NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

SMART CONTRACTS AND SECURE TRANSACTIONS : A BLOCKCHAIN ECOMMERCE FRAMEWORK

Jonathan Cardoz

Dept. of Electronics & Telecommunication
Xavier Institute of Engineering
Mumbai, India
202002001.jonathancjj@student.xavier.ac.in

Prithvi Gawade

Dept. of Electronics & Telecommunication
Xavier Institute of Engineering
Mumbai, India
202002002.prithvighv@student.xavier.ac.in

Chirac Parmar

Dept. of Electronics & Telecommunication
Xavier Institute of Engineering
Mumbai, India
202002034.chiracphs@student.xavier.ac.in

Prof. Smita Pawar

(Project Guide)
Dept. of Electronics & Telecommunication
Xavier Institute of Engineering
Mumbai, India
smita.p@xavier.ac.in

Rana Gaikwad

Dept. of Electronics & Telecommunication
Xavier Institute of Engineering
Mumbai, India
202002010.ranagds@student.xavier.ac.in

***Abstract*—This project introduces an innovative E-Commerce platform leveraging blockchain technology, specifically built on the Ethereum blockchain. The system employs a decentralized architecture, integrating Smart Contracts written in Solidity for secure and transparent transactions. Key technologies such as Metamask, React, Solidity, HardHat, and NodeJS are utilized, with Ethereum's native cryptocurrency, Ether, serving as a primary component. The decentralized nature of the blockchain ensures immutability and transparency, fostering trust between buyers and sellers. Smart Contracts automate and secure business logic, enabling seamless transactions without intermediaries. The user-friendly interface, developed with React, enhances the overall user experience. Metamask integration provides secure wallet management, facilitating seamless user interaction with the Ethereum blockchain. The backend, powered by NodeJS, ensures scalability and efficiency for various aspects of the E-Commerce platform. Adhering to best practices, the development process utilizes the HardHat environment for Ethereum smart contracts, ensuring a robust and reliable codebase for enhanced security. In summary, this project exemplifies the transformative potential of blockchain technology in decentralizing and creating trust in traditional E-Commerce. By combining Ethereum, Smart Contracts, and a modern tech stack, including React, Metamask, Solidity, HardHat, and NodeJS, the resulting platform offers users a secure, transparent, and efficient online shopping experience.**

Keywords—Blockchain, E-Commerce,Smart Contact, Ether, Metamask

INTRODUCTION

This project endeavors to revolutionize the landscape of ecommerce by integrating blockchain technology. Recognizing the challenges of trust, security, and transparency in traditional online marketplaces, the study aims to leverage blockchain's decentralized and immutable characteristics to create a secure and trustworthy ecommerce platform. The paper will explore the conceptual framework, design principles, and technical architecture of the proposed blockchain-based ecommerce website, emphasizing its potential to enhance security, transparency, and user empowerment. The goal is to contribute to the discourse on the transformative impact of blockchain in ecommerce, envisioning a future where digital transactions are characterized by increased trust and transparency..

MOTIVATION & BACKGROUND

◦ *Motivation*

The motivation behind developing a blockchain-based ecommerce website is rooted in the imperative to revolutionize the current landscape of online commerce. By harnessing the transformative potential of blockchain technology, this project seeks to address the persistent challenges of trust, security, and transparency in traditional ecommerce platforms. The immutable ledger and decentralized nature of blockchain promise to instill

unparalleled levels of security and transparency, mitigating concerns related to data manipulation, fraud, and disputes. By introducing features like smart contracts for trustless transactions and creating an immutable product history, the project aims to redefine the dynamics of online transactions, offering users a more secure, reliable, and empowering ecommerce experience. Through the fusion of cutting-edge blockchain technology with ecommerce, the project aspires to pave the way for a future where digital transactions are characterized by heightened trust, efficiency, and global accessibility.

