A Bridge between Blockchain and Decentralized Applications Web3 and Non-Web3 Crypto Wallets

1st Sarah Kapoor
Department of Cyber Security
Noida Institute of Engineering & Technology
Greater Noida, India
sarah.kapoor.3783@gmail.com

2nd Vishal Singh
Department of Cyber Security
Noida Institute of Engineering & Technology
Greater Noida, India
singhkush.vishal@gmail.com

3rd Sumit Sharma
Department of Cyber Security
Noida Institute of Engineering & Technology
Greater Noida, India
sssumitsssharma@gmail.com

4th Puneet Garg
Department of CSE - AI
KIET Group of Institutions
Delhi NCR, Ghaziabad
puneetgarg.er@gmail.com

5th Ankita
Department of CSE
SAITM, Gurugram
Delhi NCR, India
ankitam86@gmail.com

Abstract **- The Blockchain Revolution [1] is an illuminating, critically important manifesto for the next digital age. Blockchain and crypto have drastically altered the way people look at the Internet and finance over the years. DApps (decentralized Applications) are an interesting and socially important field that has emerged with the Blockchain revolution. In this paper, we discuss how Web3-based crypto wallet interacts with decentralized applications and how these wallets are different from Blockchain-based crypto wallets. Today, cryptos are considered an asset in this world, however, managing these assets seems to be a hassle. The paper will focus on different aspects of different wallets, both Web3 and traditional blockchain-based wallet (non-Web3), and understand the importance and functionality of each wallet. Finally, we will address the challenges and future aspects of these wallets in an increasingly decentralized network.**

The paper will revolve around crypto wallets and will explain how smart contracts act as a bridge between blockchain and decentralized applications. Furthermore, we will discuss how Web3 and decentralization can be a powerful tool for this world, if used ethically.

Keywords: Cryptocurrencies Forensics, Blockchain, Web3, Smart Contract, Crypto Wallet, Consensus Mechanism, Decentralized Applications, Cryptography

I. Introduction

The birth of bitcoin revolutionized the crypto industry. On 31 October 2008, an article was published by Satoshi Nakamoto which had the recipe of bitcoin. This paper was titled Bitcoin: A Peer-to-Peer Electronic Cash System [2] and it invented a purely peer-to-peer version of cash transactions. In the late 1980s, the concept of cryptographic digital money was introduced, but was shut down due to security issues. Presently, cryptocurrencies like Ethereum and Bitcoin are exponentially growing [3]. However, governments are still concerned with legalizing these because of their decentralized nature [4]. Cryptographic digital money has several drawbacks, including security hazards, scalability issues, and lack of regulation.

Crypto wallets are essential tools for managing crypto assets. Crypto wallets are software that manage crypto and deal with financial transactions of cryptographic digital money. Later in this article, we will understand the different types of wallets and discuss their benefits and limitations. However, before jumping to, we must understand the Public and Private keys concepts. Think of Public keys as your address on a blockchain; it is what you share when you want someone to send you crypto. The private keys are slightly different. They are connected cryptographically to a public key and act as a supersecret password for your transactions (Pro tip, you should never share your private keys) [5].

II. Web3 and its Applications

The idea of web3 and its revolution over the years has led us to digital cryptographic money. Therefore, let us understand Web3, then move on to understand the working of Web3. Web3[6] is an upcoming era of technology that focuses on decentralization and user ownership. Here, decentralization means that Web3 wants to allow users to interact with the Internet without any central entities. Web3 aims to provide partial ownership and to remove middlemen. Blockchains were invented to achieve this goal [13,19]. Blockchains provide a network or database where anyone can communicate, and every transaction is recorded. Blockchains provide transparency to users, which is a conflicting issue because the same transparency is also a security hazard [14,23,17]. However, if used ethically, blockchains can be a powerful tool for decentralization in different fields. For instance, blockchains can be

used in decentralized voting systems in democratic countries [15,18].

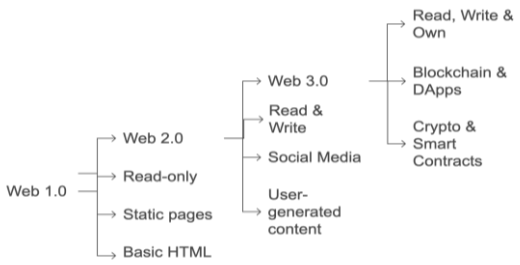

Fig 1 - Evolution of the Web

History (PoH) and Proof of Burn (PoB) [7].

