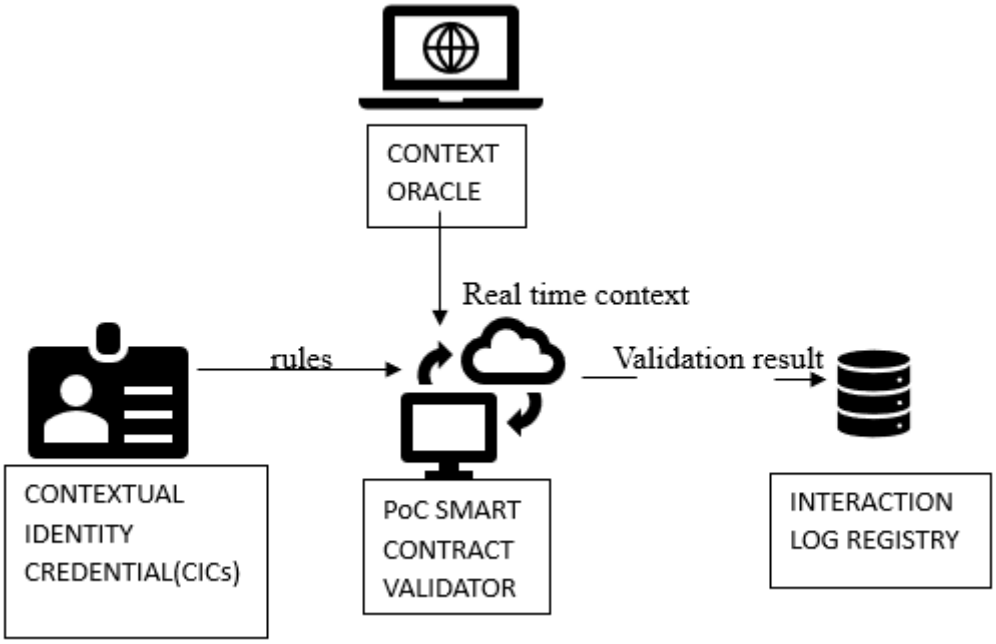
The increased adoption of decentralised identity management system has allowed the individuals control their credentials without any third-party involvement. But in this decentralised system the credentials can be used irrespective of the context. To overcome this in this paper we have proposed a novel methodology "Proof-of Context Identity Validation" which integrates context validation along with credentials whenever a user request to access a specific resource. This happens automatically on the blockchain, using smart contract, which is a secure and transparent way. In this context constraints like time, location and purpose for which the credentials can be used is predefined so that whenever a person requests access, context validation is done before giving access to specific resource. This context validation is enforced through dynamic on-chain validation.

In Proof-of-context Identity validation we have three main components:

1. Contextual Identity Credentials: This is an identity credential that includes the context in which this credential can be used. This ensures that this credential can be used only in a valid context.
   For example: For example, credentials provided by educational institution can have constraint that it

can be used only in university working hours, within a specified location and for a specific purpose.

2. Context Oracle: This is the component which is used to get the real time information from external sources like oracle. This is necessary to get the context like the time, location and the purpose for which the user is using his credentials. This is very much to find whether the credentials align with the predefined constraints. This is very important component in our Proof-of-Context Identity validation layer which helps to get the real time information about the user which is very much essential to provide access to specific service.
3. PoC Smart Contract Validator: This component is used to validate the CIC by querying the context with context oracle. It ensures whether the real time context aligns with the predefined context of the credential. If this is true, then the user gets access to the requested service. This is the main part within the blockchain which interacts with both Context Oracle and user to validate the CIC.
4. Interaction Log Registry: This is the next component which is used to log all the interactions. This is really important component which records all the interaction which is very useful to find out malicious activities. In this every interaction whether it is successful or not are recorded which helps to audit. This will help really well in finding out suspicious activities.



4.Workflow

The Proof-of-Context Validation workflow starts whenever a trusted university provide a decentralised identifier to the user which also contains context rules in which they can use. Whenever the user requests access to specific resource or service with their CIC and DID, the PoC smart contract queries the Context oracle for the real-time data like the time, user's location and the purpose of request. When the real time data given by the Context Oracle aligns with Credential predefined rules, the PoC Smart Contract accept the request and give access to the required resource or service. Otherwise, request is denied. Whenever a request has been raised by the user, the interaction is recorded in the Interaction Log Registry irrespective of whether is access is accepted is accepted or denied. This is really helpful to find suspicious activities. Further more the issuers can define more details on when, where and how the credentials can be used giving more granular control on how the identities are used. In addition, this methodology makes use of

decentralised system which ensures that there is no central authority. Here they make use of smart contracts for the context validation which helps to protect our system from attacks. This prevents our credentials being used for unauthorised access. This system also provides privacy by including only context data like time, location in on chain while the personal information is kept off chain.

