

Implementation of SHA256 for NFT Management Using Blockchain

Prateek Baranwal¹, Ritik Katiyar², Prajusha Kundu³, Meenakshi Yadav⁴

^{1,2,3}UG Student, Department of Information Technology

⁴Professor, Department of Information Technology, Galgotia's College of Engineering & Technology, Gr. Noida, India

Abstract– The rise of technology has transformed how digital assets are managed, leading to the popularity of fungible tokens (NFTs), as a key concept. This endeavour aims to create a NFT management system that tackles issues related to ownership security, transparency and accessibility within the NFT realm. By harnessing blockchain, contracts and governance mechanisms users can do their fund transfer and exchange digital assets or Crypto Currency. The unveiling of the key is part of the process. With the assistance of the OpenAI API, machine learning models craft personalized NFT visuals that are then minted on the Ethereum blockchain using Solidity based contracts. The Interplanetary File System (IPFS) bolsters data integrity and immutability by furnishing NFT metadata. This project involves a blend of business operations and management systems. Through leveraging technology and embracing governance this initiative widens access to digital assets while nurturing innovation and safeguarding digital rights. Ultimately fostering social creativity and reinforcing business digitization efforts. This study expands on NFT management systems by integrating IPFS to enhance data integrity and immutability establishing a basis, for democratizing ownership and management of assets.

Keywords - *Ethereum, Solidity, NFT, Blockchain, Smart Contracts.*

1. INTRODUCTION

The Decentralised applications, or DApps, are becoming increasingly popular in the quickly developing field of blockchain technology because of their intrinsic security, transparency, and immutability. This project makes use of Hardhat, an extensive development environment, and Solidity, the programming language for Ethereum smart contracts. The principal aim is to enable safe and transparent transactions on the Ethereum network, enhanced by personalised notes and keywords.

Through the use of Ethereum smart contracts, this dapp makes it possible for peer-to-peer transactions to occur directly without the need for middlemen. Ether can be transferred easily by users, who can also add keywords and customised messages to improve transaction functionality and traceability. In addition, the application offers a thorough history of transactions, which enables users to quickly filter and get pertinent information using predefined keywords.

1.1 Background and Origin

With the development of blockchain technology, a new age of transparent, safe, and decentralized systems has begun. Ethereum stands out as a leading force in this domain, offering an open-source, global platform for decentralized applications (dapps). At the forefront of Ethereum's innovation are the contracts that executes itself and comes with terms written directly into the code. Solidity, a high-level, contract-oriented language, was developed to facilitate the creation of smart contracts on the Ethereum Virtual Machine (EVM). However, the process of creating Ethereum dapps has proven challenging, often necessitating developers to integrate multiple frameworks and tools. In response to this complexity, this project introduces Hardhat, an Ethereum development environment that streamlines the dapp development lifecycle. Hardhat offers comprehensive tooling to simplify smart contract development, testing, and deployment, addressing the need for practical solutions tailored to real-world use cases in the Ethereum ecosystem.

1.2 Need for Detection System

In the modern digital era, the imperative for secure, transparent, and efficient transaction systems spans various industries, challenging traditional centralized systems riddled with trust issues, fraud susceptibility, and intermediary reliance, thus inflating costs and vulnerability. Blockchain technology, with its decentralized and immutable nature, offers a compelling remedy, executing transactions in a trust less environment, cutting out intermediaries, and trimming associated costs. Its inherent transparency ensures all transactions are logged in a tamper-proof distributed ledger, accessible to all, fostering accountability and curbing fraud risks. However, blockchain's adoption faces hurdles due to dapp development complexity and lack of user-friendly interfaces. This project endeavours to overcome these barriers by furnishing a seamless platform for Ethereum network-based blockchain transactions. By amalgamating Solidity and Hardhat, it empowers secure, auditable transactions embedded with custom messages and keywords, facilitating peer-to-peer transactions while tailoring functionality to industry requisites. By streamlining decentralized application development and deployment, this initiative holds promise to expedite blockchain's mainstream integration,

ushering in heightened transparency, security, and efficiency across diverse sectors, from finance to supply chain management, and beyond.