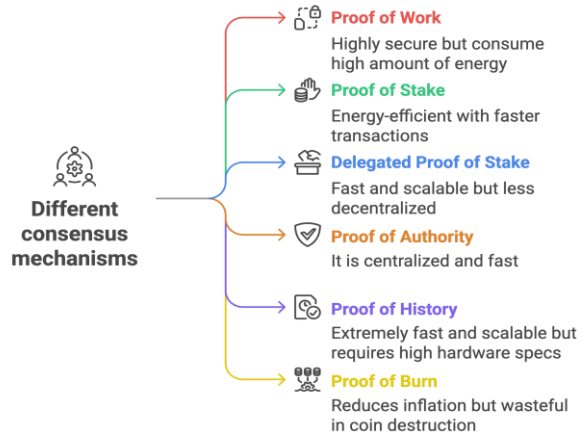

Fig 2 - Different Protocols in a Blockchain

B. Smart Contracts (Execution layer)

Smart contracts are considered a bridge between blockchains and DApps[20][27]. These are self-executable contracts with predefined rules that are encoded in the blockchain [8].

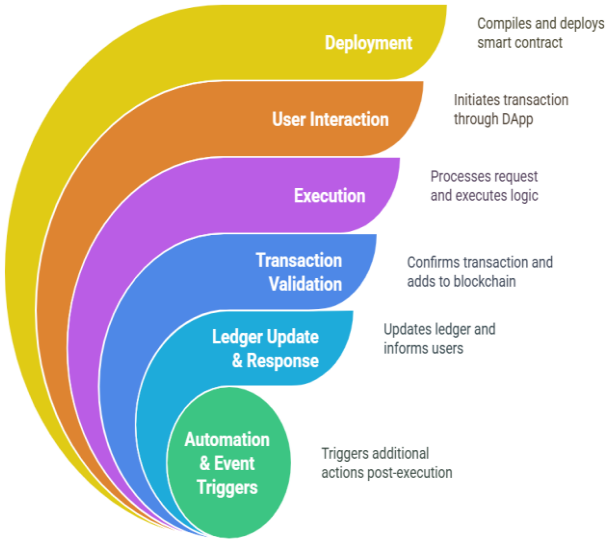

Fig 3 - Smart Contract Execution Process

This is user interaction layer [9], connects user to blockchain networks via Wallet interface. Non-custodial (Web3 wallets) are discussed in section 4.2 of this paper [22][28].

D. Decentralized Applications (DApps)

These Application runs on blockchain instead of centralized server and use smart contracts for functions like finance (DeFi), gaming(GameFi). It requires Web3 wallets to interact with users.

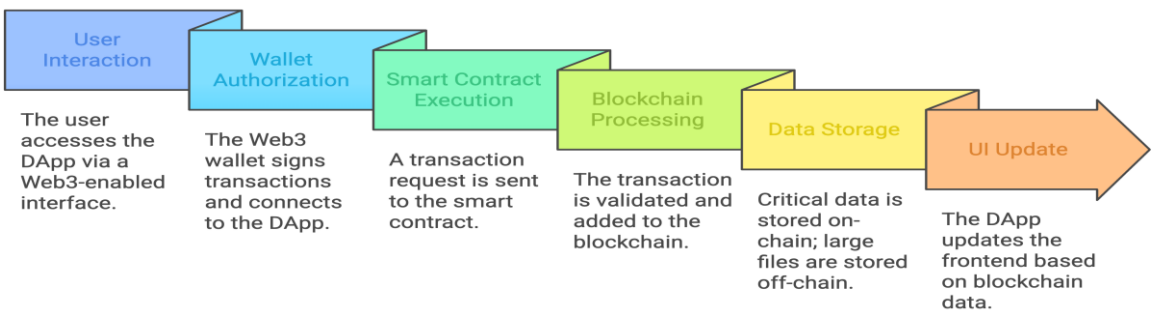

Fig 4 - DApp Functionality Sequence

IV. CRYPTO WALLET

A crypto wallet [10] is a tool that interacts with blockchain to perform transactions, think of it like your regular wallet, but it stores crypto currencies not cash [21][25]. It manages cryptographic private and public keys. Public key is an address of your crypto wallet (just like your bank account number) and private keys are used to confirm the transaction and prove your ownership of the wallet. These are like passwords and you should never share it and it's also used to recover your wallet in case you lose it. Most security breaches occur because the attacker obtains access to private keys [29].