- *Background*

Traditional e-commerce platforms face challenges such as data breaches, payment disputes, and a lack of transparency. The introduction of blockchain technology addresses these issues by providing a decentralized, secure, and transparent framework for conducting transactions. This project aims to leverage the unique features of blockchain to revolutionize the e-commerce industry. The use of a blockchain ledger ensures that all transactions are recorded in a tamper proof manner, enhancing the integrity of the platform. Smart contracts automate and en force agreements, reducing the need for intermediaries and streamlining the transaction process. This not only improves efficiency but also lowers costs for both buyers and sellers. Additionally, by incorporating tokenization, the project can introduce a new layer of flexibility and ownership in e-commerce. Users can tokenize assets, facilitating fractional ownership and enabling a more diverse range of transactions. 2 The global nature of blockchain allows for seamless international transactions, eliminating barriers associated with currency conversions and traditional banking systems. This project envisions creating a truly global e-commerce ecosystem that is accessible to users around the world.

OBJECTIVES

- *To Create Secure Platform*

Develop a robust blockchain-based platform that ensures secure transactions, data integrity, and protection against fraudulent activities market..

- *To Implement Transparent Transactions*

Utilize blockchain's decentralized ledger to enable transparent and tamper-proof transac tion records, fostering trust between buyers, sellers, and the platform .

- *To Enable Secure Payments*

Integrate secure cryptocurrency and traditional payment methods, allowing customers to transact seamlessly while leveraging the benefits of blockchain's secure payment infrastructure. .

- *To Establish Provenance Tracking:*

Implement a traceability system powered by blockchain to track the provenance of each product providing buyers with detailed historical information about the components they purchase.

- *To Ensure Data Privacy*

Prioritize user data privacy by implementing advanced encryption and decentralization techniques, giving users full control over their personal information.

LITERATURE REVIEW

In conducting the literature review for our project, we delved into several IEEE papers to acquire a comprehensive understanding of the current state-of-the-art in the relevant field. These IEEE publications served as invaluable resources, offering insights into key methodologies, technological advancements, and theoretical frameworks that informed and guided the development of our project. By synthesizing information from these rigorously peer-reviewed sources, we aimed to ensure the robustness and validity of our approach, aligning our work with established research and fostering a foundation of knowledge that enhances the credibility and innovation of our project. The wealth of knowledge gleaned from these IEEE papers not only facilitated a nuanced comprehension of the existing literature but also inspired creative solutions and methodologies, positioning our project within the broader context of cutting-edge research in the field.

Paper Title	Author	Year	Summary	Advantages	Disadvantages
IEEE ACCESS SPECIAL SECTION EDITORIAL: Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies	1.Debiao He 2.Kim-Kwang Raymond Choo 3.Neeraj Kumar 4.Aniello Castiglione	2018.	The paper reviews e-Commerce integration in agriculture (2017-2021), highlighting Blockchain's potential, e-commerce development, and direct marketing benefits.	1. It highlights the importance of addressing security and privacy concerns in blockchain technologies, which is crucial for their widespread adoption.	1.Limited scope of the editorial, as it does not cover all the possible research challenges and opportunities in this field.
Blockchain and Autonomous Vehicles: Recent Advances and Future Directions	1.Saurabh Jain 2.Neelu Jyoti Ahuja 3. P. Shrikant 4., Kishor Vinayak Bhadane 5.Bharathram Nagalh 6.Adarsh Kumar	2021	The paper explores recent advances and future directions at the intersection of blockchain and autonomous vehicles, examining the potential synergies and developments in this emerging field.	1.It sheds light on the potential benefits of using blockchain in the realm of autonomous vehicles 2. The paper identifies future directions for research and development. By outlining the gaps and challenges in the current use of blockchain in autonomous vehicles, it provides a roadmap for further exploration and innovation in this domain.	1.Lack of smart contract-based smart and secure data handling in an autonomous vehicle 2.Vehicle's internal parameters for blockchain network 3.Massive storage requirements
Blockchain Technology and Cryptocurrencies	1.Siddharth Rajput 2.Archana Singh 3. Smiti Khurana 4. Tushar Bansal 5. Sanyukta Shreshtha	2019	The paper provides an overview of blockchain technology and cryptocurrencies, covering key concepts, functionalities, and potential applications in the realm of decentralized digital currencies.	1.Provides a tangible form of documentation, which can be useful in legal or regulatory contexts. 2.Lower Optional Cost 3.Enhanced Security And Confidentiality	1.Since bitcoins are not settling to a fused establishment, government, or bank their expenses may rise and fall fundamentally. 2.Clients may pick bitcoins to pay for unlawful items and endeavors (illegal substances, firearms, etc) by methods for the

