SENDKRYPT – AN APPLICATION FOR SECURE ETHEREUM TRANSACTION

[1]T.T. Mathangi, [2]R. B. Supraja, [3]M. Subasri, [4]K.G. Niveetha

[1]Assistant Professor, [2,3,4]UG Students
Information Technology
K.L.N. College of Engineering
Pottapalayam, India

***Abstract*- Blockchain technology has been widely acknowledged for its potential to enhance trust, security, transparency, and data traceability within business networks. Transactions that occur through blockchain are immutable, meaning they cannot be altered. Web 3.0, also known as the third generation of the World Wide Web (WWW), is a decentralized network with blockchain technology at its core. This enables an expanding range of new applications and services. Solidity is an object-oriented, high-level language used for implementing smart contracts Smart contracts refer to programs that are stored on a blockchain and are designed to execute automatically when specific pre-defined conditions are fulfilled. MetaMask is a software cryptocurrency wallet that allows users to interact with the Ethereum blockchain. The frontend of this web application uses the React JavaScript library to create interactive user interfaces. The application allows users to send transactions through the blockchain in an efficient and user-friendly manner.**

I. INTRODUCTION

In an era where trust and transparency are paramount in business transactions, blockchain technology emerges as a beacon of reliability, offering unparalleled security and data integrity across diverse networks. It is within this transformative landscape that our project embarks on a mission to redefine the intersection of web applications and blockchain technology. At its core, our endeavor seeks to seamlessly integrate React JS, a leading UI component library, with the robust capabilities of blockchain technology, particularly Ethereum. Leveraging MetaMask for secure communication on the blockchain platform, our web application empowers users to initiate transactions and engage in seamless communication, all while enjoying the benefits of enhanced security and efficiency. Our primary objective revolves around the seamless fusion of React JS with blockchain technology, enabling users to execute transactions with ease and confidence. By bridging the gap between anonymous and identified parties, our web application streamlines business and trade interactions, often eliminating the need for intermediaries and facilitating smoother, more efficient transactions. In the broader context of the internet's evolution, our project aligns with the principles of Web 3.0, a paradigm shift driven by decentralized technologies such as blockchain. Unlike traditional web platforms, which rely on centralized services, Web 3.0 operates in a decentralized manner, empowering individuals to own and govern segments of the internet. Central to our project's functionality are smart contracts, self-executing programs residing on blockchains that automate predefined rules and conditions. These contracts, distinguished by their autonomy and decentralization, transcend traditional currency transactions, paving the way for trustless interactions between parties. Ethereum serves as the cornerstone of our project, providing both a platform and a programming language for the creation and dissemination of decentralized applications. With its Turing-complete language and virtual machine, Ethereum enables the execution of diverse cryptocurrency projects and smart contracts, facilitating seamless program execution across the network.

Complementing Ethereum is MetaMask, a cryptocurrency wallet software that enables users to securely interact with the blockchain. By providing a user-friendly interface for accessing Ethereum wallets and engaging in decentralized application transactions, MetaMask plays a crucial role in facilitating secure connections and transactions on our platform. Underpinning the development of smart contracts is Solidity, an object-oriented, high-level language designed for crafting blockchain-based programs. With its fusion of networking, assembly language, and web development conventions, Solidity provides a powerful tool for realizing the full potential of smart contracts. Finally, React JS emerges as the backbone of our project's frontend, enabling the creation of interactive and user-friendly applications for various platforms. By dispensing with specialized template languages and empowering developers to build UI components using JavaScript, React JS facilitates a seamless and intuitive user experience for executing transactions through the blockchain. In summary, our project represents a convergence of cutting-edge technologies aimed at revolutionizing the way transactions are conducted and business processes are streamlined in the digital age. By seamlessly integrating React JS with blockchain technology, we aspire to unlock new possibilities for trust, transparency, and efficiency in the global marketplace.

II. RELATED WORKS

1. WEI CAI, ZEHUA WANG, JASON B.ERNST, ZHEN HONG,AND VICTOR C.M. LEUNG, "Decentralized Applications: The Blockchain-Empowered Software System", IEEE Access 10.1109/ACCESS.2018.2870644

This paper traces the development of blockchain systems to reveal the importance of decentralized applications (DApps) and the future value of blockchain. In this paper they survey the state-of-the-art DApps and discuss the direction of blockchain development to fulfill the desirable characteristics of DApps.

