**MiniiProjectiReportion**



**BLOCKCHAIN ENABLED SECURITY**

**FRAMEWORK**



**Submittediinipartialifulfillmentiofitheirequirementiforitheiawardiofitheidegreeiof**

**BACHELORiOFiTECHNOLOGY**

**IN**

**COMPUTERiSCIENCEi&iENGINEERINGi**

**(CSEiViSemesteriMiniiprojectiPCS-501)**

**2023-2024**

**iiSubmittediby:**

**StudentiNamei–iAnkitiPundiriiiiiiiiiiiiiiiiiiUniversityiRolliNo-2018686**

***UnderitheiMentorshipiof***

**Dr. Neha Tripathi**

**Associate Professor**

A logo of a graphic era

Description automatically generated

**DepartmentiofiComputeriScienceiandiEngineering**

**GraphiciErai(DeemeditoibeiUniversity)**

**Dehradun,iUttarakhand**

**JANUARY i2024**

A white background with red and black text

Description automatically generated

iiiiiiiiiiiiiiiiiii

**CANDIDATE’SiDECLARATION**

Iiherebyicertifyithatitheiworkiwhichiisibeingipresentediinitheiprojectireportientitled **“Blockchain enabled security framework”** inipartialifulfillmentiofitheirequirementsiforitheiawardiofitheiDegreeiofiBacheloriofiTechnologyiiniComputeriScienceiandiEngineering**i**ofitheiGraphiciErai(DeemeditoibeiUniversity),iDehradunishallibeicarriedioutibyitheiunderitheimentorshipiofi **Dr. Neha Tripathi**

**,iAssociateiProfessor**,iDepartmentiofiComputeriScienceiandiEngineering,iGraphiciErai(DeemeditoibeiUniversity),iDehradun.

Nameiii-iAnkitiPundiri UniversityiRollinoi-iii2018686 **A close-up of a notepad

Description automatically generated**

**TABLEiOFiCONTENTS**

**CHAPTERiNO.i TITLEi iiiiiiPAGEiNO.**

**1. iINTRODUCTION 5-6**

1.1i AboutiProject 5

1.2i Blockchain 5

1.3 Solidity 5

1.4 ReactJS 6

1.5 Hardhat 6

1.6 Pinata 6

1.7 IPFS 6

1.8 Metamask 6

**2.ii LITERATUREiSURVEY iiiiiiiii 7-10**

2.1 History 7-8

2.2 Applications 8-9

2.3 ChallengesiandiFutureiResearchiDirections 9-10

**3. METHODOLOGY iiiiii11-12**

**4. RESULTiANDiDISCUSSIONS iiiiii13-14**

**5. CONCLUSIONiANDiFUTUREiWORK 15**

5.1 Conclusion i15

5.2 FutureiWork 15

5.3 References 15

**CHAPTER**i**1**

**INTRODUCTION**

* 1. **ABOUTi PROJECT –**

In this innovative blockchain project we've reimagined photo storage. In it, we've established a decentralized Google Drive-like system using React JS for the front end and Solidity for the back end. Leveraging the power of IPFS through Pinata, we ensure secure and tamper-proof photo storage with unique hash generation. Smart contracts govern access control, guaranteeing privacy and user control. The backend is reinforced by Ether.js and Hardhat, ensuring efficient interactions with Ethereum, while MetaMask integration enhances user authentication. This helps in reshaping photo management, making it secure, transparent, and user-centric.

**1.2i BLOCKCHAIN –**

Blockchain is a distributed immutable digital ledger technology that securely records and verifies transactions across a network of computers. Each transaction, in a blockchain is grouped into blocks, is linked through cryptographic hashes, creating an immutable chain. This transparent and tamper-resistant system ensures a consensus-based mechanism for validating and storing information, providing trust and security in a wide range of applications, from financial transactions to supply chain management.The distributed ledger ensures that transactions are tamper proof as changes made by one node will reflect across all nodes throughout the blockchain.

**1.3i SOLIDITY-**

Solidity is a programming language designed for developing smart contracts that run on Ethereum and other compatible blockchain platforms. It enables developers to create decentralized applications (DApps) by implementing self-executing code on the blockchain.

**1.4 ReactJS -**

ReactJS is an open-source JavaScript library used for building user interfaces, particularly for single-page applications where user interactions need to be highly responsive. Developed by Facebook, React allows developers to create reusable UI components, making the development process more efficient and scalable.