					online dull web, as bitcoins can be harder to pursue.
A Privacy-Preserving E-Commerce System Based on the Blockchain Technology	1.Yiming Jiang, 2. Chenxu Wang 3.Yawei Wang 4. Lang Gao	2019	The paper introduces a privacy-focused E-commerce model using private smart contracts and zero-knowledge proofs. It addresses privacy concerns by ensuring transactions without revealing personal data, employing blockchain, zk-SNARKs, and IoT measures.	1.Enhanced privacy 2.Transparency and trust 3.Efficient transactions	1.One drawback is the potential for slower transaction processing times. 2.complexity and lack of user-friendly interfaces.
A Reliable E-commerce Business Model Using Blockchain Based Product Grading System	1.Ching-Nung Yang 2.Yi-Cheng Chen 3. Shih-Yu Chen 4. Song-Yu Wu	2019	The paper proposes a blockchain-based Product Grading System (BPGS) to address disputes over varying product quality perceptions in online shopping.	1.Enhancing Trust and Data Security 2.Streamlining Supply Chain Management	1.Scalability is an issue. 2.Blockchain is not a Distributed Computing System
A Systematic Survey of e-Commerce Applications with Blockchain in Agro Sector	1.Ashok Murugesan 2.Kumar Ramasamy 3.Aravind P 4. Bathri Narayanan V 5.Daniel Raja J	2021	It explores the integration of blockchain technology in e-commerce platforms specific to agriculture, highlighting trends, challenges, and potential benefits within this domain.	1.The use of blockchain technology can enhance transparency and traceability in the agro sector 2.Can provide a secure and immutable record of transactions, ensuring the authenticity of products and reducing the risk of fraud.	1.The implementation of blockchain technology requires a significant investment in infrastructure and training.
The Diversity Layout of E-commerce Applications Based on Android	1.Yi Liu 2. Chuanchang Liu 3.Zhiyuan Su	2018	The paper underscores the significance of mobile e-commerce apps in the mobile Internet era, focusing on the necessity for diverse and flexible homepage layouts.	1.It allows for greater customization and personalization. 2.Android provides a wide range of options for designing layouts, allowing developers to create unique and visually appealing interfaces. This can help to enhance the user	1.The fragmentation of the Android ecosystem. 2.Android has various different versions and making application compatible for every version is a difficult task
Towards Formal Modeling and Analysis of UPI Protocols	1.Sreekanth Malladi	2021	The paper explores UPI (Unified Payments Interface), a mobile payment framework connecting customers and merchants. It addresses reported vulnerabilities by proposing the modeling of UPI protocols as conventional cryptographic protocols.	1.It sheds light on UPI framework. 2.It Models UPI with conventional cryptographic protocol to test for security breaches	1.Informal Weakness Discovery 2.Simplification of Protocols - this could lead to abstraction from real world complexities 3.Unconventional Features - It suggests changes in unconventional features which may affect correctness/effectiveness.
Developing an E-Commerce Website	1.Syed Emdad Ullah 2.Tania Alauddin 3. Hasan U. Zaman	2016	The paper addresses the disparity between e-commerce and brick-and-mortar businesses, outlining challenges and solutions for e-commerce website development	1.Provides practical insights into the process of developing an e-commerce website.	1.May lack in-depth technical details or advanced strategies for experienced developers.