2. SATPAL SINGH KUSHWAHA, SANDEEP JOSHI, DILBAG SINGH, MANJIT KAUR, AND HEUNG-NO LEE, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract", IEEE Access 10.1109/ACCESS.2021.3140091

In this paper, a systematic review of the security vulnerabilities in the Ethereum blockchain was presented. The main objective of this paper is to discuss Ethereum smart contract security vulnerabilities, detection tools, real life attacks and preventive mechanisms. Various future directions were also discussed in the field of the Ethereum blockchain-based smart contract that can help the researchers to set the directions for future research in this domain.

3. PEILIN ZHENG, ZIGUIJIANG, JIAJING WU, ZIBINZHENG, " Blockchain-Based Decentralized Application: A Survey", IEEE Open Journal of the Computer Society 10.1109/OJCS.2023.3251854

This paper provides a comprehensive overview of DApps for further research. First, the definitions and typical architectures of DApps were presented. Then they categorize them into different types, and summarize their typical advantages and challenges. Finally, they provide an overview of the recent research problems of DApps from the perspectives of economics, security, and performance and then figure out promising research opportunities in the future.

4. CANGHAI WU, JIE XIONG, HUANLIANG XIONG, YINGDING ZHAO, AND WENLONG YI, "A Review on Recent Progress of Smart Contract in Blockchain", IEEE Access 10.1109/ACCESS.2022.3174052

This article briefly summarizes the development process of blockchain, and then focuses on the research progress of blockchain 2.0-smart contracts. Second, the related concepts of smart contracts were presented, and the working mechanism of smart contracts and the difficulties faced by smart contracts were elaborated. Finally, in response to these problems and dilemmas, the corresponding solutions and ideas were summarized, and the future challenges and development trends of smart contracts were analyzed and judged.

III. PROBLEM STATEMENT

In the realm of Ethereum transactions, complex processes and a lack of user-friendly interfaces pose significant challenges. Our project seeks to address these issues by seamlessly integrating MetaMask wallet functionality, thus enhancing user security, simplify transaction processes.

IV. METHODOLOGY

User Wallet Creation with MetaMask

User Wallet Creation with MetaMask To begin utilizing the system, users are required to create a wallet using MetaMask. MetaMask is a popular Ethereum wallet that operates as a browser extension. It provides a secure and convenient interface for users to manage their Ethereum funds and interact with decentralized applications. The wallet creation process involves generating a unique cryptographic key pair, consisting of a public address and a private key. These keys serve as the user's digital identity and enable secure transactions on the Ethereum network.

Selection of Test Network

Selection of Test Network Upon wallet creation, users can select a test network to operate on. The system offers several options for test networks, including Robsten Test Network, Kovan Test Network, Rinkeby Test Network, and Goerli Test Network. These test networks replicate the functionality of the main Ethereum network but operate with test tokens instead of real Ether. This allows users to experiment and test their transactions without incurring any real financial costs or affecting the live Ethereum network.

Addition of Dummy Ethers to the Wallet

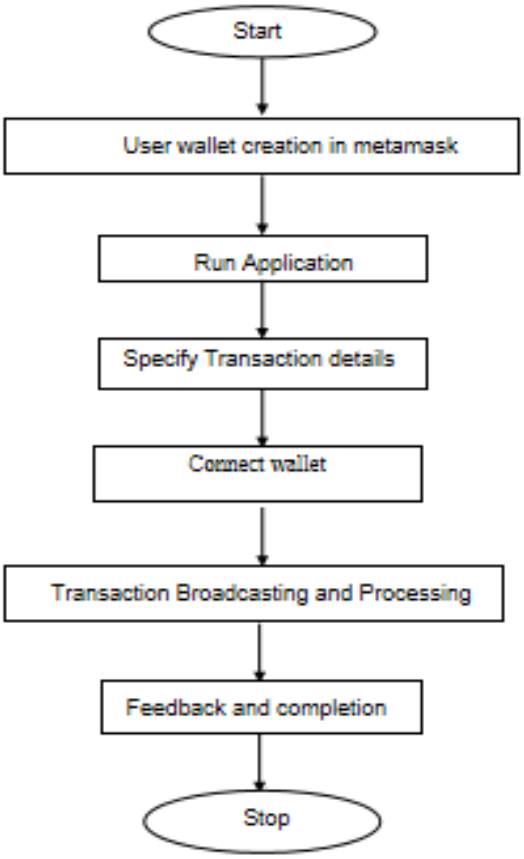
Addition of Dummy Ethers to the Wallet In order to conduct transactions within the test network, users are required to add dummy Ethers to their MetaMask wallet. These dummy Ethers serve as the test currency for executing transactions on the selected test network. By adding dummy Ethers, users can simulate real-world transaction scenarios and assess the functionality and efficiency of the system without risking actual funds.