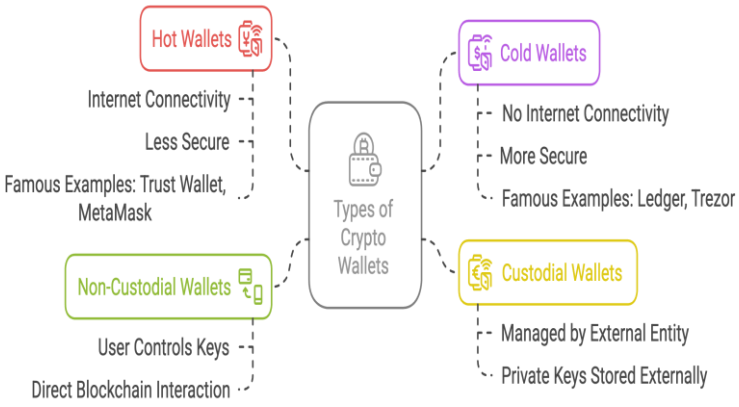

Fig 5 - Types of Crypto Wallets and Their Characteristics

A. Types of crypto wallets

1) Hot wallets (Connected to the Internet)

a) You can use it anywhere if you have an Internet connection.
b) Less secure, has higher risk of hack due to network connectivity.
c) Famous examples are Trust Wallet, MetaMask

. 2) Cold Wallets (Not Connected to Internet)

a) They are not convenient for regular use.
b) They provide better security than Hot Wallets
c) Famous examples are Ledger, Trezor (they are hardware wallets)

B. Custodial and Non-Custodial Wallets

- *Custodial Wallets*- These are Non-Web3 Wallets (aka traditional wallet). These wallets are managed by an external entity or exchange [28]. The private keys are stored in their databases and the user has no control over security. Custodial wallets are usually considered less secure.

- *Non-Custodial Wallets* – A wallet that helps users connect with Blockchain networks and interact with Dapps [27][29]. In these wallets the public and private keys are given to the user and there are no third-party applications [26]. The security of these wallets depends totally on the user and it becomes their responsibility to make sure that their private keys are safely stored.

V. *COMPARISON TABLE:*

Comparison Table

Feature	***Web3 Wallet***	***Non-Web3 Wallet***
Security	High security since private keys are stored by users. Higher risk of losing private keys.	Less security since private keys are stored by a centralized server and are prone to breaches.
Decentralization	Fully decentralized	Centralized to some extent; private keys are stored by third parties.
Control	Users have complete control over funds	Users depend on third parties for funds.
Usability	Requires blockchain understanding.	Requires a basic account set-up