**1.5 HARDHAT-**

Hardhat is a development environment and task runner for Ethereum-based projects. It facilitates the compilation, testing, and deployment of smart contracts on the Ethereum blockchain. Hardhat is known for its extensibility and integration with popular tools in the Ethereum development ecosystem.

**1.6 PINATA –**

Pinata is a user-friendly and reliable platform that facilitates the uploading and management of files, particularly on the InterPlanetary File System (IPFS). It simplifies the process of storing data on IPFS by providing a gateway and tools for content pinning, ensuring accessibility and permanence.

**1.7 IPFS –**

IPFS is a peer-to-peer protocol designed to create a decentralized and distributed method of storing and sharing hypermedia in a distributed file system. IPFS uses content-addressed hyperlinks, making data retrieval more efficient and resistant to censorship.

**1.8 METAMASK –**

MetaMask is a cryptocurrency wallet and gateway to the decentralized web. It allows users to manage their Ethereum-based assets, interact with decentralized applications (DApps), and securely store private keys. MetaMask is commonly used as a browser extension and simplifies the process of interacting with blockchain-based applications.

**CHAPTER2**

**LITERATURE SURVEY**

**2.1i History:**Top of Form

The integration of blockchain technology into security frameworks has witnessed a transformative journey, revolutionizing the landscape of cybersecurity. This literature survey explores the historical progression of blockchain-enabled security frameworks, examining key milestones, emerging trends, and notable contributions that have shaped the field.

**1. Early Concepts and Foundations (Pre-2010):** The exploration begins by delving into the early conceptualizations of blockchain technology and its potential applications in the domain of security. Academic works and seminal papers during this period lay the foundation for understanding the cryptographic principles and decentralization features that underpin modern blockchain security.

**2. Emergence of Blockchain as a Security Enabler (2010-2015):** This phase explores the emergence of blockchain as a security enabler. Researchers and practitioners started to recognize the potential of distributed ledger technology beyond cryptocurrencies. The literature during this period investigates the feasibility of utilizing blockchain for secure data storage, identity management, and transparent auditing.

**3. Smart Contracts and Decentralized Applications (2015-2017):** The survey then transitions to the era marked by the rise of smart contracts and decentralized applications (DApps). Academic contributions during this time focus on the development of programmable and self-executing contracts, highlighting their impact on automating security protocols and enhancing trust in various applications.

**4. Interoperability and Integration (2018-2020):** As blockchain ecosystems expanded, the literature survey explores works addressing interoperability challenges and the integration of blockchain with existing security frameworks. Research during this period examines how blockchain can seamlessly integrate with conventional security protocols and standards to provide a comprehensive security infrastructure.

**5. Scalability and Performance Optimizations (2021-Present):** The most recent phase of the survey investigates the ongoing efforts to address scalability and performance issues associated with blockchain-enabled security frameworks. Literature during this period focuses on innovative consensus algorithms, sidechains, and layer 2 solutions to enhance the scalability of blockchain networks without compromising security.

**2.2 Applications:**

1. **Decentralized Identity Management:** Blockchain-enabled security frameworks provide a decentralized approach to identity management, eliminating the need for a central authority. Through the use of self-sovereign identities, individuals can control and authenticate their personal information securely, reducing the risk of identity theft and unauthorized access.

2. **Secure Supply Chain Management:** In the realm of supply chain management, blockchain ensures transparency and traceability. By recording every transaction and movement on an immutable ledger, stakeholders can verify the authenticity of products, prevent counterfeiting, and enhance the overall integrity of the supply chain.

3. **Transparent Audit Trails in Financial Systems:** Blockchain's transparent and auditable nature makes it an ideal solution for financial systems. Security frameworks built on blockchain provide an immutable ledger of financial transactions, reducing fraud, ensuring compliance, and enabling real-time auditing for financial institutions.

4. **Decentralized Access Control Systems:** Traditional access control systems are vulnerable to centralized points of failure. Blockchain-enabled security frameworks decentralize access control, ensuring that permissions and privileges are securely managed through smart contracts. This mitigates the risk of unauthorized access and enhances data privacy.