Specification of Transaction Details and Metamask Integration

Specification of Transaction Details To initiate an Ethereum transaction, users need to specify certain details. These details include the "from" address, which represents the sender's Ethereum address, the "to" address, which denotes the recipient's Ethereum address, and the value of the transaction, indicating the amount of Ether to be transferred. This step ensures that the transaction is properly directed and accurately reflects the intended transfer of funds between users.

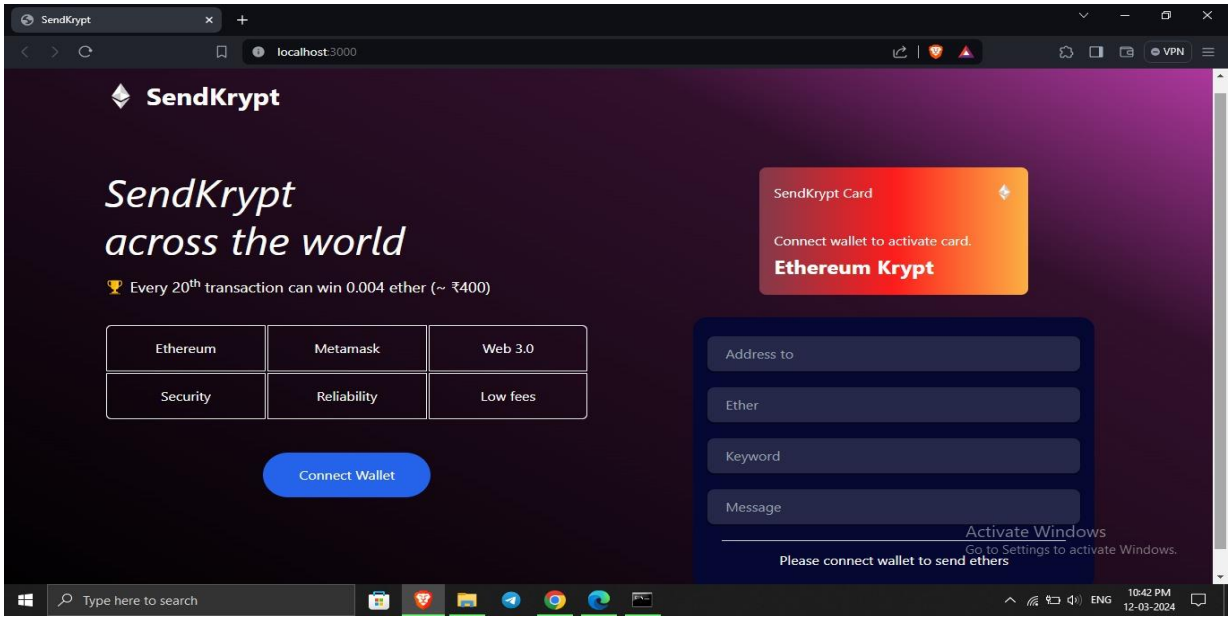
Transaction Broadcasting and Feedback

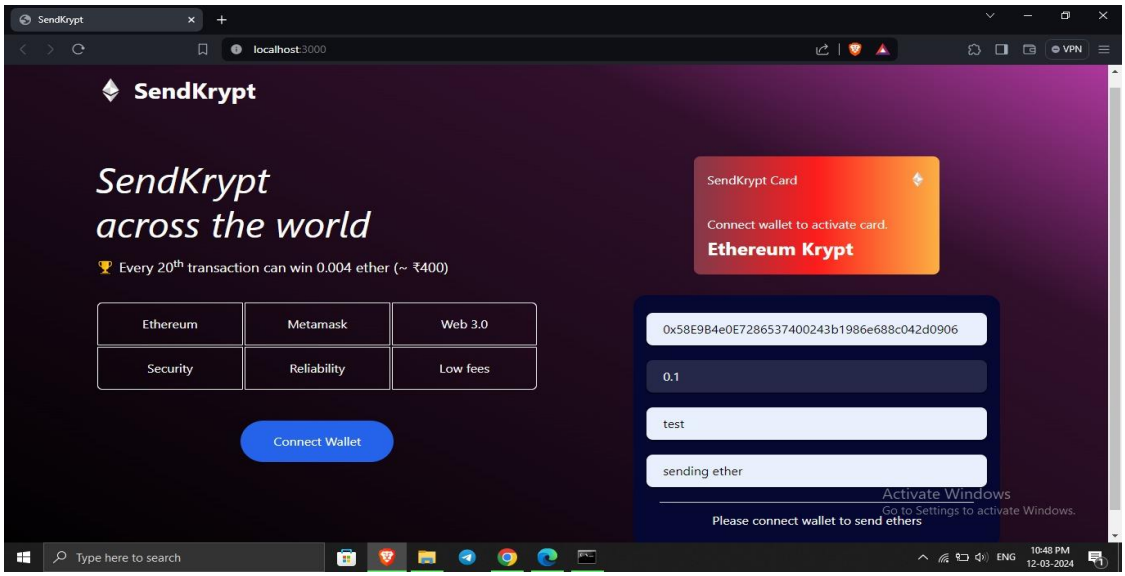
Handling of Transaction Parameters by MetaMask Several transaction parameters are handled by MetaMask to facilitate smooth and secure transactions. One such parameter is the nonce. In Ethereum, each transaction is assigned a unique nonce, which ensures that the transaction can only be processed by the blockchain once. This nonce value prevents duplicate or fraudulent transactions from being executed.