LIMITATIONS OF EXISTING SYSTEM

- *Centralized Control:*

Issue: Traditional e-commerce platforms are typically centralized, meaning they are con trolled by a single entity. This centralization can lead to a lack of transparency and potential abuse of power.

- *Trust and Transparency:*

Users often lack visibility into the supply chain and authenticity of products. Trust can be eroded due to concerns about counterfeit goods and inaccurate product information.

- *Payment Disputes and Chargebacks:*

Issue: Chargebacks and payment disputes are common in traditional e-commerce, leading to friction between buyers and sellers. The resolution process is often time-consuming.

- *Data Security and Privacy:*

Issue: Centralized storage of user data makes traditional e-commerce platforms vulnerable to data breaches and privacy concerns.

- *International Transactions and Currency Conversion:*

Issue: Traditional e-commerce platforms may face challenges in providing seamless inter national transactions, including issues related to currency conversion and cross-border payments.

- *High Transaction Costs:*

Issue: Traditional payment gateways and financial intermediaries often impose transaction fees, especially for international transactions, leading to higher costs for both buyers and sellers.

PROBLEM STATEMENT

"To create a secure and transparent marketplace to confidently buy, sell, and trace authentic products and to boost the preservation and growth of the businesses."

IMPLEMENTATION

- *Framework:*

1.Define the goals of the experiment. What do you want to learn about using blockchain technology for e-commerce ?

2. Identify the key metrics that will be used to measure success. This could include metrics such as the number of transactions processed per second, average transaction time, percentage of successful transactions, cost per transaction, number of active users, and customer satisfaction.

3.Choose a blockchain platform. There are a number of different blockchain platforms available, each with its own strengths and weaknesses. Factors to consider when choosing a platform include scalability, security, and cost.

4.Design the e-commerce website. The website should be designed to be user-friendly and to support the key features and functionality that you want to experiment with.

5.Develop the e-commerce website. This will involve developing the front-end and back-end of the website, as well as integrating with the chosen blockchain platform.

6.Deploy the e-commerce website. Once the website is developed, it needs to be deployed to a production environment.

7.Recruit participants for the experiment. This could involve recruiting existing customers or members of the public.

8.Provide participants with training on how to use the e-commerce website and the blockchain platform.

9.Collect data on the key metrics that were identified in the planning phase. This can be done by logging all transactions and user interactions.

10.Monitor the performance of the e-commerce website and the blockchain platform. This includes tracking metrics such as response times and CPU usage.

11.Analyze the data that was collected during the experimentation phase. This will involve identifying trends and patterns in the data.

12.Draw conclusions about the benefits and challenges of using blockchain technology for e-commerce.

13.Identify areas for improvement.

◦ *Algorithm*

1.Initialize the blockchain platform. This may involve creating a new blockchain or connecting to an existing one.

2.Create a smart contract for the e-commerce website. The smart contract will define the rules and procedures for buying and selling products on the website.

3.Deploy the smart contract to the blockchain. Once the smart contract is deployed, it can be used to process transactions on the e-commerce website.

4.Create a user account for each participant in the experiment. Each user account will have a unique address on the blockchain.

5.Allow participants to deposit cryptocurrencies into their user accounts. This will allow them to purchase products on the e-commerce website.

CIRCUIT DESIGN

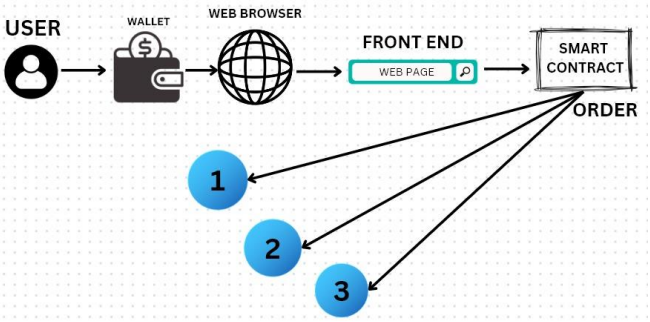

Fig.1 Smart Contracts

In the above diagram the user will connect his wallet to the website that we have created for our e commerce store Then through the web browser and with the help of the user friendly UI the user can purchase any product using ether As this is being carried out the smart contracts will handle the transaction that is meant to be executed over the block chain Taking care of the order and all the details of the product the smart contracts will then act upon the blockchain to do so.

