International Journal of Innovative Research in Engineering
Volume 6, Issue 2 (March - April 2025), PP: 111-115.
https://www.doi.org/10.59256/ijire.20240502012
www.theijire.com
ISSN No: 2582-8746

Block chain-Driven Web Authentication with Dynamic Code Generation

Gowtham Arjun[1], G. Fathima[2]
[1]*M.Sc., CFIS, Department of Computer Science and Engineering, Dr. MGR University, Chennai, Tamilnadu, India.*
[2]*Faculty, Centre for cyber forensics and information security, university of madras, Chennai, Tamilnadu, India.*

How to cite this paper:
Gowtham Arjun[1], G. Fathima[2] "Blockchain-Driven Web Authentication with Dynamic Code Generation Networks", IJIRE-V6I2-111-115.

Abstract: *As we depend more and more on online platforms, keeping user login secure is a top priority. Traditional methods, which often store usernames and passwords on central servers, are increasingly at risk from cyberattacks like data breaches, phishing scams, and identity theft. To overcome these problems, this project suggests a decentralized login system based on block chain technology. Blockchain provides a secure and transparent record where login information are managed safely without a central authority. Smart contracts enable automated checks that are resistant to tampering and unauthorized access. Unlike standard systems, this approach eliminates the single point of failure by spreading data across a blockchain network, ensuring better uptime and security. Users have more control over their online identities because blockchain-based systems avoid storing cleartext passwords or sensitive information in one location. Integrating blockchain with crypto wallets, like MetaMask, further strengthens user login by enabling secure, key-based identity checks. This method not only boosts user confidence and privacy but also fits with the future of the decentralized web (Web3). This proposed solution shows how blockchain can transform login systems by providing a secure, scalable, and transparent alternative to traditional login processes.*

Key Words: *Blockchain Technology, MetaMask, Ganache, Web3.js, Truffle, Solidity, Decentralized Storage, Smart Contracts, Time-Sensitive Codes, Hashing, Phishing, Data Integrity, Decentralized Applications (dApps)*

I.INTRODUCTION

In the digital world we live in today, security has become a top concern, especially when it comes to user authentication. Most websites and applications still use traditional login methods involving usernames and passwords. While this has been the norm for years, it is no longer reliable in protecting sensitive information. Centralized systems that store user credentials in a single database are vulnerable to hacking, leaks, and unauthorized access. If attackers breach a server, they can gain access to thousands or even millions of user accounts at once. This puts not only personal data at risk but also financial information and user trust. Even with the use of stronger password policies or two-factor authentication (2FA), the issue is not completely solved. Hackers have developed advanced methods like phishing, social engineering, and SIM swapping to bypass 2FA systems. A major concern is also password fatigue, where users tend to reuse passwords across different platforms, making all their accounts vulnerable if one is compromised [1]. According to research, most users continue to follow unsafe practices due to the complexity of managing multiple secure passwords. As online platforms grow and store increasing amounts of private data, the weaknesses of centralized systems become more visible. Therefore, there is a clear need for a more robust, decentralized approach to authentication that does not rely on trusting a single server or third party to protect identity.[2]

Blockchain technology has emerged as a powerful solution to these issues by offering a secure, decentralized method of handling digital identities. Unlike centralized systems, blockchain uses a network of nodes to verify and store information, making it almost impossible for a single point of failure to compromise the system. Data stored on the blockchain is encrypted and immutable, meaning it cannot be altered or deleted by any single entity. Smart contracts, which are self-executing programs stored on the blockchain, can automate the verification process and ensure that rules are followed exactly as programmed. This removes the need for traditional intermediaries and increases both efficiency and trust. One major advantage of blockchain-based authentication is the concept of self-sovereign identity (SSI), where users have full control over their digital identity. Instead of giving personal data to multiple platforms, users can store verifiable credentials in digital wallets and selectively share them when needed [3]. SSI protects privacy and gives individuals ownership of their identity. Large tech companies and independent organizations are already exploring this space. For example, Microsoft's ION project and the Sovrin Network are building systems where users can log in securely without relying on passwords or third-party servers [4]. As internet services become more advanced, blockchain-based authentication stands out as a secure, user-controlled, and future-ready alternative to traditional login methods.

