iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53256

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Crypto Using Web 3.0

Prof. Priyanka Abhale[1], Shubhangi Nannware[2], Dhiraj Mahajan[3], Shrikrishna Pingale[4], Neha Jadhav[5]
ALARD College of Engineering & Management
(ALARD Knowledge Park, Survey No. 50, Marunji, Near Rajiv Gandhi IT Park, Hinjewadi, Pune-411057)
Approved by AICTE. Recognized by DTE. NAAC Accredited. Affiliated to SPPU (Pune University)

Abstract: ***Web 2.0 and now Web 3.0 has created great heights in the face of the Internet industry. The distance from Web 1.0 to Web 2.0 has been covered for almost a decade. But soon after Web 2.0 a new Web 3.0 evolved which has not only raised the level of interest but also many questions among developers, users, and regulators. Do we need it at this stage, what are the forcing factors, how it is different from Web 2.0 and the Semantic Web, what are its social, moral, and security implications, is it only about personalization, all these questions have made Web 3.0 popular among its stakeholders. In this paper, the primary focus will be on the relationship between Web 2.0, Web 3.0, and the Semantic Web while the second will be on the rising security concerns about rapid and sequential Web developments. However, the changing business models in the future of Web 3.0 will also be highlighted***

I. INTRODUCTION

A. Web and It's Generaton

Web 1.0 is first version of internet i.e., World Wide Web. It was evolved in 1991 to 2004. It was just like a newspaper where we can read information but cannot share our own thoughts, ideas and cannot respond to it and was immutable. Web 1.0 sites are not interactive, visitors can only visit these sites but cannot contribute to it. Web 2.0 also known as participatory refers to websites that emphasizes usergenerated content.

It was evolved by Darcy DeNucci in 2004. Web 2.0 website allows users to interact and collaborate with each other through social media but it is not much secure as we share our personal data to websites. Companies use users data for advertisement purpose. To solve the issues in Web 2.0, Web 3.0 evolved in 2014. Work on Web 3.0 is in progress. In this the whole control of data will be on user and no one can hack it as it will be encrypted. User will data whom to show their data. Web 3.0 is seen as the next evolution of the internet.

It aims to change our current web and make it more decentralized, open, and trustworthy, giving the control over content and audience back to users.

B. Blockchain

Blockchain is a decentralized, digital ledger that records transactions on multiple computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows for secure and transparent record-keeping and helps to prevent fraud and tampering. In a blockchain system, transactions are grouped into blocks and added to a chain in a linear, chronological order. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. This creates a permanent and unchangeable record of all transactions, which can be viewed by anyone with access to the blockchain.

II. PROBLEM STATEMENT AND MOTIVATION

A. Problem Statement

Web base application having serious concern of cybersecurity worldwide because of vulnerably present in web-based applications, due to this in recent years there is a rise in cyber-attacks on web application. According to some recent Data Breach Investigations Report (DBIR) cyberattacks on web based application are rapidly increasing and only few businesses are prepared for attacks and able to defend themselves.

Because of growth in cyber attracts company has to spend extra money for security. Its costing companies around 10 trillion dollars annually by 2025, up from 3 trillion in 2015. In recent years attackers shifted their goal from big MNC to small growing businesses because they are easy to attack because of lack of security infrastructure and less cyber-security expertise. Due to this companies facing losses and spending extra money on securities.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

B. Motivation

As we conduct research on web 2.0, we got to known that web 2.0 having to much issues with it, like it use the centralize system , lack of privacy , insufficient information about what and where the data was stored, lack of data ownership, misinformation. For overcoming all of this issues we are using the web 3 , because web 3 insure that the user can own their data , it use decentralized system so that single authorities cant have full control on users data, it insure security because it integrate blockchain technology with it and there are multiple features that web 3.0 provide which are missing in web 2.0

III. OBJECTIVES OF THE STUDY

Enhance the security of the web-based application so that it will be difficult to breach the system and steal the data stored in the system. Use blockchain technology to build a secure communication method such as encryption, because blockchain creates a network chain that can not be changed, hacked, or manipulated. Implementation of Web 3 to decentralize the network which will provide greater transparency on the internet, so that everyone is the owner of their data and control their data. Thus it is difficult to access data without permission.