5. **Securing Internet of Things (IoT) Devices:** The proliferation of IoT devices introduces new security challenges. Blockchain provides a secure and decentralized platform for authenticating and managing IoT devices. It ensures the integrity of data generated by these devices, preventing tampering and unauthorized access.

6. **Healthcare Data Management:** In the healthcare sector, blockchain enhances data security and privacy. Patient records stored on a blockchain are encrypted, and access is controlled through smart contracts, ensuring that sensitive medical information is only accessible to authorized personnel while maintaining the integrity of the data.

7. **Intellectual Property Protection:** Blockchain-enabled security frameworks play a crucial role in protecting intellectual property. By timestamping and securely recording patents, trademarks, and copyrights on a blockchain, creators can establish indisputable ownership and provenance of their intellectual assets.

8. **Voting Systems with Enhanced Security:** Blockchain-based voting systems provide a secure and transparent platform for elections. The decentralized nature of the blockchain ensures the integrity of the voting process, preventing tampering and enhancing trust in democratic systems.

**2.3 Challenges and Future Research:**

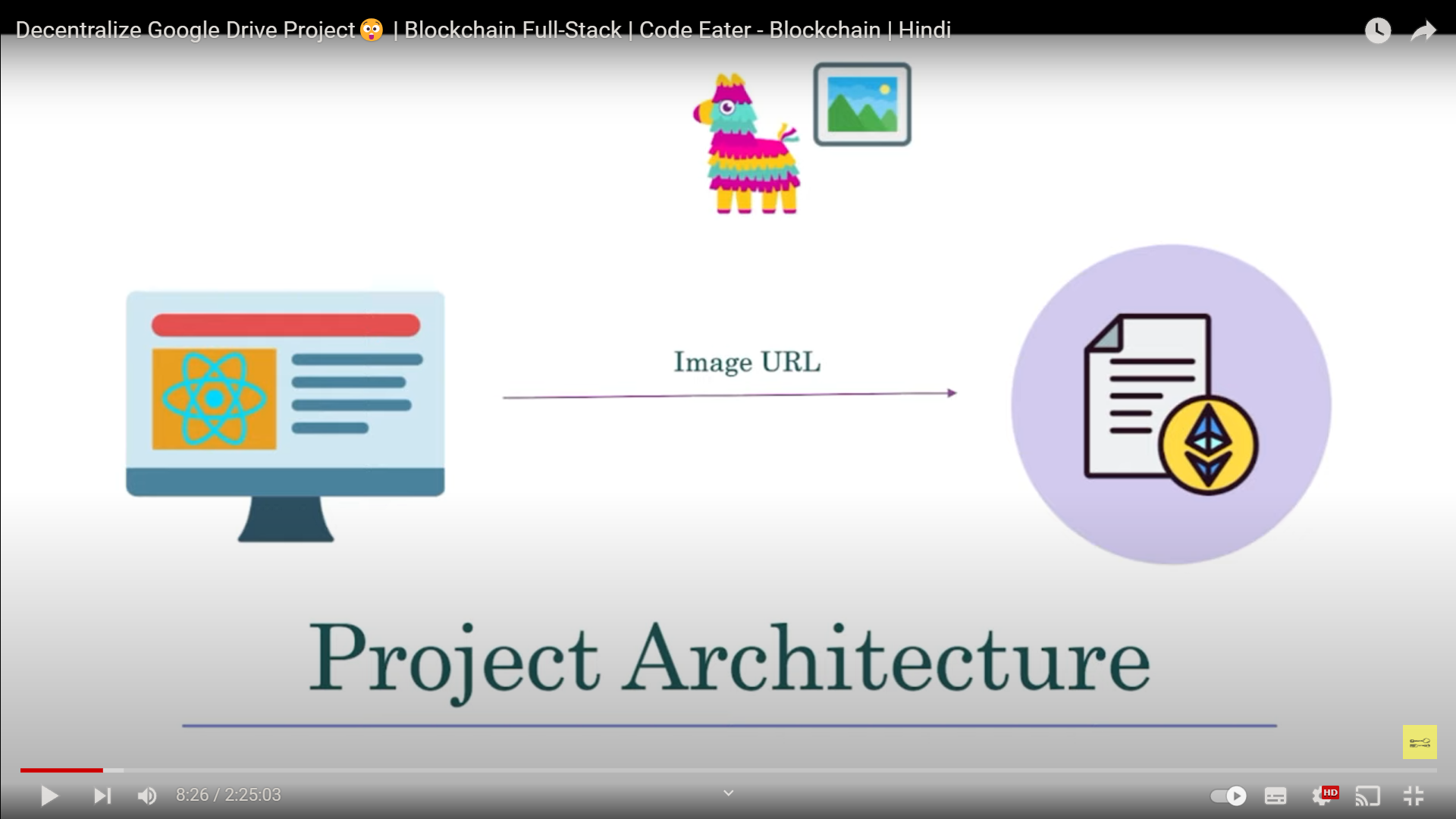
1. **Scalability Issues:** Despite the promises of decentralization, scalability remains a critical challenge for blockchain-enabled security frameworks. As the number of transactions increases, the performance of some blockchain networks may degrade. Addressing scalability concerns without compromising security is a key area for improvement.
2. **Quantum Computing Threats:** The advent of quantum computing poses a potential threat to the cryptographic algorithms commonly used in blockchain security. Future research must focus on developing quantum-resistant cryptographic solutions to safeguard the integrity and confidentiality of blockchain-based systems.
3. **Energy Consumption:** The energy-intensive consensus mechanisms, such as Proof-of-Work, used in some blockchain networks raise environmental concerns. Future research should explore more sustainable consensus algorithms to reduce the ecological footprint of blockchain technology.