1.3 Importance of NFT Management System

With the development of blockchain and token currencies the financing systems has been redefined enabling the representation of unique, indivisible, and non-interchangeable assets on the blockchain. NFT marketplaces serve as crucial platforms for buying, selling, and discovering these unique digital assets, leveraging blockchain technology to ensure secure, transparent, and immutable transactions. Crypto wallets play a vital role in the NFT ecosystem, serving as secure digital storage for these valuable assets by storing private keys that grant ownership and control over NFTs. Projects integrating NFT functionality into decentralized applications (dapps), such as those utilizing Solidity, Hardhat, and the Ethereum blockchain, enhance the utility and traceability of NFT ownership transfers by allowing users to attach custom messages and keywords to transactions. This integration opens new avenues for personalization and storytelling within the NFT space, unlocking a new frontier in digital asset ownership and trade that empowers creators, collectors, and businesses to explore innovative business models, foster communities, and drive the evolution of the digital economy.

1.4 NFT-Creation

NFT creation refers to the process of creating or issuing a new digital asset, such as a non-fungible token (NFT), on a network. When an NFT is created, a unique token is generated and associated with a specific digital asset, making it distinct from other tokens on the same blockchain. This process typically involves deploying a smart contract on the blockchain.

2. LITERATURE REVIEW

Due to their potential to upend established financial systems and facilitate safe, decentralized transactions, cryptocurrencies and the blockchain technology that powers them have attracted a lot of attention recently. Numerous investigators have investigated the potential uses of blockchain technology and cryptocurrency in diverse fields, such as user authentication and banking. Using MetaMask, an online wallet extension, Choi and Kim (2019) present a blockchain-based user authentication paradigm. According to them, this method addresses the issue of service providers gaining control of and stealing personal information by employing centralized servers for user management and authentication. Users can ensure decentralized control and security by storing their encrypted personal information in a Smart Contract by utilizing MetaMask and the Ethereum public blockchain [1]. With an

emphasis on Bitcoin, DeVries (2016) offers a thorough examination of cryptocurrencies. Writer draws attention to the benefits of Bitcoin, including its fixed supply limit and potential to act as a haven against inflation of currency values. Nevertheless, the study also addresses the paper's shortcomings, including the blockchain's public nature, which poses privacy issues, and the security problems with bitcoin wallets and exchanges [2]. Pamu et al. (2022) provide an overview of decentralized cryptocurrency wallet applications that leverage the Ethereum ledger in their study. They suggest a system design that stores cryptocurrency and transaction data on the Ethereum blockchain, facilitating safe and open financial transactions. The writers also go over the drawbacks of blockchain-based wallets, namely sluggish transaction times and security flaws [3]. Yadav et al. (2020) investigate the application of blockchain technology in conjunction with cryptocurrency wallets. Financial security solutions. The benefits of utilising blockchain-based wallets over conventional e-wallets are emphasised, including the removal of third-party intervention and increased anonymity via the use of hexadecimal addresses. The authors stress the significance of safe authentication procedures and transaction tracking in their workflow for integrating blockchain-based wallets into the financial system [4]. Di Angelo and Salzer (2020) concentrate on Ethereum platform wallet contracts. In order to increase trust and security through transparency and features like daily limitations, permissions, multi-signatures, and recovery methods, they suggest implementing wallet functionalities as smart contracts [5]. Martiny (2021) offers a tutorial on how to use the web3.js JavaScript library and the Ethereum blockchain with MetaMask to create one-click login flows. The author describes the procedures needed in A decentralized authentication system's realistic implementation is demonstrated with user authentication, nonce generation, private key signing, and signature verification [6]. The possible effects of blockchain technology on a number of industries, including financial services, are covered by Tapscott and Tapscott (2016). They stress the benefits of blockchain, including decentralization, security, and transparency, and they contend that technology has the potential to completely transform how transactions are carried out and documented [7]. In the groundbreaking paper that created Bitcoin, Nakamoto (2008) suggested a decentralized blockchain-based peer-to-peer electronic payment system. The groundwork for the creation of cryptocurrencies and the investigation of blockchain technology's potential uses was established by this paper [8]. The banking industry could benefit from the combination of blockchain technology and cryptocurrencies by improving security, transparency, and effectiveness in monetary exchanges. For wider implementation, nevertheless, issues including scalability, regulatory constraints, and user adoption still need to be resolved. Sustained investigation and

advancement within this domain may yield inventive resolutions that fundamentally alter the conventional banking terrain.

3. FEATURES CONSIDERED

Authors can tokenize their original works as NFTs through a decentralised NFT marketplace, which uses blockchain technology to facilitate safe transactions. By implementing automated execution and royalty payments, smart contracts offer an open and secure environment for NFT trading.