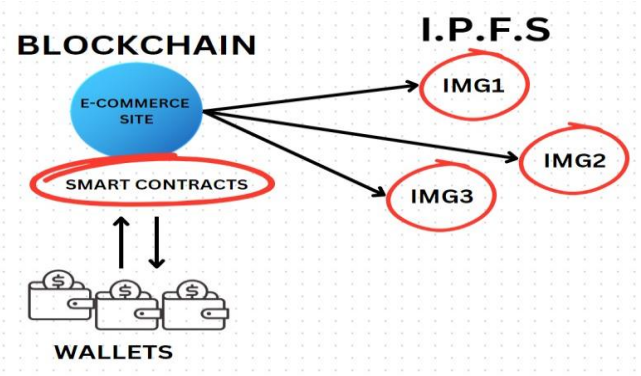

Fig.2 IPFS (Inter Planetary File System)

INTER PLANETARY FILES SYSTEMS is like a backend of the block chain that helps store files and pictures in the blockchain and we use this to obtain the pictures on our front end to display for the users to make it easy for them to get a discrete view of the product.

SOFTWARE USED

◦ *Vs Code*

Visual Studio Code (VS Code) is a lightweight, cross-platform source code editor developed by Microsoft. It supports numerous programming languages, offers smart code completion, integrates Git for version control, includes an integrated terminal, and is highly customizable through extensions. VS Code is widely used for its speed, versatility, and a large community contributing to its ongoing development. It will be used for front-end design.

◦ *Pinata*

Pinata is a cloud-based service that simplifies and accelerates the development of decentralized applications (DApps) on blockchain networks, particularly for the Inter Planetary File System (IPFS). It offers tools and services for managing, pinning, and distributing content on IPFS, making it easier for developers to handle the storage and retrieval of data within decentralized applications. Pinata simplifies the process of interacting with IPFS, providing developers with an efficient solution for managing and sharing data in a decentralized and distributed manner. It will be used for IPFS(Inter Planetary File System)

◦ *Ethereum*

Ethereum is a decentralized blockchain platform that enables the creation and execution of smart contracts and decentralized applications (DApps). Its native cryptocurrency is called Ether (ETH). Ethereum's key features include a Turing-complete scripting language for smart contracts, a decentralized virtual machine (EVM) to execute these contracts, and a consensus mechanism called Proof of Stake (PoS) that is transitioning from Proof of Work (PoW). Ethereum aims to provide a global, open-source platform for building decentralized applications, fostering innovation in the blockchain space. It is using etherium blockchain for online payment purposes.

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 2, December 2023
E – ISSN – 2583-7559

RESULTS

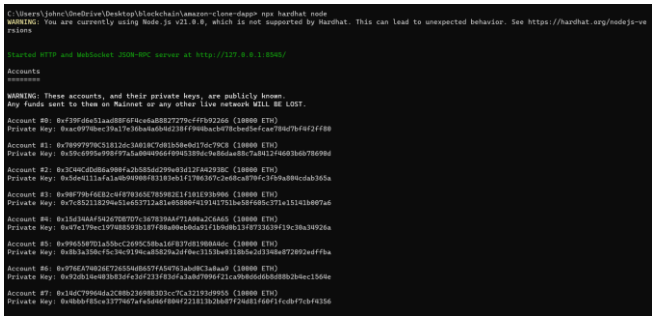

Fig 10.1 Result 1

The project is currently using HardHat framework with Solidity and JavaScript coding languages. We created SmartContracts for product listing section. We also used Pinata for storing the data (images) onto IPFS(Inter Planetary File System) which will be required to display data on front-end.