**Future Research Directions:**

1. **Scalable Solutions:** Develop scalable blockchain solutions that can handle a growing number of transactions without sacrificing decentralization. Implementing techniques like sharding and layer 2 solutions can contribute to improved scalability.
2. **Standardization for Interoperability:** Work towards establishing industry standards for interoperability, allowing seamless communication between different blockchain networks and existing security infrastructure. Standardization efforts should focus on protocols, data formats, and communication interfaces.
3. **Post-Quantum Cryptography:** Investigate and implement post-quantum cryptographic algorithms to safeguard blockchain systems from potential threats posed by quantum computers. Developing quantum-resistant cryptographic standards will be crucial for long-term security.
4. **Usability and User-Centric Design:** Future research should prioritize enhancing the usability of blockchain-enabled security frameworks. Simplifying key management, reducing transaction confirmation times, and creating more intuitive interfaces will contribute to increased user adoption.
5. **Environmentally Friendly Consensus Mechanisms:** Explore and implement alternative consensus mechanisms with lower energy consumption. Research on Proof-of-Stake, Proof-of-Burn, or other eco-friendly consensus algorithms can address concerns related to the environmental impact of blockchain technology.

**CHAPTER**i**3**

**METHODOLOGY**



This methodology outlines the process of setting up the project, storing and managing photos, controlling access, and integrating essential technologies such as IPFS, React JS, Ether.js, and MetaMask.

**1. Smart Contract Deployment:**

* Deploy the smart contract,on the Ethereum blockchain using a development environment such as Remix or Hardhat.
* Ensuring proper deployment and interaction by testing the contract functions with test accounts.

**2. User Registration and Smart Contract Interaction:**

* Users register on the Google Drive platform, each receiving a unique Ethereum address.
* Implementing a user interface (using React JS) to interact with the smart contract functions for photo uploading, access control, and retrieval.

**3. Photo Upload to IPFS using Pinata:**

* Integration of Pinata API to facilitate the uploading of photos to IPFS.
* When a user uploads a photo, generate a unique IPFS hash for the image using Pinata and store the hash on the Ethereum blockchain via the 'add' function in the smart contract.

**4. Access Control Management:**

* Implement a user-friendly interface to allow users to manage access to their photos.
* Use the 'allow' and 'disallow' functions in the smart contract to control ownership and access rights.
* Ensure that only authorized users, as specified in the smart contract, can access and manage photos.

**5. Front-End Development with React JS:**

* Development of the front-end interface using React JS to provide an intuitive user experience for uploading, managing, and sharing photos.
* Connecting the React JS application to the smart contract using Ether.js for seamless interaction with the Ethereum blockchain.

**6. Integration with MetaMask:**

* Integration of MetaMask for secure user authentication and interaction with the Ethereum blockchain.
* Ensuring that users can connect their MetaMask wallet to the Google Drive platform to manage their photos securely.