3.1 User-Friendly Interface

Developed using React.js and Tailwind CSS, the interface allows users to seamlessly browse, create, buy, and sell NFTs. Features like advanced search, filtering, and user authentication enhance the user experience.

3.2 Metadata Management

To maintain data integrity and tamper resistance, NFT metadata is saved on decentralized storage systems like IPFS. Accurate asset descriptions are achieved through the use of metadata standards.

3.3 Security and Privacy

In order to ensure compliance with data protection laws like the CCPA and GDPR, security and privacy are given first priority through encryption systems that safeguard private keys and sensitive data, access restrictions, and permission schemes for restricted access.

3.4 Scalability and Interoperability

The marketplace is designed for scalability, leveraging layer 2 protocols or interoperability solutions to support cross-platform integration and seamless asset exchange, adhering to common protocols and standards for NFTs like ERC-721 and ERC-1155.

3.5 Environmental Sustainability

Environmental sustainability is considered, with exploration of solutions like renewable energy sources or energy-efficient consensus mechanisms to mitigate the environmental impact of NFT minting and trading.

4. METHODOLOGY

The NFT Management System was developed through a number of stages, which included creating the client for interactions on chain, putting smart contracts on the Ethereum chain, connecting with external handlers, testing, and assessment. We have gone through every stage, including the frameworks and subsystems employed, and the integration is done and the errors are fixed and documented. Furthermore, we outline the

processes that were employed to securely connect users' wallets, create user profiles to oversee NFT collecting and its other functionality mint on the chain network, create unique hash and message digest for the block creation for NFTs using proof of stake and create NFTs. This project's purpose is to in share a insightful paper of our project to provide guidance and insights for creating safe, user-friendly decentralized app for blockchain-based digital Fund and asset management.

4.1 Building Client

Building a client for our NFT management project involves several crucial steps to ensure a seamless and secure user experience. Firstly, integrating wallet functionalities like MetaMask allows us to securely connect their wallets to our chain on sepolia network without any security concerns. Next, creating smart contracts with Solidity ensures the authenticity and scarcity of NFTs. Utilizing Truffle for development and Ganache for local testing enhances the development process. Web3.js facilitates blockchain interaction, while robust security measures protect user data. The user interface, built with React.js and Tailwind CSS, ensures accessibility and usability, making the platform user-friendly for all. The Tokens is surety to be discrete and transferable across users via the unique identifier on the blockchain.

4.2 Wallet Integration

This NFT Management System has a function for Wallet Connectivity, which lets users safely link their MetaMask wallets to the decentralized app without disclosing their private keys, is a vital feature. This is accomplished by using MetaMask [9], a well-known browser addon that serves as a medium between the webapp window and wallet. The NFT webapp gives message users to connect their wallet with the help of MetaMask when they first access it. After connecting, the user does not need to manually enter their private keys to use the dApp's functionalities, such minting and creating NFTs. This removes the possibility of theft of any of your intellectual property. To build this amazing project we have incorporated two public libraries with the NFT Marketplace App that are React.js [10] and Ether.js [11], a popular library for performing operations on Ethereum-chain. This step makes gives us functionality to connect the dApp with its user's cryptocurrency wallets through the MetaMask. The Ether.js library provides some methods for sending and receiving data from the chain, making it possible for us to connect the App with ethereum [12] network.

4.3 Generator Function






The main task of our project is to create a block for the new transaction based on some input parameters given by user. We have made an API, which gives us direct

access to a pretrained DALL-E model that can create images from text prompts, to implement this feature. An NFT is created by the user entering a keyword or phrase that represent the message from the user about your asset or transaction. These form data are sent with the help of our backend server, which uses the DALL-E model to create a unique image by interacting with the OpenAI API. This model allows to produce various and high-quality images. Additionally, the concept enables the construction of distinctive, personalised NFTs that are difficult to duplicate. Blockchain technology offers security, immutability and decentralised database are combined in the NFT generation process to create unique and valuable digital assets. Through the utilisation of these methods, the NFT Marketplace decentralized App offers customers a distinctive and thrilling method to generate, possess, and exchange NFTs.

4.4 NFT-Minting

On the blockchain, users can save and market exclusive intellectual properties assets thanks to the NFT generator function. We are used IPFS to store our data in decentralized way of storing, the Ethereum development environment by Hardhat, and the Ai model in tandem to develop this feature. The user must first enter the necessary data to generate image before creating an NFT. The minting procedure begins when the user clicks the "Transfer" button then after the transaction is done. Next, the smart contract's mint function is triggered, which generates a new block on the Ethereum test chain and. The token's qualities, includes the sender address, receiver address and the amount of Ethereum, and the timestamp of transaction, are also specified in the smart contract.