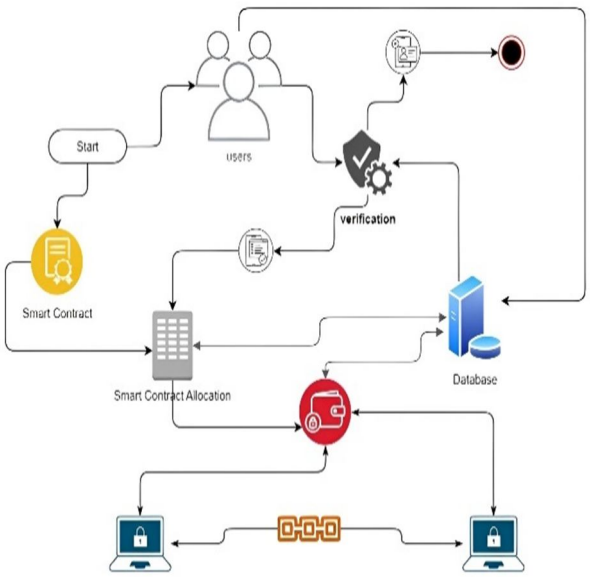
IV. SCOPE OF THE STUDY

Web 3.0 is a term used to describe the next generation of the World Wide Web, which is being developed to be more intelligent, immersive, and interactive. Web 3.0 technologies are expected to include artificial intelligence, virtual and augmented reality, and the Internet of Things (IoT). Blockchain is a distributed ledger technology that allows for the creation of secure and transparent record-keeping systems. It is decentralized, meaning it is not controlled by a single entity, and it uses cryptography to ensure the integrity and security of the data it stores. One possible scope for a project involving both web 3.0 and blockchain could be the development of a decentralized platform for securely and transparently storing and accessing data generated by IoT devices. This platform could use blockchain technology to store and verify the data, and web 3.0 technologies such as artificial intelligence and virtual reality could be used to interact with and analyse the data in meaningful ways. Another possible scope for a project involving web 3.0 and blockchain could be the creation of a decentralized marketplace for buying and selling virtual goods and services, using blockchain technology to facilitate secure and transparent transactions and web 3.0 technologies to enhance the user experience.

V. SYSTEM DESIGN

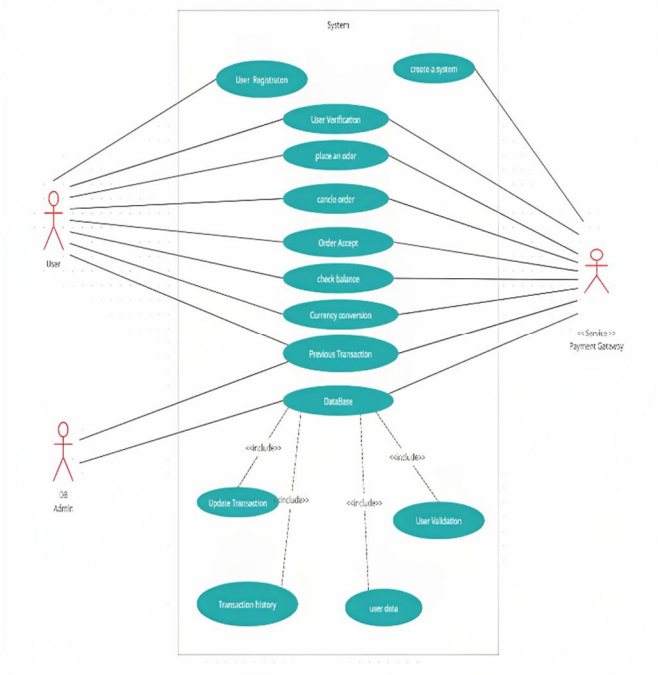
A. Project Architecrure Diagram

An architectural diagram is a visual representation that shows the physical implementation of the components of a software system. It shows the general structure of the software system and the associations, boundaries and limits between each element.



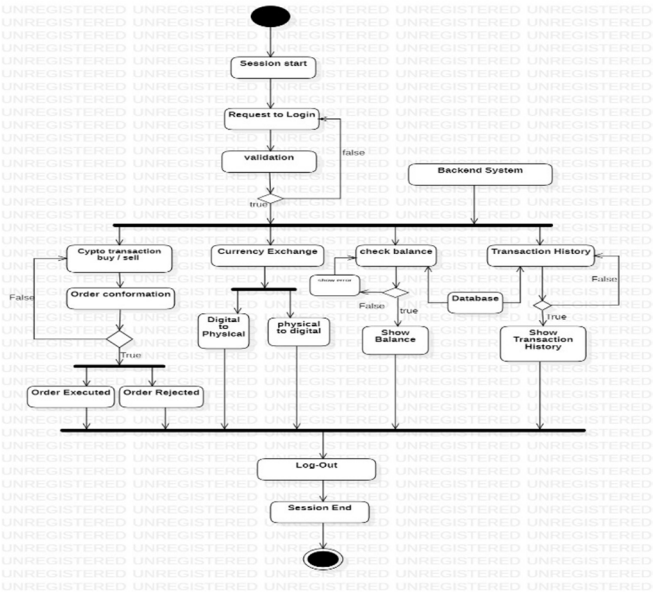
B. Use Case Diagram

Use case diagrams describe the high-level functions and scope of the system, these diagrams also identify the interactions between the system and its actors. A Use case diagram outlines how external entities user interact with an internal software system.