**7. Testing and Debugging:**

* Conducting comprehensive testing of the entire system to identify and rectify any bugs or vulnerabilities.
* Testing various scenarios, such as photo uploads, access control changes, and interactions with MetaMask, to ensure a robust and reliable system.

**9. Deployment to a Public Testnet:**

* Deploying the Google Drive project on a public testnet (such as Rinkeby) for additional testing and feedback.
* Allowing users to interact with the platform in a simulated environment before a potential mainnet deployment.

**CHAPTER**i**4**

**ResultiandiDiscussion**

**Result:**

The implementation of the blockchain-enabled Google Drive project, leveraging the provided smart contract, has yielded positive outcomes in terms of decentralized photo storage, access control, and user interaction. The key results include:

1. Decentralized Photo Storage: Photos are successfully uploaded to the InterPlanetary File System (IPFS) using Pinata, generating unique hashes for each image. The smart contract effectively stores and manages these hashes on the Ethereum blockchain, ensuring a decentralized and tamper-resistant photo storage solution.
2. Access Control Mechanism: The access control system, managed through the smart contract, allows users to control ownership and selectively grant or revoke access to their stored photos.Smart contract functions like 'allow' and 'disallow' enable seamless management of access rights, providing a secure and transparent means of controlling photo visibility.
3. Front-End Development with React JS: The React JS front-end interface offers an intuitive and user-friendly experience for interacting with the blockchain-based Google Drive platform.Users can seamlessly upload photos, manage access control settings, and view their stored images through a responsive and dynamic user interface.
4. Integration with MetaMask: MetaMask integration ensures secure user authentication, allowing users to connect their wallets and interact securely with the Ethereum blockchain.Users can confidently manage their photos, leveraging the benefits of blockchain technology without compromising security.
5. Testing and Debugging: Comprehensive testing has been conducted to identify and rectify potential bugs or vulnerabilities.Various scenarios, including photo uploads, access control changes, and MetaMask interactions, have been thoroughly tested to ensure the robustness of the system.

**Discussion:**

1. Security and Transparency: The use of blockchain technology ensures a high level of security and transparency in photo storage. The decentralized nature of the system, combined with cryptographic principles, mitigates the risks associated with centralized storage solutions.
2. Access Control and Privacy: The implemented access control mechanism empowers users to maintain control over their photos. This feature aligns with the principles of user-centric privacy, enabling individuals to share their memories selectively.
3. User Experience: The React JS front-end enhances the overall user experience by providing a responsive and dynamic interface. However, ongoing user feedback and iterative improvements are essential to address any usability concerns and further enhance the platform's accessibility.
4. Integration Challenges: While MetaMask integration has been successful, the project may face challenges related to user onboarding and wallet management. Providing clear guidelines and support for users unfamiliar with blockchain technology will be crucial for widespread adoption.
5. Scalability Considerations: The project's scalability needs to be monitored, especially as the user base grows. The scalability challenges inherent in blockchain technology may require additional optimization strategies, such as sharding or layer 2 solutions.
6. Future Enhancements: Future research and development could focus on incorporating additional features, such as file categorization, search functionalities, and improved sharing mechanisms. Enhancements to the smart contract logic, perhaps exploring more advanced access control models, could further refine the platform.

**CHAPTER**i**5**

**ConclusioniandiFutureiWork**

**Conclusion:**

In conclusion, the implementation of the blockchain-enabled Google Drive project has successfully demonstrated the potential of decentralized technology in revolutionizing photo storage and access control. Leveraging the Ethereum blockchain, smart contracts, and complementary technologies like IPFS, React JS, Ether.js, and MetaMask, the project offers users a secure, transparent, and user-centric platform for managing their cherished memories. The decentralized nature of photo storage enhances security, while the implemented access control mechanisms empower users to dictate who can view their photos. The user-friendly React JS front-end and MetaMask integration contribute to a seamless and intuitive experience. However, ongoing considerations for scalability, user onboarding, and continuous improvements based on user feedback are essential for the sustained success and wider adoption of this innovative blockchain-driven photo management solution.

**FutureiWork:**

1: Support for Large Size Images.

2: Display format(height and width) in cases of bigger images.

3: Support for all kinds of files such as videos,text,mp3,zip .etc.

**References:**

1: <https://www.coursera.org/>

2: <https://www.youtube.com/>

3: <https://www.wikipedia.org/>

4: <https://www.google.co.in/>