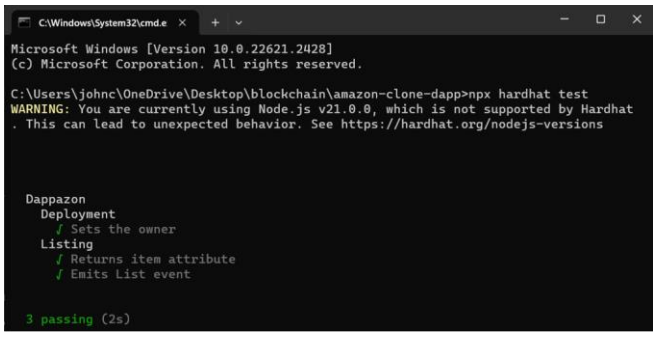

Fig.10.2 Result 2

Initially we studied the basics of Solidity language. Using Solidity we programmed the Smart Contracts and we also used JavaScript for programming.This is the output of SmartContracts on Cmd. The Hardhat deploys the Solidity and JavaScript files using Mocha framework and Chai libraries.

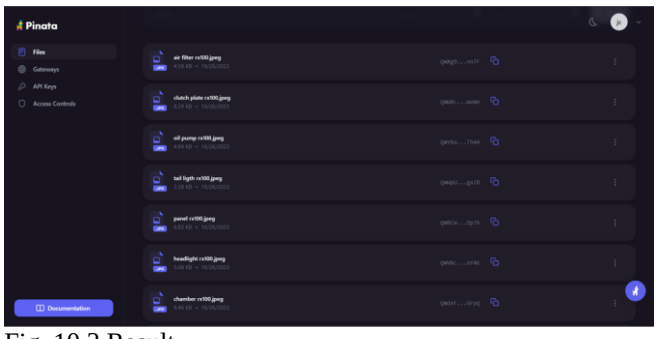

Fig. 10.3 Result

Since the blokchain does not diplay images directly we will be using Pinata database. This is the output we obtained after we uploaded data using Pinata onto IPFS(Inter Planetary File System).This data will be further displayed on the front-end of the website. This is a seperate database used to upload images onto blockchain.

CONCLUSION AND FUTURE SCOPE

In conclusion, our experiment on the "Blockchain-Based E-commerce Website" has been a significant journey marked by notable achievements and advancements in the realm of de centralized and secure online transactions. Over the course of this semester, we successfully conceptualized and implemented smart contracts, elevating the integrity and transparency of our e-commerce platform. The utilization of smart contracts not only streamlined the listing of products but also ensured a trustless environment for both buyers and sellers.

A pivotal aspect of our project involved harnessing the power of Pinata to seamlessly integrate images into the InterPlanetary File System (IPFS). This strategic move not only en hanced the accessibility and durability of our data but also contributed to the overall decen tralization of our e-commerce ecosystem.

Looking ahead, the next semester holds the promise of further refinement and comple tion of our project. We are determined to finalize the front-end of the website and seamlessly integrate all components to provide users with a seamless and intuitive experience. The journey doesn't end here; rather, it extends into the next semester, where we aim to bring the vision of a fully functional blockchain-based e-commerce platform to fruition.

In summary, this semester has been instrumental in laying the foundation for our blockchain based e-commerce website. The incorporation of smart contracts, Pinata, and IPFS has posi tioned our project at the forefront of technological innovation in the e-commerce landscape. As we continue to evolve and refine our platform, the upcoming semester holds the promise of transforming our vision into a tangible, user-friendly reality

REFERENCES

[1] C. Liu, Y. Liu and J. Chen, "Study on Dynamic Interface Layout for Android Application," Computer and Modernization, pp. 197-200, 2013.

[2] J. Zhu, R. He, "The Usability Testing on the Application Interface Layout of Android Mobile," Packaging Engineering, vol. 35, pp. 61-64, 2014.

[3] Android Developers, [Online]. Available: http://developer.android.com/index.html.

[4] M. Burton and D. Felker, Android Application Development For Dummies, Wiley Sons, 2015.