NFT is now available for viewing on the Marketplace and is formally minted. Anyone can read the name, description, price, and image of the NFT by accessing the metadata URI that is maintained on IPFS. The NFT's uniqueness and ability to be transferred between users are guaranteed by the token ID on the blockchain.

| | | | | |
|-------------------------|---|---------|-----|------|
| eth_chainId |  | Success | 200 | 19ms |
| eth_getTransactionCount |  | Success | 200 | 33ms |
| eth_feeHistory |  | Success | 200 | 38ms |
| eth_getBlockByNumber |  | Success | 200 | 25ms |
| eth_estimateGas |  | Success | 200 | 40ms |

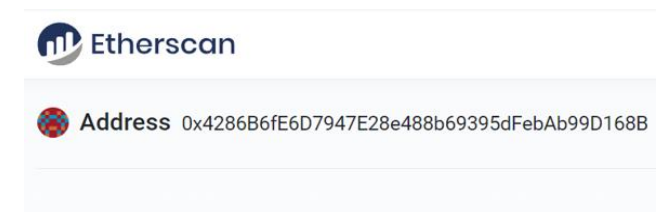
4.5 Network & Testnet

We thoroughly tested our NFT Marketplace dApp on Ethereum test networks like Testnet and Sepolia to guarantee its dependability and security. Testnet, which uses test ETH from faucets like Testeth Faucet, enables

developers to implement and test smart contracts without actual financial risk. For testing intricate dApps, Sepolia, a more recent test network, provides better performance and stability. Before going live on the mainnet, our test networks allow for thorough debugging and optimization, ensuring that our marketplace runs smoothly and that our smart contracts are reliable. By using test ETH from faucets, we can ensure that our testing procedures accurately reflect real-world scenarios without having to pay real money.

4.6 Smart Contract

Deploying a smart contract using Hardhat involves several key steps. First, install Hardhat and initialize a new project using `npx hardhat`. Write the smart contract in Solidity, then compile it using `npx hardhat compile`. Next, create a deployment script in the script's directory. This script uses the Hardhat Runtime Environment (HRE) to deploy the contract to the Ethereum network. Run the deployment script with `sepolia` network configuration. Ensure your network configuration is set up correctly in `hardhat.config.js`. Upon successful deployment, Hardhat logs the contract address.

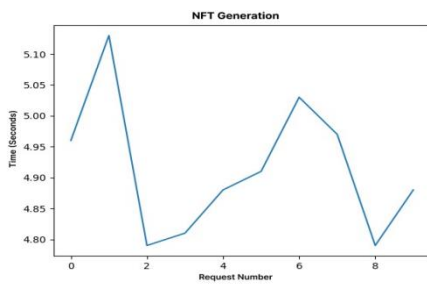


5. RESULT ANALYSIS

In this section, we are showcase the results for our project and its performance and subsystem's analysis. The Sepolia testnet's smart contract transactions were used to mint NFTs, and the time system took to produce response to our generating request was measured as part of the performance test [3]. Ten users from throughout the testing batch were polled for the performance study in order to assess the marketplace's smoothness in operations, connectivity, and robustness as well as the hashing message procedure and general use case scenario. To better highlight the results, we provide the research results as bar graphs. Additionally, feedback was gathered on the ease of navigation and the intuitiveness of the user interface. The performance data is presented alongside these findings to offer a comprehensive view of the system's efficiency and user satisfaction. This analysis aims to identify areas for improvement and validate the overall effectiveness of our NFT marketplace platform.

5.1 Performance Analysis

In order to generate NFT images for the performance test, AI models were used, and contract transactions on the Sepolia test network were used to mint NFTs.



Time Graph for performance

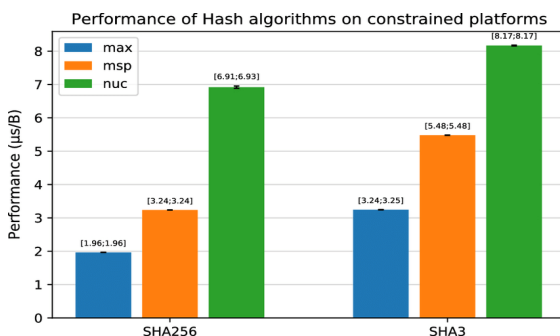
To see the performance test results, we displayed two graphs. The graphs' x-axis displays the number of distinct requests send through us, and the y-axis displays the waiting time for the completion of every request.