II.LITERATURE REVIEW

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020) [5] Yang Liu, Debiao He, Mohammad S. Obaidat, Neeraj Kumar, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo conducted a comprehensive review of blockchain-based identity management systems. Their study analyzed various solutions developed between 2017 and 2020, highlighting the shift towards self-sovereign identity models. They emphasized the benefits of decentralization in enhancing user control and privacy. The paper also identified existing challenges and potential research opportunities in the field. This work serves as a valuable resource for understanding the evolution and current state of blockchain-based identity management.

Panait, A.-E., Olimid, R. F., & Stefanescu, A. (2020) [6] Andreea-Elena Panait, Ruxandra F. Olimid, and Alin Stefanescu explored the privacy and security aspects of blockchain-based identity management solutions. They analyzed ten prominent implementations, assessing their strengths and weaknesses. The study highlighted the potential of blockchain to enhance privacy but also pointed out existing challenges, such as scalability and regulatory issues. The authors concluded that while blockchain-based identity systems are promising, their widespread adoption requires further refinement. This work encourages further development and research in blockchain identity systems.

Alharbi, M., & Hussain, F. K. (2022) [7] Mekhled Alharbi and Farookh Khadeer Hussain provided a systematic review of blockchain-based identity management systems. They classified the systems based on their design and features, identifying key challenges such as scalability, interoperability, and user adoption. The paper highlighted that blockchain technology offers a more secure and user-centric approach compared to traditional identity management systems. The authors also explored future directions for research, suggesting that improved standards and frameworks could accelerate blockchain adoption in identity management.

Lim, S. Y., Fotsing, P. T., Almasri, A., et al. (2018) [8] Shu Yun Lim and colleagues conducted an in-depth exploration of blockchain technology's role in identity management and authentication services. They compared traditional and blockchain-based authentication methods, emphasizing the latter's ability to improve data control and integrity. The authors also discussed the various industries, such as banking and healthcare, where blockchain could revolutionize identity management. Despite these promising advantages, security risks and the slow pace of adoption were acknowledged as significant hurdles.

Sadhu, A. K. R. (2021) [9] Ashok Kumar Reddy Sadhu critically reviewed blockchain-based Identity and Access Management (IAM) systems, focusing on their architectural designs and real-world implementations. The study discusses key elements of blockchain, such as decentralization and cryptographic techniques, and how these features enhance security and privacy. The author identified challenges related to the adoption of these technologies, such as resistance to change and regulatory issues. The paper also provides suggestions for future research in optimizing blockchain for IAM systems.

Seyam, H., & Habbal, A. (2023) [10] H. Seyam and A. Habbal provided a systematic review of blockchain-based identity management solutions. Their research examined several decentralized authentication systems, addressing both their security and privacy benefits. The study identified key obstacles in the widespread adoption of blockchain for identity management, such as issues related to scaling and user onboarding. The authors concluded that the technology's tamper-resistance and cryptographic guarantees offer significant advantages over traditional identity management systems, urging for further research to overcome existing challenges.

Vaziry, A., Barman, K., & Herbke, P.2024 [11] Awid Vaziry, Kaustabh Barman, and Patrick Herbke reviewed on-chain identity solutions, focusing on mechanisms such as zero-knowledge proofs and public key infrastructures. The paper addressed challenges in linking digital identities to real-world entities, with an emphasis on privacy-preserving technologies. Despite significant advancements, the authors noted that bridging trust between digital and physical identities remains a major challenge. Their work highlights research gaps and urges further investigation into trusted identity solutions in the Web3 context.