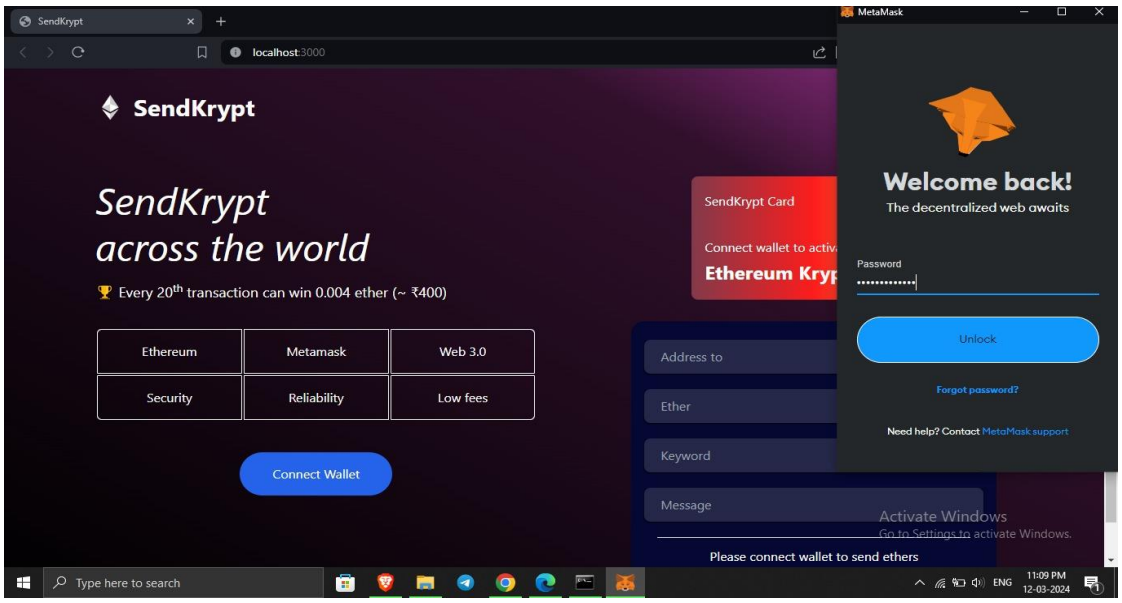


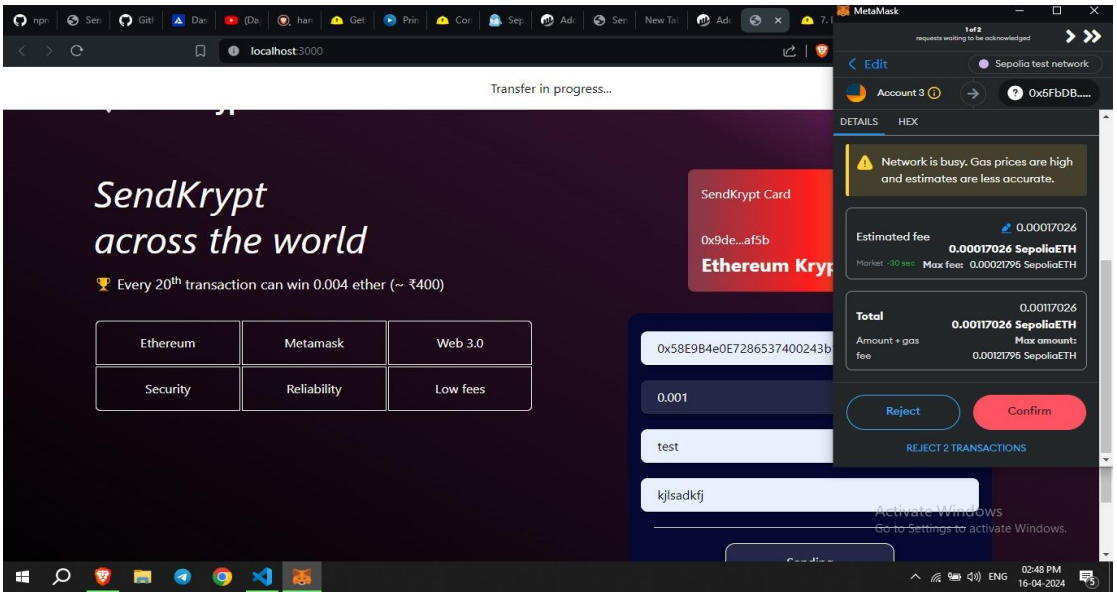
Flow Diagram

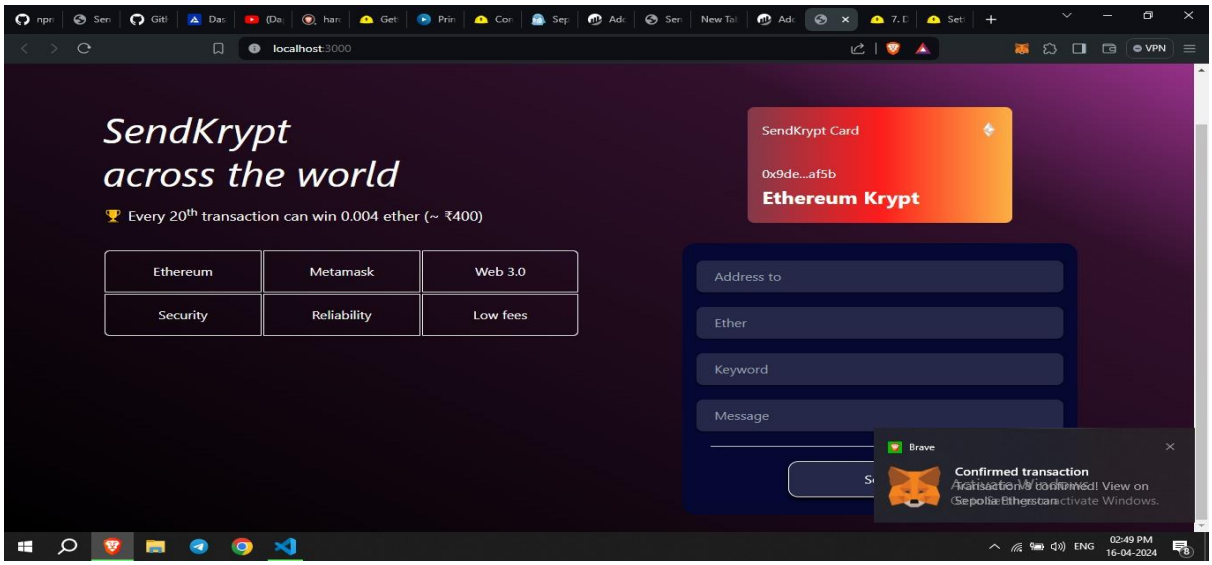
V. OUTPUT SCREENSHOTS




SendKrypt
localhost:3000
SendKrypt
SendKrypt across the world
Every 20th transaction can win 0.004 ether (~ ₹400)
Ethereum
Metamask
Web 3.0
Security
Reliability
Low fees
Connect Wallet
SendKrypt Card
Connect wallet to activate card.
Ethereum Krypt
0x58E9B4e0E7286537400243b1986e688c042d0906
0.1
test
sending ether
Please connect wallet to send ethers
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
10:48 PM
12-03-2024