Although this has immense potential, it has limitations as well. Defining context rules for each case can be complicated and time consuming. Also, dependency on the oracle for real-time data can be time consuming and also sometimes untrustworthy. So, we should use decentralised oracle which does depend on the central authority so that the information can be trustworthy. In the future we can in cooperate Zero Knowledge Proof which enhances the privacy by validating whether the rules are followed without actually revealing the personal information of the user. Also adding a system called federated learning will allow the system learn where different identities are used which helps them to adjust the context rules without revealing the user's personal information which is more secure.

5. Experimental Setup

We are creating a practical setup in our decentralised system to check our new idea "Proof-Of-Context Identity Validation". Instead of spending real money, we work in a test network like Sepolia. We use Ethereum Blockchain for this. We built smart contracts which gets executed when predefined conditions are met and this is built using Solidity. For making it easy for the users to send access requests, we create a simple webpage using React JS. Since our idea is to validate the request based on their context, we have to integrate the blockchain with an external service called ChainLink Oracle which gives us the real time data needed to validate the context. For managing and testing smart contracts we use special tools like Hardhat and Truffle.

In setup we have four main components:

1. Contextual Identity Credential: This is given to users by the trusted organisation like university which includes user's identity and rules about when, where and how it could be used.
2. Context Oracle: this layer is used to get the real time information like the current time, user's location and the purpose of a specific access request.
3. PoC smart contract validator: This layer is used to check whether the real time information we get through the Context Oracle matches with the rules attached with the user's credentials.
4. Interaction Log Registry: This is used to keep the records of the log irrespective of whether the access is provided or denied. This helps in auditing and find out if any suspicious activities are happening.

The process begins when the issuer like university or any trusted organisation issues Decentralised Identifier along with along with a Contextual identity credential to the user. Whenever a user request's access the rules defined for their CIC is checked with the real time data produced by the Context Oracle. After validation if the rules of the user's credentials match with real time data, then they are granted the access otherwise the access is denied. Interaction Log Registry logs all the records even if the action is denied.

6. Experimental result

Since we have not done any testing or simulated testing I am going to discuss the expected outcome of our methodology Proof-Of-Context Identity Validation. This outcome is based on the architecture, the experimental setup. The results mentioned below are the possible outcomes of this methodology:

Access Decision Time: This access decision time depends on various parts of the system like Context-Oracle, the Proof-Of-Context Smart Contract Validator, and the time the Blockchain takes to validate the transaction. The context Oracle is expected to give the real time data on an average 1.5 seconds. This is based on the typical performance of the decentralised oracle like chainlink.
The Proof-Of-Context smart contract validator is expected to complete the validation within 0.5 seconds. So in total the expected access time in 2 second which is fast enough in practical use.
System Efficiency and scalability: The system is expected to be efficient and it will be able to handle many numbers of users and access request as long as the infrastructure and oracle is working efficiently.

- Transaction Throughput: Since Proof-Of-Context Identity Validation works on blockchain it can handle many transactions in a second as long as oracle services are not overloaded.
- Gas Consumption: Running smart contracts in Ethereum costs gas which cost approximately 50000 to 150000 gas units. For PoC-Iv the gas cost is expected to be similar to this. So, this is affordable for moderate use.

Security and privacy: Proof-of-Context Identity Validation uses blockchain's security. It will keep only necessary information on chain and will keep all the personal information off chain. Since validation is done based on the context not only based on the identity, this prevents unauthorised access and malicious activities happening.
4)Interaction logging and Auditability: Whenever a person gives an access requests the log details are recorded in the Interaction Log Registry which ensures that no malicious activities are happening. This ensures auditability and transparency. So, if someone tries to access the system from different location, time or purpose other than the rules mentioned for that identity credentials then we can easily trace out those people. This helps really well in preventing any malicious activities.
Oracle dependency and real-time data availability: Since for real time data we are depending on external services like Oracle, this poses a problem. If the Oracle experiences some downtime or gives some inaccurate data this poses a potential risk since our Proof-Of-Context Identity Validation is depending on this for real-time data. So, in the future we have to iterate to create decentralised oracle so it doesn't depend on central authority for the data. This helps to reduce the dependence on a single source.
Future Testing and improvements: Though these are the expected outcome, real time testing is required to find out the potential vulnerabilities and benefits of this system. And also, we can integrate Zero Knowledge Proof and Federated Learning which helps to improve privacy and adaptability, which improves the overall performance of the system.