III.PROPOSED METHODOLOGY

This project is about building a safe login system using blockchain instead of the usual password storage on servers. It uses a website where users log in through MetaMask, a popular crypto wallet, and confirms their actions using blockchain transactions. This way, users control their identity without needing a central server to manage passwords.

3.1 User Signup and Wallet Connection

When someone opens the website, they first connect their MetaMask wallet(fig3.1) (fig3.2). This wallet acts like their digital identity. After connecting, the user can sign up by entering a username and password(fig3.3). These details are turned into a secure format (called hashing) so the original information is hidden. Then, this hashed data is saved on the blockchain using a smart contract, with user approval through MetaMask(fig3.4). No real passwords are stored anywhere, which makes it much harder for hackers to steal them.

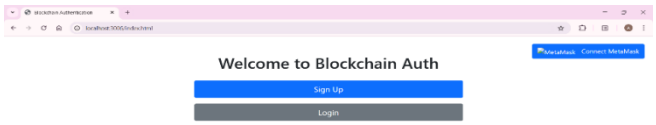

Fig 3.1

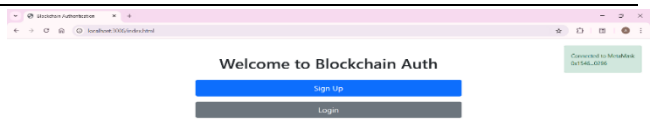

Fig 3.2

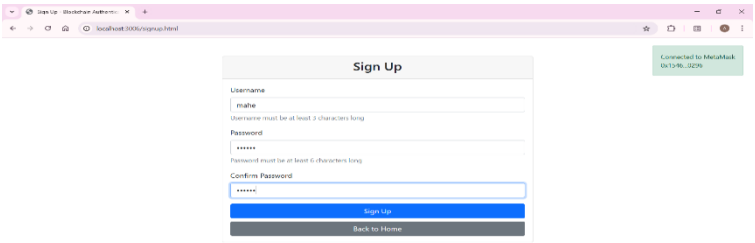

Fig 3.3

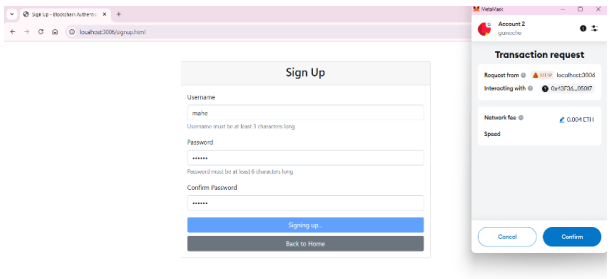

Fig 3.4

3.2 Login with Password and Blockchain Check

To log in, users enter the same username and password(fig3.5). The system checks if these matches what's stored in the blockchain (again, by comparing the hashed versions). If they match, a special 4-digit code is created through the smart contract. To get this code, the user must confirm another action in MetaMask (3.6) (3.7). This proves they own the wallet and adds an extra layer of safety to the login process.