5.2 Demonstrating MetaMask Functionality

Here, we provide examples of MetaMask transactions using sender and recipient screenshots. Make sure MetaMask is first configured and linked to a network. Put cryptocurrency into each wallet. By confirming the amount and petrol fee, as well as the recipient's address, the sender starts the transaction. The recipient then checks their MetaMask wallet to confirm the receipt. Both parties have the option to examine the transaction using a blockchain explorer such as Etherscan.

5.3 Algorithm - SHA256

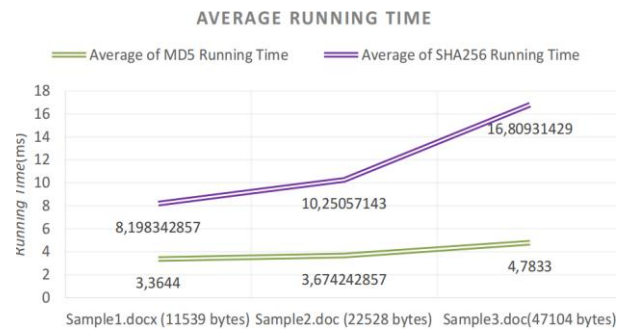
SHA256 comes from the family of SHA2 algorithms which are algorithms that performs hashing on the data for data integrity and security. It was made by the NSA and released NIST in the year 2001. With the ability to produce a 256-bit hash value from any amount of input data, it guarantees a high degree of security for a variety of uses, such as password hashing, digital signatures, and certifications.



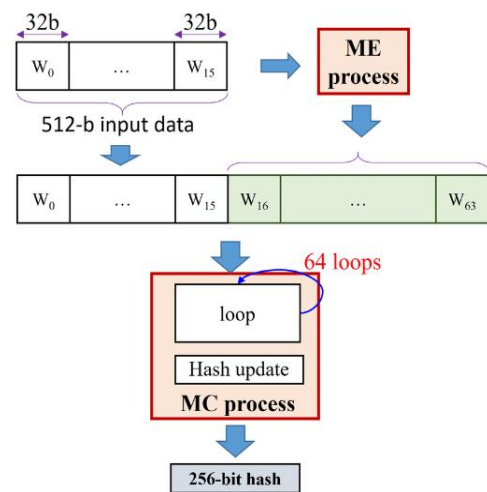
5.4 Why SHA256?

A message digest in blockchain is a fixed-size numerical representation (hash) of a data point produced by a hash function. It functions as a digital fingerprint, enabling users to confirm that the data has not been changed, so guaranteeing data integrity. The hash functions SHA-256

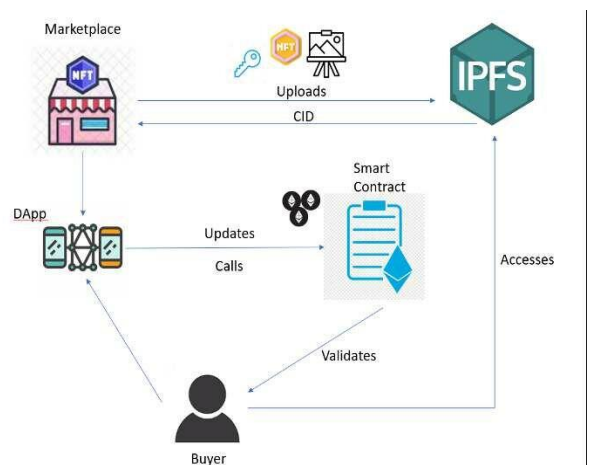
and SHA-3 are often utilized. SHA-256 is considered "almost unique" because it will likely produce a different hash for each different input message.



5.4 Architectural Designs



Architecture of SHA256



Transaction Data flow

6. FUTURE WORK

While the NFT dApp offers a new approach to secure digital way of fund transfer and management using hardhat development technology on Ethereum and AI

models, there are many limitations that are there in the idea as scalability as blockchains are difficult to expand and the second most concerning issue is the energy consumption as it takes lot of energy to create a block on chain as a part of its consensus mechanism be addressed in future iterations of the app. First, the NFT creation process is currently limited to the API. Future work could include developing custom learning models that are better suited for custom generation task and can handle a wider range of input types. Second, the application is currently deployed on the sepolia Testnet, which allows secure and controlled testing, but limits scalability and real-world applicability. Future work may include bringing the dApp to the web to enable real NFT trading. It does not support Tokens resale, which is an important function of crypto markets. Future work could include developing a secure and open mechanism for NFT resale. Finally, the user interface can have many more features like a storage vault and a system to embed social media platforms be further refined to improve user experience and accessibility by adding improved design and usability principles and additional features such as social sharing can help in community building and innovating our current market with trust issues.