VI. LITERATURE REVIEW*:*

Sno.	*Author*	*Title*	*Research focus*	*Methodology*	*Limitations*	*Reference for our study*
1.	Tom Barbereaua,Balázs Bodó b	Beyond financial regulation of crypto-asset wallet software: In search of secondary liability	The paper focuses on finding Alternative approaches for regulating noncustodial crypto wallets and explains the risks faced by users and providers.	It reviews the legal framework that the governments are using to regulate non-custodial wallets.	The primary focus of the paper are the legal aspects of regulations instead of technical issues like security management.	Introduction to blockchain and types of wallets.
2.	Deepika sharma, Martha Sucharitha	Investigating Security Flaws in Cryptocurrency Wallets and Developing Strategies to Enhance Their Security	The paper focuses on security vulnerabilities (phishing, smart contract exploits etc) in crypto wallets and explores different strategies for improving security.	The study uses security analysis to identify common attacks in cryptocurrency wallets. They categorize these attacks and offer solutions like multi-signature authentication.	The paper focuses on current attacks and does not focus on upcoming attacks that might come with the growth of blockchain technologies.	it highlights security vulnerabilities in Web3 wallets, which are useful for comparisons among different wallets.
3.	Satoshi Nakamoto	Bitcoin: A Peer to-Peer Electronic Cash System	The original theory and working of Bitcoin and decentralised digital cryptography came from this paper.	The methodology works on different consensus mechanisms like POW,POS etc.	Limitations include scalability issues, high power consumption due to complex mechanisms.	The paper gave us an introduction to blockchain and working of crypto mechanisms. The paper also gave us an understanding of how blockchains act as a bridge that supports dApps.
4.	Vitalik Buterin	Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform	The paper expands on Bitcoin's logic and creates a blockchain platform where programmers can create self-executing contracts.	Ethereum uses a similar methodology as Bitcoin. However, it also uses scripting language to execute smart contracts on the Ethereum virtual machine.	Ethereum faces challenges like network congestion, Smart contract vulnerabilities and scalability issues.	Ethereum is the foundation of DApps and Web3 wallets. Ethereum's smart contracts helps us understand why blockchain is considered a secure bridge.
5.	Wang, W., Hoang, D. T., Hu, P., & Xie, S.	Security Challenges and Opportunities in Smart Contracts	This paper discusses security vulnerabilities in smart contracts and provides strategies for enhancing security in smart contracts.	The study analyses past attacks and categorises them based on their root cause.	Smart contract upgradability is a very real issue.	Our study on Web3 wallets as a bridge to DApps benefits from understanding common vulnerabilities and best practices in smart contract security, ensuring safer interactions between users, wallets, and decentralized applications.

VII. CHALLENGES FACED

- *Security Threats:* The rise of cryptos has increased vulnerabilities such as phishing attacks, smart contract exploits, and private key losses [11].
- *Scalability issues:* With large networks like Ethereum, network congestion is a common problem.
- *High Gas Fees*: Expensive transaction fees make certain blockchains less user-friendly [12].
- Multichain wallets face interconnectivity issues while deployment because they work on different blockchains simultaneously.

VIII. CONCLUSION

Through this paper we understand how Blockchain and Web3 wallets have come a long way since 1980.This paper explains the importance and different aspects of custodial and non-custodial wallets. We understand how smart contracts act as a bridge between blockchain and decentralised applications. Despite their advantages, Web3 wallets still face challenges like security issues, scalability issues and more. We believe that these issues can be resolved with time and growth. Future research should explore solutions for these issues and that there is still a lot left to discover about blockchains and Web3.

REFERENCES

[1] Barbereau, T., & Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. Computer Law & Security Review, 49.

[2] Gupta, S., & Garg, P. (2023). Code-based post-quantum cryptographic technique: Digital signature. In Quantum-safe cryptography algorithms and approaches: Impacts of quantum computing on cybersecurity (p. 193). De Gruyter. https://doi.org/10.1515/9783110798159-014

[3] S. Houy, P. Schmid, And A. Bartel, "Security aspects of cryptocurrency wallets— A systematic literature review," Umeå University & Technical University of Munich, 2023.

[4] Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[6] Prakash, A., Avasthi, S., Kumari, P., & Rawat, M. (2023). Modern healthcare system: Unveiling the possibility of quantum computing in medical and biomedical zones. In Quantum-safe cryptography algorithms and approaches: Impacts of quantum computing on cybersecurity (p. 249). De Gruyter. https://doi.org/10.1515/9783110798159

[7] Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153-174. https://doi.org/10.20955/r.103.153-74

[8] M.C Valiente and J. Pavone, "Web3-DAO: An ontology for decentralized autonomous organizations," 2023.

[9] Wang, W., et al. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7, 22328-22370. https://doi.org/10.1109/ACCESS.2019.2896108

[10] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 1, pp. 1-34, 2020.