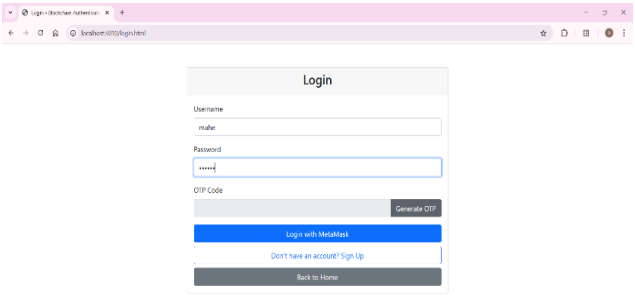

Fig 3.5

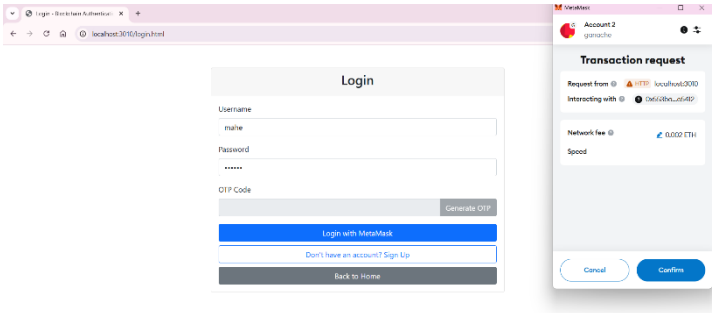

Fig 3.6

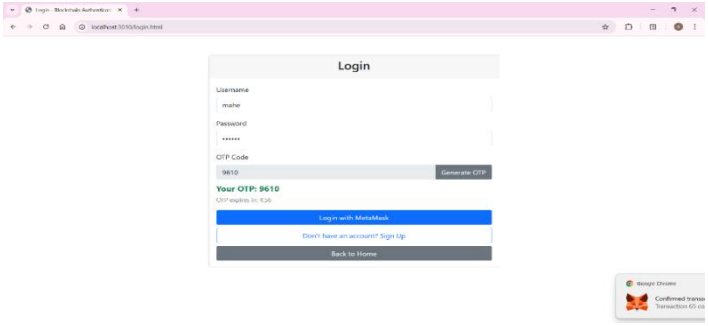

Fig 3.7

3.3 Time-Limited Code Generation

The 4-digit code created is like a temporary passcode and changes every five minutes. This helps stop anyone from reusing old codes. The smart contract takes care of this by using blockchain time, which is very reliable. Without confirming

through MetaMask, users can't see the code. This keeps the system more secure and ensures only the real user gets the code.

3.4 Final Login and Access Granting

Once the user enters the correct code, they're asked one last time to confirm their login through MetaMask(fig3.8). After this, the system checks everything: the wallet ownership, the password match, and the correct code. If all is good, the user is allowed to log in and taken to a secure logout page.

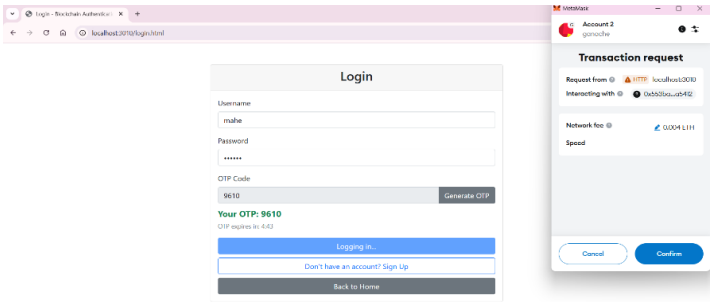

Fig 3.8

3.5 Logout and Session End

When the user clicks the logout button(fig3.9). This clears any saved temporary data like the code or login status. This means once the user logs out, no one can reuse that session. The system doesn't save anything on the browser or computer, which keeps it safe from common web threats. All the important checks happen on the blockchain, making it secure and trustworthy.