7. CONCLUSION

In conclusion, we can say the NFT Management System Webapp development shows the potential of crypto currencies and blockchain technologies and AI models to create robust, secure, transparent, and friendly platforms to manage and sell or buy our assets. Our dApp reports several issues in NFT management system, including secure wallet for crypto, block generation on the blockchain, and NFT trading application. The integration of the image generating API with the Ethereum network made it possible to create unique NFTs that are not easy to copy, thus creating valuable and unique assets. The studies show that our dApp is easy to use. In the upcoming years the directions for research and development in this area will include improving the scalability and the adaptation in our current banking system. exploring new areas where we can use tokens to pay for services. Overall, our NFT Marketplace application is an important step forward in the development of decentralized applications for token and fund management and transaction management.

REFERENCES

- [1] Choi, N., & Kim, H. (2019). A Blockchain-based User Authentication Model Using MetaMask. *Korea Science*, 5(9), 6016-8896.
- [2] DeVries, P. D. (2016). An analysis of cryptocurrency, bitcoin, and the future. *International Journal of Business Management and Commerce*, 1(2), 1-9.

- [3] Pamu, D., Harshad, Birari, T., Kadam, T., & Kedare, N. (2022). Survey Paper on Decentralized Crypto Wallet Application using Ethereum Ledger. *International Journal of Advance Research, Ideas and Innovations in Technology*, 8(6), 496-499.
- [4] Yadav, N. S., Goar, V. K., & Kuri, M. (2020). Crypto Wallet: A Perfect Combination with Blockchain and Security Solution for Banking. *International Journal of Psychosocial Rehabilitation*, 24(2), 6056-6066.
- [5] Di Angelo, M., & Salzer, G. (2020). Wallet Contracts on Ethereum. In *Tokenized Securities and Crypto Enforcer* (pp. 95-115). Apress, Berkeley, CA.
- [6] Martiny, A. (2021). MetaMask Tutorial: One-click Login With Blockchain Made Easy. <https://www.toptal.com/ethereum/one-click-login-flows-a-metamask-tutorial>
- [7] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.
- [8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [9] "The crypto wallet for Defi, Web3 Dapps and NFTs — MetaMask." *Metamask.io*, 2023. Retrieved from <https://metamask.io/> (accessed Apr. 09, 2023). [10] "Getting Started - React." *Reactjs.org*, 2021. Retrieved from <https://legacy.reactjs.org/docs/getting-started.html> (accessed Apr. 09, 2023).
- [11] "Documentation." *Ethers.org*, 2023. Retrieved from <https://docs.ethers.org/v5/> (accessed Apr. 09, 2023).
- [12] "Ethereum Developer Resources — ethereum.org." *Ethereum*.
- [13] "OpenAI API." *Openai.com*, 2023. Retrieved from <https://platform.openai.com/docs/> (accessed Apr. 09, 2023).
- [14] "Express - Node.js web application framework." *Expressjs.com*, 2017.
- [15] Contract ABI Specification. Retrieved from <https://docs.soliditylang.org/en/latest/abi-spec.html#>
- [16] Contract ABI Specification. Retrieved from <https://docs.soliditylang.org/en/latest/abi-spec.html#>
- [15] Contract ABI Specification. Retrieved from <https://docs.soliditylang.org/en/latest/abi-spec.html#>
- [16] Sepolia Network. (n.d.). Retrieved from <https://sepolia.etherscan.io/>

[17] Deploy smart contract. (n.d.). Retrieved from <https://docs.alchemy.com/docs/hello-world-smart-contract>

[18] Shafique, M., Khurram, M., Amjad, F., & Khalid, H. (2020). Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. In *IEEE International Conference on Communications (ICC)* (pp. 1-6). Dublin, Ireland.
doi:10.1109/ICC40277.2020.9149359

[19] IEIE Transactions on Smart Processing and Computing. (2022). IEIESPC, 11(5), 385-391.
<https://doi.org/10.5573/IEIESPC.2022.11.5.385>