[11] Gautam, V. K., Gupta, S., & Garg, P. (2024, March). Automatic Irrigation System using IoT. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 100-103). IEEE. **DOI:** 10.1109/AUTOCOM60220.2024.10486085

[12] Ramasamy, L. K., Khan, F., Joghee, S., Dempere, J., & Garg, P. (2024, March). Forecast of Students' Mental Health Combining an Artificial Intelligence Technique and Fuzzy Inference System. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 85-90). IEEE. https://doi.org/10.1109/AUTOCOM60220.2024.10486194

[13] Rajput, R., Sukumar, V., Patnaik, P., Garg, P., & Ranjan, M. (2024, March). The Cognitive Analysis for an Approach to Neuroscience. In 2024 International Conference on Automation and Computation (AUTOCOM) (pp. 524-528). IEEE. **DOI:** 10.1109/AUTOCOM60220.2024.10486081

[14] Dixit, A., Sethi, P., Garg, P., Pruthi, J., & Chauhan, R. (2024, July). CNN based lip-reading system for visual input: A review. In AIP Conference Proceedings (Vol. 3121, No. 1). AIP Publishing. https://doi.org/10.1063/5.0221717

[15] Bose, D., Arora, B., Srivastava, A. K., & Garg, P. (2024, May). A Computer Vision Based Framework for Posture Analysis and Performance Prediction in Athletes. In 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) (pp. 942-947). IEEE. DOI: 10.1109/IC3SE62002.2024.10593041

[16] Singh, M., Garg, P., Srivastava, S., & Saggu, A. K. (2024, April). Revolutionizing Arrhythmia Classification: Unleashing the Power of Machine Learning and Data Amplification for Precision Healthcare. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 516-522). IEEE. **DOI:** 10.1109/CCICT62777.2024.00086

[17] Kumar, R., Das, R., Garg, P., & Pandita, N. (2024, April). Duplicate Node Detection Method for Wireless Sensors. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 512-515). IEEE. **DOI:** 10.1109/CCICT62777.2024.00085

[18] Bhardwaj, H., Das, R., Garg, P., & Kumar, R. (2024, April). Handwritten Text Recognition Using Deep Learning. In 2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 506-511). IEEE. **DOI:** 10.1109/AIST55798.2022.10065348

[19] Gill, A., Jain, D., Sharma, J., Kumar, A., & Garg, P. (2024, May). Deep learning approach for facial identification for online transactions. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 715-722). IEEE. **DOI:** 10.1109/INNOCOMP63224.2024.00123

[20] Mittal, H. K., Dalal, P., Garg, P., & Joon, R. (2024, May). Forecasting Pollution Trends: Comparing Linear, Logistic Regression, and Neural Networks. In

2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 411-419). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00074

[21] Malik, T., Nandal, V., & Garg, P. (2024, May). Deep Learning-Based Classification of Diabetic Retinopathy: Leveraging the Power of VGG-19. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 645-651). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00111

[22] Srivastava, A. K., Verma, I., & Garg, P. (2024, May). Improvements in Recommendation Systems Using Graph Neural Networks. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 668-672). IEEE. **DOI:** 10.1109/INNOCOMP63224.2024.00115

[23] Aggarwal, A., Jain, D., Gupta, A., & Garg, P. (2024, May). Analysis and Prediction of Churn and Retention Rate of Customers in Telecom Industry Using Logistic Regression. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 723-727). IEEE. **DOI:** 10.1109/INNOCOMP63224.2024.00124

[24] Mittal, H. K., Arsalan, M., & Garg, P. (2024, May). A Novel Deep Learning Model for Effective Story Point Estimation in Agile Software Development. In 2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP) (pp. 404-410). IEEE. DOI: 10.1109/INNOCOMP63224.2024.00073

[25] Arya, A., Garg, P., Vellanki, S., Latha, M., Khan, M. A., & Chhbra, G. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. Journal of Electrical Systems, 20(6s), 1051-1058. https://doi.org/10.52783/jes.2837

[26] Gupta, S., & Garg, P. (2024). Mobile Edge Computing for Decentralized Systems. Decentralized Systems and Distributed Computing, 75-88. DOI: 10.1002/9781394205127.ch4

[27] Gupta, M., Garg, P., & Malik, C. (2024). Ensemble learning-based analysis of perinatal disorders in women. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 91-105). Academic Press. https://doi.org/10.1016/B978-0-443-21889-7.00016-6

[28] Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. Artificial Intelligence and Machine Learning for Women's Health Issues, 137-150. https://doi.org/10.1016/B978-0-443-21889-7.00010-5

[29] Garg, P. (2024). Prediction of female pregnancy complication using artificial intelligence. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 17-35). Academic Press. https://doi.org/10.1016/B978-0-443-21889-7.00001-4