7.Applications and Challenges

7.1 Applications

EDUCATION: POC-IV is very useful in educational institutions to manage the credentials of the students. This ensures that these credentials cannot be used for any malicious intent. For example, when university issues certificate to the student, they can bound the certificate with constraints in which they can use this certificate. The constraints can be that the certificate can be used in campuses and trusted online platforms which prevent any misuse of the certificate. This can also be used to control access to special academic purposes, which ensures that the certificate is used only for intended purpose.
Hospital: POC-IV is also useful in hospitals for manging medical licenses and practitioner credentials. We can bound the medical licenses with context constraints like the license in valid only in hospital location and also only during the hospital working hours. This ensures that even id the license get stolen

and they try to access the hospital system using the medical license they are denied access as they are at different location. This ensures that the details of the patients are secure enough.

Financial Services and Digital Wallet: POC-IV is really useful in financial services. This defines constraints on the banking credentials and digital wallet. For Digital Wallet constraint like this can be accessed only during business hours can protect the system from unauthorised access. Similarly for bank account we can constraint the amount of money a person can withdraw in one go or a particular day.

Company and enterprises: Company often gives their employees employee Id and login account to get access to company data and internal system of the company. So POC-IV can be used to bound the credentials with constraints like this can be used only during working hours, or only in the computer provided by the company, or for a specific task. This ensures that that even if the credentials are stolen that cannot be used in any other computer or time. This ensures that even if the someone with malicious intent tries to access to companies internal-system they are denied the access.

7.3 Challenges

1. Flexibility in defining contextual rules: It is really complicated to define context for each type of credentials. The contextual rule we define must be flexible, secure. We have to define the most perfect context for each credential's which is really difficult. If the rules we define is strict and complicated it would be difficult to use in practice.
2. Difficulty in getting real-time data: To get real time data we use the context oracle. These external sources can provide untrusty and inaccurate data sometimes. This can lead to a problem since the users can get access only when their credential rules align's with the real-time data like location, time and purpose.
3. Regulatory compliance and standardisation: Different regions and industries have different regulatory requirement. So, the implementation of Proof-of-context Identity Validation will be difficult based on the regulatory requirement of each region and industry.
4. Scalability issues: As number of users and transactions increases the system become less respondent because of the traffic. Smart Contracts which validate the context will become overwhelmed as the number of transactions and users increase which make the entire blockchain system inefficient to use. So appropriate must be done.

8.Conclusion

In this paper we have proposed a novel methodology "Proof-of-Context Identity Validation" as an extension to existing blockchain based identity systems. In this along with the identity authentication, we have in-cooperated context validation which enhances the overall security since this ensures that not only the identity but also the context of credential usage is also validated. This has immense potential of development. We use PoC Smart Contracts for this validation by querying with the context oracle. This provides an extra layer of security to the existing decentralised blockchain based system. This methodology overcome the shortcomings of the existing blockchain based system providing secure, transparent and tamper proof way of storing data validating the context of credential usage as well. Even though it is a great idea having immense potential of success, it also has challenges. The main challenge is with defining the context like time, location and purpose of credentials. It also has privacy concerns. Future works can be done to enhance privacy, to establish a standardised technique for context-based validation. We can in-cooperate Zero Knowledge Proof which is used to validation of the context is done without revealing the personal information od the user. Also, we can use federated learning for making the

system learn how different identities are used by the users and also in which context they are using this so that the system will be able to adjust the context rules based on their learning.