[5] S. Thejaswini and K. R. Ranjitha, "Blockchain in Agriculture by using Decentralized Peer to Peer Networks," in 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020, pp. 600-606, doi: 10.1109/ICISC47916.2020.9171083.

[6] Lakshmi P, Divya K et al., "Farm Direct Marketing," 2020 International Research Journal of Engineering and Technology (IRJET).

[7] H. M. Kim and M. Laskowski, "Agriculture on the Blockchain: Sustainable Solutions for Food, Farmers, and Financing," in D. Tapscott (Ed.), Supply Chain Revolution, Barrow Books, 2018.

[8] F. Xiang and D. Wang, "Research on Operation Mode of a 'Reinternet Plus' Agricultural Products Intelligent Supply Chain," in 2020 International Conference on Urban Engineering Science (ICUEMS), Zhuhai, China, 2020, pp. 208-211, doi: 10.1109/ICUEMS50872.2020.00053.

[9] D. He, K.-K. R. Choo, N. Kumar, A. Castiglione, "Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies," DOI: 10.1109/ACCESS.2018.2882658.

[10] S. Jain, N. J. Ahuja, P. Shrikant, K. V. Bhadane, B. Nagalh, A. Kumar, "Blockchain and Autonomous Vehicles: Recent Advances and Future Directions," DOI: 10.1109/ACCESS.2021.3113649.

[11] S. Rajput, A. Singh, S. Khurana, "Blockchain Technology and Cryptocurrencies," DOI: 10.1109/AICAI.2019.8701371.

[12] Y. Jiang, C. Wang, Y. Wang, L. Gao, "A Privacy-Preserving E-Commerce System Based on Blockchain Technology," DOI: 10.1109/IWBOSE.2019.866647.

[13] C.-N. Yang, Y.-C. Chen, "A Reliable E-commerce Business Model Using Blockchain Based Product Grading System," DOI: 10.1109/ICBDA.2019.8713204.

[14] A. M. Kumar, R. Kumar, "A Systematic Survey of e-Commerce Applications with Blockchain in Agro Sector," DOI: 10.1109/ICACCS51430.2021.9.

[15] Y. Liu, C. Liu, Z. Su, "The Diversity Layout of E-commerce Applications Based on Android," in CCWC, DOI: 10.1109/CCWC517.

[16] S. Malladi, "Towards Formal Modeling and Analysis of UPI Protocols," DOI: 10.1109/ICICV50876.2021.9388452.

[17] How to build a Fullstack DApp on Ethereum with Solidity React - 2022, [Online]. Available: https://youtu.be/1dWxCERfaE?si=N2JtGEJoT3vcFbFF.

[18] Code a Web 3.0 Amazon Clone Step-By-Step with Solidity, Ethers.js, React Hardhat, [Online]. Available: https://youtu.be/X1ahXNYkpL8?si=LtyqI8s-9kA9Hxn.

[19] Learn how to create Blockchain from scratch | JavaScript Blockchain |Code Eater - Blockchain | Hindi, [Online]. Available: https://youtu.be/7OR12WF2-3Y?si=OTdI9GV8jBOlTBW.

[20] Learn how to create Blockchain from scratch | JavaScript Blockchain |Code Eater - Blockchain | Hindi, [Online]. Available: https://youtu.be/7OR12WF2-3Y?si=Oz125SrxzuFZn7uE.

[21] Blockchain Ecommerce App Tutorial (Accept ERC20 Token Payments), [Online]. Available: https://youtu.be/f5npM1PvoyE?si=acyeb6rMafeHxFwR.

[22] "How to store data in blockchain," GeeksforGeeks, [Online]. Available: https://www.geeksforgeeks.org/how-to-store-data-in-blockchain/.

[23] "Implement a blockchain cryptocurrency payment system," DevTeam.space, [Online]. Available: https://www.devteam.space/blog/implement-a-blockchain-cryptocurrency-payment-system/.

[24] "IPFS," SolidityDeveloper.com, [Online]. Available: https://soliditydeveloper.com/ipfs.