C. Activity Diagram crypto wallet

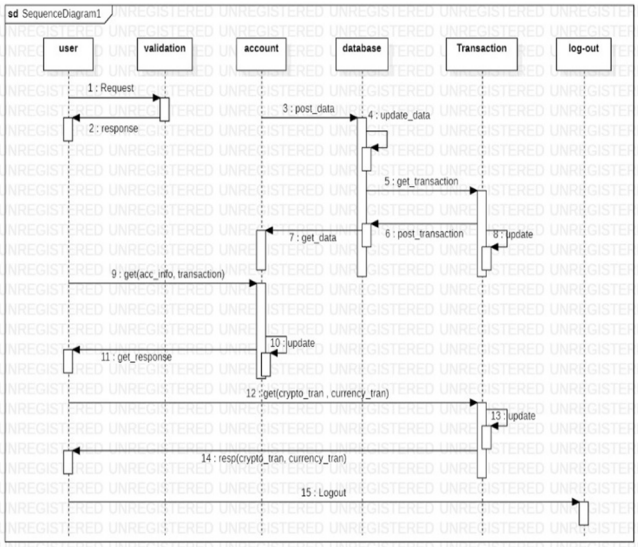
Activity diagrams are graphical representations of workflows with support for selection, repetition, and concurrency of step-by-step activities and tasks.



D. Sequence Diagram

A sequence diagram or system sequence diagram (SSD) shows process interactions arranged in time sequence in the field of software engineering It depicts the processes involved and the sequence of messages exchanged between the processes needed to carry out the functionality

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com



VI. IMPLEMENTATION

A. *MetaMask Integration*

1) Install MetaMask browser extension and set up an account.
2) Use the MetaMask JavaScript library to interact with MetaMask from your application.
3) Connect your application to the user's MetaMask wallet by requesting permission and accessing the user's Ethereum accounts.

B. *Smart Contract Development*

1) Develop your smart contracts using Solidity, the programming language for Ethereum.
2) Use a development framework like Truffle or Hardhat to compile, deploy, and test your smart contracts.
3) Define the functionality of your smart contracts, such as managing wallets, handling transactions, and interacting with external contracts.

C. *Front-End Development*

1) Build the front-end of your application using web technologies such as HTML, CSS, and JavaScript.
2) Use a JavaScript framework like React, Vue.js, or Angular to create a dynamic and interactive user interface.
3) Implement the necessary components to interact with MetaMask, such as requesting user permission, displaying wallet information, and sending transactions.

D. *MetaMask API Usage*

1) Utilize the MetaMask JavaScript library to interact with MetaMask's API.
2) Use methods like Ethereum. Request to request user permission, sign transactions, and retrieve account information.
3) Handle different events emitted by MetaMask, such as when the user connects/disconnects their wallet or changes accounts.

E. *Transaction Handling*

1) Implement the logic to create and send transactions using the user's MetaMask wallet.
2) Handle transaction signing and broadcasting to the Ethereum network.
3) Monitor transaction status and provide appropriate feedback to the user.

F. *Security Considerations*

1) Ensure that sensitive user information, such as private keys or seed phrases, is not exposed or stored insecurely.
2) Implement appropriate security measures to prevent unauthorized access or malicious activities.
3) Validate user inputs and sanitize data to prevent common security vulnerabilities, such as cross-site scripting (XSS) attacks.