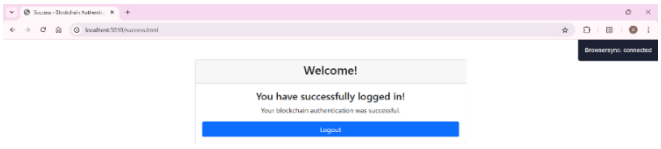

Fig 3.9

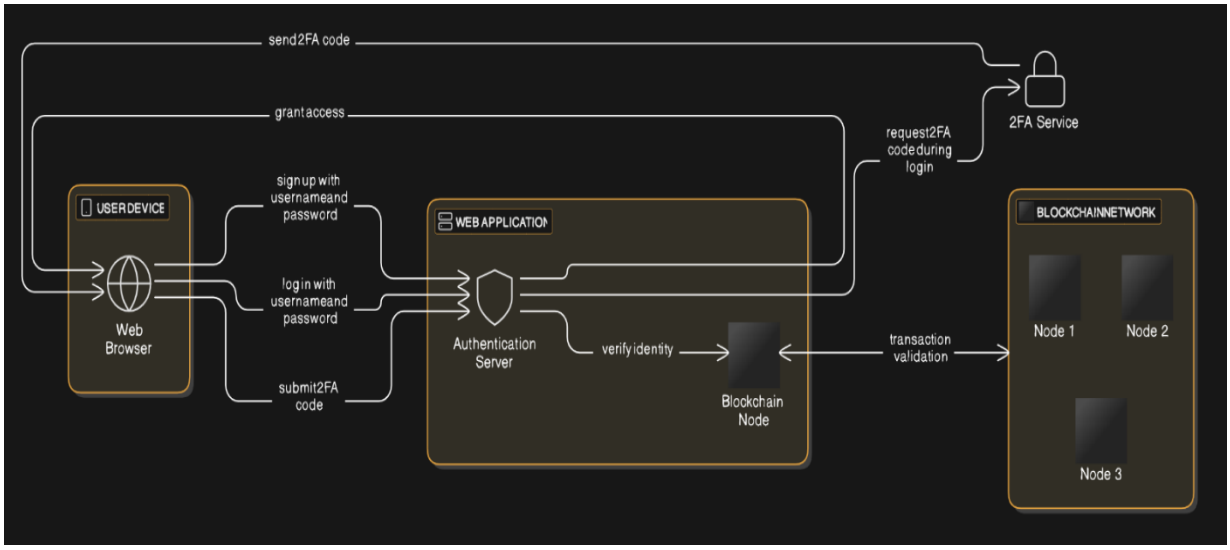

Fig 3.10 system architecture

IV.FINDINGS

The project demonstrated that using blockchain technology for web authentication offers a highly secure and user-centric alternative to traditional server-based methods. The integration of MetaMask wallets plays a crucial role in ensuring that sensitive user data is not stored in a centralized server, which is a common vulnerability in conventional authentication systems. Instead, user credentials, after being hashed, are securely stored on the blockchain, which is decentralized and

resistant to tampering. This decentralized approach minimizes the risk of data breaches, as the data is distributed across the blockchain network, making it difficult for attackers to compromise. Blockchain's immutable nature ensures the authenticity and integrity of the stored credentials, as any changes or unauthorized access attempts are easily detectable. In this way, the system offers a higher level of security than traditional centralized databases and gives users full control over their personal data.[12]

Additionally, the implementation of a dynamic 4-digit code that changes every five minutes significantly enhances the security of the authentication process [13]. This feature is similar to a time-sensitive OTP, which is designed to minimize the risk of old codes being reused or intercepted. The dynamic code is generated by a smart contract on the blockchain, linked to the user's wallet, and can only be retrieved by the wallet owner who must approve the transaction in MetaMask[14]. This provides a second layer of authentication, ensuring that only the legitimate user can access the code and complete the login process. The system's design also ensures that no sensitive data is stored on the client-side, meaning there are no risks of session hijacking through browser vulnerabilities or local storage. Once the user logs out, all temporary session data, including access codes, is cleared, further protecting against unauthorized access. This ensures that the system remains stateless, offering better privacy and security by preventing any leftover data that could be exploited. Overall, this project presents a more secure, privacy-focused, and user-controlled alternative to traditional web authentication systems.

V.CONCLUSION

In conclusion, the blockchain-based authentication system developed in this project offers a significant improvement in security and privacy compared to traditional authentication methods. By utilizing blockchain technology, user credentials are securely stored and protected through cryptographic methods, making it much harder for attackers to compromise sensitive data. Traditional centralized authentication systems, where data is stored on vulnerable servers, are prone to data breaches and hacking attacks. This new decentralized approach eliminates the need for central storage, ensuring that only the user, through their MetaMask wallet, has control over their authentication data. This design minimizes the risks associated with centralized systems, providing a much safer solution for both users and service providers.