9. References

1. Riko Herwanto, Eddy Sumartono, Didit Saputra and Salman Farizy "Enhancing Cybersecurity with Blockchain-based Identity Management," , Global International Journal for Innovative Research, 2024.Available Online:https://www.researchgate.net/publication/383527499_Enhancing_Cybersecurity_with_Blockchain-based_Identity_Management
2. Nikhil Ghadge, "Use Of Blockchain Technology To Strengthen Identity And Access Management," SSRN electronic Journal, March 2024, Available Online:https://www.researchgate.net/publication/381156132_USE_OF_BLOCKCHAIN_TECHNOLOGY_TO_STRENGTHEN_IDENTITY_AND_ACCESS_MANAGEMENT_IAM,.
3. Yuhao Liu, "A Framework for Decentralized Identity and Credential Management Leveraging Blockchain Technology," Proceedings of the 8th International Conference on Economic Management and green development. Available Online: https://www.researchgate.net/publication/385328281_A_Framework_for_Decentralized_Identity_and_Credential_Management_Leveraging_Blockchain_Technology,.
4. Haifa Alanzi and Mohammed Alkhatib, "Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A System Review," ,APPL. SCI. 2022,12,12415.Available Online: https://www.researchgate.net/publication/366014400_Towards_Improving_Privacy_and_Security_of_Identity_Management_Systems_Using_Blockchain_Technology_A_Systematic_Review .
5. M. Ade and S. Dubois, "Blockchain-based Identity Management for Secure Financial and Healthcare Transactions," Available Online: https://www.researchgate.net/topic/Blockchains/publications/389362196.
6. Sharma Rhodes, Chen Zhang and Hennah Adebayo “AI-powered Knowledge Transfer: Enhancing Learning with blockchain technology”, March,2025. Available Online:https://www.researchgate.net/publication/389891562_AI-Powered_Knowledge_Transfer_Enhancing_Learning_with_Blockchain_Security,.
7. Heena Khanna, Gitanjali Gupta, and Harsh Sharma, "Investigating Identity Management and Authentication Solutions Using Blockchain Technology," Available Online:https://www.researchgate.net/publication/383104615_Investigating_Identity_Management_and_Authentication_Solutions_Using_Blockchain_Technology.
8. Gopika S and Vaishnavi N” Blockchain based identity Management System”, ISSn:2456-3307, pp.1413-1420, March 2025. Available Online: https://ijsrcseit.com/index.php/home/article/view/CSEIT25112471.
9. M. Kuperberg et al., "Blockchain Usage for Government-Issued Electronic IDs: A Survey", Advanced Information Systems Engineering Workshops, pp. 155-167, 2019.
10. K. Mudliar, "A comprehensive integration of national identity with blockchain technology", International Conference on Communication information and Computing Technology (ICCICT) IEEE, pp. 1-6, 2018.

11. R. Rivera et al., "How digital identity on blockchain can contribute in a smart city environment", International Smart Cities Conference (ISC2), pp. 1-4, 2017.
12. Y. Liu et al., "Blockchain-based identity management systems: A review" in Journal of Network and Computer Applications, Elsevier Ltd., 2020.
13. R. Khan, "Blockchain based land registry system using Ethereum Blockchain", Journal of Xi'an University of Architecture & Technology, pp. 3640-3648, 2020.
14. M. Sharples and J. Domingue, "The blockchain and kudos: a distributed system for educational record reputation and reward", Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL), pp. 490-496, 2015.
15. M. Pilkington, "Blockchain technology: principles and applications" in Research Handbook on Digital Transformations, France: University of Burgundy, 2016.
16. M. Kuperberg et al., "Blockchain Usage for Government-Issued Electronic IDs: A Survey", Advanced Information Systems Engineering Workshops, pp. 155-167, 2019.
17. Karamchand, G.K(2023),” Automating Cybersecurity with Machine Learning and Predictive Analytics” Journal of Computational Innovation,3(1).
18. Govindarajan, Balaji & Eeti, Shanmukha & Goel, Om & Goel, Punit “Optimizing Dats Migration in Legacy insurance systems using Modern Techniques”, 373-400, 2023
19. K. K. Tirupati, I. Khan, L. Kumar, S. H. Kendyala, A. Kumar and S. S. Chamarthy, “Blockchain-Driven Secure Communication and Trust Management Framework for the Internet of Vehicles”, 2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART), 2024, pp.499-505, doi:10.1109/SMART63812.2024.10882534.
20. Zyskind, G., Nathan, O., & Petland, A. (2015),” Decentralized Privacy: Using Blockchain to Protect Personal Data”,2015 IEEE Security and Privacy Workshops (SPW), 180-184. DOI: 10.1109/spw.2015.27.
21. Wood, G. (2014),” Ethereum: A Secure Decentralized Generalized Transaction Ledger” Ethereum Project Yellow Paper. Available Online: https://ethereum.org/en/whitepaper/.