SendKrypt
localhost:3000
SendKrypt
SendKrypt across the world
Every 20th transaction can win 0.004 ether (~ ₹400)
Ethereum
Metamask
Web 3.0
Security
Reliability
Low fees
Connect Wallet
SendKrypt Card
Ethereum Kryp
Address to
Ether
Keyword
Message
Please connect wallet to send ethers
Activate Windows
Go to Settings to activate Windows.
MetaMask
Welcome back!
The decentralized web awaits
Password
Unlock
Forgot password?
Need help? Contact MetaMask support
Type here to search
ENG
11:09 PM
12-03-2024


localhost:3000
Transfer in progress...
SendKrypt
SendKrypt across the world
Every 20th transaction can win 0.004 ether (~ ₹400)
Ethereum
Metamask
Web 3.0
Security
Reliability
Low fees
SendKrypt Card
0x9de...af5b
Ethereum Kryp
0x58E9B4e0E7286537400243b
0.001
test
kjlsadkfj
MetaMask
Edit
Sepolia test network
Account 3
0x5FbDB.....
DETAILS
HEX
Network is busy. Gas prices are high and estimates are less accurate.
Estimated fee
0.00017026
0.00017026 SepoliaETH
Max fee: 0.00021795 SepoliaETH
Total
0.00117026
0.00117026 SepoliaETH
Amount + gas fee
Max amount:
0.00121795 SepoliaETH
Reject
Confirm
REJECT 2 TRANSACTIONS
Activate Windows
Go to Settings to activate Windows.
ENG
02:48 PM
16-04-2024



VI. RESULT AND CONCLUSION

To sum up, our project leverages blockchain's benefits to ensure trust and transparency in Ethereum transactions. By integrating with MetaMask wallets, we bridge the gap between users and the Ethereum blockchain, offering a secure and user-friendly platform for managing Ethereum transactions.

VII. FUTURE ENHANCEMENT

Integrating additional features into the platform, such as support for different cryptocurrencies beyond Ethereum, thereby expanding its utility and appeal to a broader user base.Enabling Multi-Factor Authentication(MFA) adds an extra layer of security by requiring users to provide authentication such as one-time passcodes sent via SMS or email before accessing their accounts.

REFERENCES:

[1] WEI CAI, ZEHUA WANG, JASON B.ERNST, ZHEN HONG,AND VICTOR C.M. LEUNG,"Decentralized Applications: The Blockchain-Empowered Software System", IEEE Access 10.1109/ACCESS.2018.2870644

[2] Jianfei Zhou, Tianxing Jiang, Haijun Wang, Meng Wu, Ting Chen, "DAppHunter: Identifying Inconsistent Behaviors of Blockchain-based Decentralized Applications", IEEE 0.1109/ICSE-SEIP58684.2023.00008

[3] ANDREA PINNA, SIMONA IBBA, GAVINA BARALLA, ROBERTO TONELLI, AND MICHELE MARCHESI, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics", IEEE Access 10.1109/ACCESS.2019.2921936

[4] Peilin Zheng, Ziguijiang, Jiajing Wu, ZibinZheng, "Blockchain-Based Decentralized Application: A Survey", IEEE Open Journal of the Computer Society 10.1109/OJCS.2023.3251854

[5] XIAO FAN LIU, XIN-JIAN JIANG, SI-HAO LIU, CHI KONG TSE,"Knowledge Discovery in Cryptocurrency Transactions: A Survey", IEEE Access 10.1109/ACCESS.2021.3062652

[6] LEO BESANCON, CATARINA FERREIRA DA SILVA, PARISA GHODOUS, JEAN-PATRICK GELAS, "A Blockchain Ontology for DApps Development", IEEE Access 10.1109/ACCESS.2022.3173313

[7] SARWAR SAYEED, HECTOR MARCO-GISBERT, TOM CAIRA, "Smart Contract: Attacks and Protections", IEEE Access 10.1109/ACCESS.2020.2970495

[8] SATPAL SINGH KUSHWAHA, SANDEEP JOSHI, DILBAG SINGH, MANJIT KAUR, HEUNG-NO LEE, "Ethereum Smart Contract Analysis Tools: A Systematic Review", IEEE Access 10.1109/ACCESS.2022.3169902

[9] Niclas Kannengieser, Sebastian Lins, Christian Sander, Klaus Winter, Hellmuth Frey, and Ali Sunyaev, "Challenges and Common Solutions in Smart Contract Development", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 48, NO. 11, NOVEMBER 2022

[10] SATPAL SINGH KUSHWAHA, SANDEEP JOSHI, DILBAG SINGH, MANJIT KAUR, AND HEUNG-NO LEE, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract", IEEE Access 10.1109/ACCESS.2021.3140091