Additionally, the dynamic generation of time-sensitive access codes enhances security by ensuring that login credentials are always changing, making it difficult for hackers to reuse or intercept the codes. The smart contract ensures that these codes are only accessible to the user, further protecting against unauthorized access. Another important aspect of this system is its stateless nature, where no sensitive data is stored on the user's device or in browser cookies, reducing the risk of session hijacking or exploitation. The overall design is not only secure but also user-friendly, as it empowers users with greater control over their data while simplifying the authentication process. The project's successful implementation demonstrates the vast potential of blockchain technology in the future of web authentication. As blockchain continues to evolve, it is likely that more websites and applications will adopt similar decentralized authentication systems, leading to a more secure, transparent, and privacy-focused digital environment for users worldwide

References

[1] Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. Information Technology for Development, 20(2), 196–213. https://doi.org/10.1080/02681102.2013.814040

[2] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni, Bubbles of Trust: A decentralized blockchain based authentication system for IoT, Computers & Security, Volume 78,2018,Pages 126-142,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.06.004.

[3] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 2020, pp. 90-95, https://doi.org/10.1109/MobileCloud48802.2020.00021.

[4] C. N. Butincu and A. Alexandrescu, "Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems," in IEEE Access, vol. 12, pp. 60928-60942, 2024, https://doi.org10.1109/ACCESS.2024.3394537.

[5] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166, 102731. https://doi.org/10.1016/j.jnca.2020.102731

[6] Panait, A.-E., Olimid, R. F., & Stefanescu, A. (2020). Identity Management on Blockchain -- Privacy and Security Aspects. arXiv preprint arXiv:2004.13107. https://arxiv.org/abs/2004.13107

[7] Alharbi, M., & Hussain, F. K. (2022). A Systematic Literature Review of Blockchain Technology for Identity Management. In Advanced Information Networking and Applications (pp. 345–359). Springer. https://doi.org/10.1007/978-3-030-99619-2_33

[8] Lim, S. Y., Fotsing, P. T., Almasri, A., et al. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), 1735–1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

[9] Sadhu, A. K. R. (2021). Reimagining Digital Identity Management: A Critical Review of Blockchain-Based Identity and Access Management (IAM) Systems - Architectures, Security Mechanisms, and Industry-Specific Applications. Advances in Deep Learning Techniques, 1(2), 1–22. https://thesciencebrigade.com/adlt/article/view/252

[10] Seyam, H., & Habbal, A. (2023). A Systematic Review of Blockchain-based Identity Management Solutions. International Conference on Recent Academic Studies, 1(1), 246–253. https://doi.org/10.59287/icras.712

[11] Vaziry, A., Barman, K., & Herbke, P. (2024). SoK: Bridging Trust into the Blockchain. A Systematic Review on On-Chain Identity. arXiv preprint arXiv:2407.17276. https://arxiv.org/abs/2407.17276

*[12]Kamboj, P., Khare, S. & Pal, S. User authentication using Blockchain based smart contract in role-based access control. Peer-to-Peer Netw. Appl. **14**, 2961–2976 (2021). https://doi.org/10.1007/s12083-021-01150-1*

[13]Bianchi, G., Valeriani, L. (2023). Time Is on My Side: Forward-Replay Attacks to TOTP Authentication. In: Arief, B., Monreale, A., Sirivianos, M., Li, S. (eds) Security and Privacy in Social Networks and Big Data. SocialSec 2023. Lecture Notes in Computer Science, vol 14097. Springer, Singapore. https://doi.org/10.1007/978-981-99-5177-2_7

[14]J. P. Cruz, Y. Kaji and N. Yanai, "RBAC-SC: Role-Based Access Control Using Smart Contract," in IEEE Access, vol. 6, pp. 12240-12251, 2018, https://doi.org10.1109/ACCESS.2018.2812844