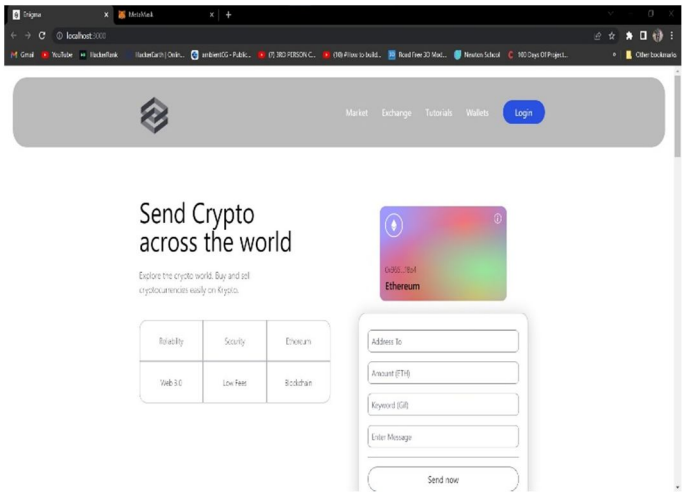
G. Testing and Deployment

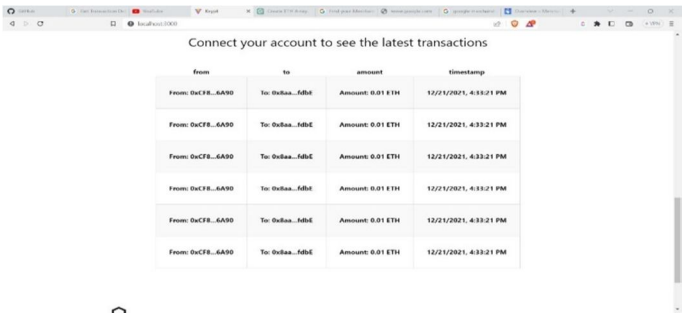
1) Thoroughly test your application, including unit tests, integration tests, and end-to-end tests.

2) Use a testing framework like Mocha or Jest to write and execute tests for your smart contracts and front-end components.

3) Prepare your application for deployment to a hosting platform or a decentralized storage system like IPFS (Interplanetary File System).

VII. RESULT





VIII. CONCLUSION

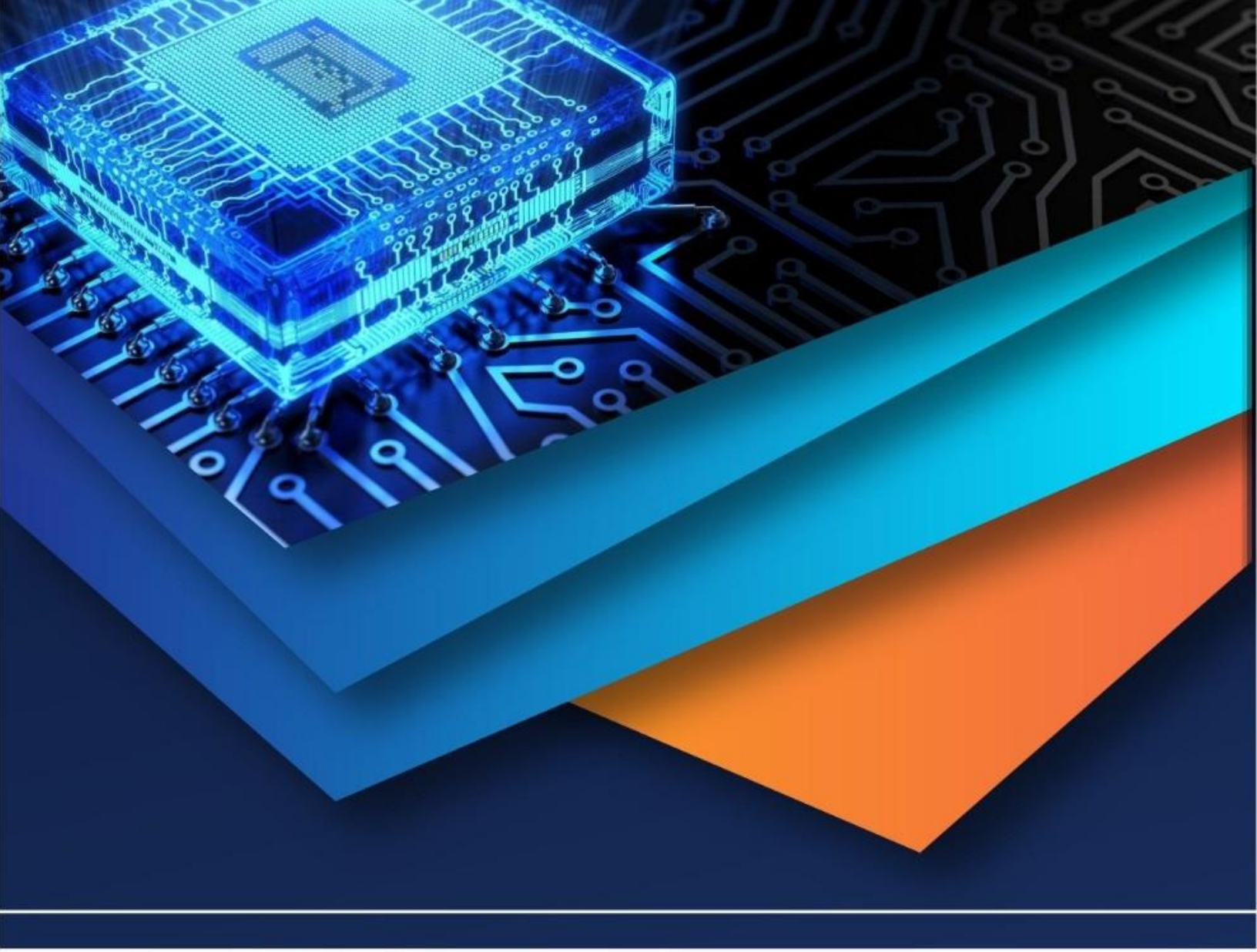
In this Project, we have successfully studied about Crypto using web3 where user can store and manage their own transactions or data. We also learned how to Use the Blockchain technology to build the secure communication method such as encryption , because block-chain create a network chain that can not be changed, hacked or manipulated. Implementation of Web 3 to decentralizes the network which will provide greater transparency on internet, so that every one is owner of their data and control their data. Thus it is difficult to access data without permission. we provided the first generic and measurable definition for Web3.0 based on our observations and analysis of the blockchain infrastructure evolution. Within this definition, we articulate three key infrastructural enablers: individual smart-contract capable blockchains, federated or centralized state publishers, and interoperability platforms to hyper connect those isolated systems. Then, we presented Hyper Service, the first interoperability platform usable in the era of Web3.0.

IX. ACKNOWLEDGEMENT

This paper was supported by Alard College of Engineering & Management, Pune 411057. We are very thankful to all those who have provided us valuable guidance towards the completion of this Seminar Report on “Crypto Using Web 3.0 Using Block chain” as part of the syllabus of our course. We express our sincere gratitude towards the cooperative department who has provided us with valuable assistance and requirements for the system development. We are very grateful and want to express our thanks to Prof. Shuchi Goplani for guiding us in the right manner, correcting our doubts by giving us their time whenever we required, and providing their knowledge and experience in making this project.

REFERENCES

[1] P. Gazi, A. Kiayias, and D. Zindros, “Proof-of-stake Sidechains, “in IEEE Symposium on Security & Privacy, 2019.
[2] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, 2014.
[3] “Bitcoin Wiki: Atomic Cross-Chain Trading,” https://en.bitcoin. it/wiki/Atomic_swap, Accessed on 2019.
[4] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, “Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing,” in USENIX Security Symposium, 2016.
[5] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin NG: A Scalable Blockchain Protocol,” in USENIX NSDI, 2016.
[6] J. Wang and H. Wang, “Monoxide: Scale out blockchains with asynchronous consensus zones,” in USENIX NSDI, 2019.
[7] M. Zamani, M. Movahedi, and M. Raykova, “RapidChain:ScalingBlockchain via Full Sharding,” in ACM CCS, 2018.
[8] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “OmniLedger: A Secure, Scale-out, Decentralized Ledger via Sharding,” in IEEE Symposium on Security and Privacy, 2018.
[9] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, “Chainspace: A Sharded Smart Contracts Platform, ”NDSS, 2017.
[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts,” in IEEE Symposium on Security and Privacy, 2016.
[11] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. M. John- son, A. Juels, A. Miller, and D. Song, “Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution,” in IEEE EuroS&P,2019.
[12] J. Krupp and C. Rossow, “teEther: Gnawing at Ethereum to Automatically Exploit Smart Contracts,” in USENIX Security Symposium, 2018.
[13] L. Breidenbach, I. Cornell Tech, P. Daian, F. Tramer, and A. Juels, “Enter the Hydra: Towards Principled Bug Bounties and ExploitResistant Smart Contracts,” in 27th USENIX Security Symposium, 2018.
[14] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” in ACM CCS, 2016.
[15] H. Wu, W. Zheng, A. Chiesa, R. A. Popa, and I. Stoica, “DIZK: A Distributed Zero Knowledge Proof System,” in USENIX Security Symposium, 2018.
[16] F. Zhang, D. Maram, H. Malvai, S. Goldfeder, and A. Juels, “DECO: Liberating web data using decentralized oracles for TLS,” in ACM SIGSAC CCS, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY