SAPIENZA
UNIVERSITÀ DI ROMA

Donuts Games - Report

A game-based decentralized app

Cybersecurity course - Blockchain and Distributed Ledgers project

Students:

Andrea Nisio - 1993155
nisio.1993155@studenti.uniroma1.it

Federico Giustozzi - 1692615
giustozzi.1692615@studenti.uniroma1.it

Stefano Bruonori - 1802004
brunori.1802004@studenti.uniroma1.it

Academic Year 2022/2023

Contents

1 Preface

As part of a university blockchain project, we developed a decentralized application (DApp) that offers an engaging experience through mini-games like Tetris, Minesweeper, and Snake. Players compete to earn Donuts (DNT) tokens, which can be used to purchase unique NFTs, traded for Ethereum (ETH), or acquired by answering quizzes on topics such as Blockchain, Smart Contracts, and Ethereum. The integration of gaming with blockchain technology provides users with a dynamic platform where they can have fun while gaining and trading digital assets. Additionally, users can monitor their progress and standings through a dedicated "scores" section within the DApp.

- **Andrea Nisio**:
  - Solidity Development
  - JavaScript Development
  - Architectural Design
  - Documentation Design
  - Presentation
- **Stefano Brunori**:
  - Solidity Development
  - JavaScript Development
  - Token Engineering
  - Presentation
- **Federico Giustozzi**:
  - HTML Front-end Development
  - JavaScript Development
  - Presentation

This report outlines the development and functionality of our decentralized application (DApp) designed for a university blockchain project. It details the system architecture, from front-end design to back-end implementation, and the integration of smart contracts and token systems. The report also covers the deployment process, testing methodologies, and documentation provided, concluding with an evaluation of the project's success and suggestions for future improvements.

2 Background

Blockchain technology, originally introduced as the underlying system for Bitcoin, has evolved into a versatile and disruptive innovation. The concept of a blockchain dates back to the early 1990s when Stuart Haber and W. Scott Stornetta proposed a system to timestamp digital documents to prevent backdating or tampering. However, it was not until 2008, when an individual or group under the pseudonym Satoshi Nakamoto published the Bitcoin white paper, that the blockchain concept was formalized and implemented as the foundational technology for cryptocurrency.

The rationale behind blockchain technology is to create a decentralized ledger that records transactions across a distributed network of computers. This approach enhances security and transparency by eliminating the need for a central authority and reducing the risk of single points of failure. Blockchain operates on the principle of consensus, where network participants agree on the validity of transactions through various mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS). Each transaction is recorded in a "block," which is then cryptographically linked to the previous block, forming a continuous "chain" of blocks. This structure ensures that once data is recorded, it cannot be altered without altering all subsequent blocks, thus providing a high level of security and integrity.

Key concepts in blockchain technology include:

- **Decentralization**: Unlike traditional centralized databases, blockchain distributes data across a network of nodes, ensuring that no single entity has control over the entire database.
- **Consensus Mechanisms**: Techniques like Proof of Work (PoW) and Proof of Stake (PoS) are used to validate and agree on transactions within the network, maintaining data consistency and security.
- **Immutability**: Once data is recorded in a blockchain, it is extremely difficult to alter or delete, providing a permanent and tamper-evident record.
- **Smart Contracts**: Self-executing contracts with the terms of the agreement directly written into code, allowing for automated and trustless transactions between parties.

2.1 Application Domain

The application domain of blockchain technology extends far beyond its initial use case in cryptocurrency. Its potential to transform various industries is becoming increasingly evident as organizations explore its benefits for enhancing transparency, security, and efficiency.

In the financial sector, blockchain is revolutionizing traditional banking and payment systems by enabling faster, more secure transactions with reduced costs. Decentralized Finance (DeFi) platforms leverage blockchain to offer financial services such as lending, borrowing, and trading without intermediaries, thus democratizing access to financial resources.

Supply chain management is another area where blockchain technology is making significant strides. By providing an immutable record of each transaction and movement within the supply chain, blockchain enhances traceability and accountability. This capability helps in verifying the authenticity of goods, reducing fraud, and improving overall efficiency in logistics.

Healthcare is also experiencing transformative changes due to blockchain. The technology can securely manage patient records, ensuring that data is only accessible to authorized individuals while maintaining privacy and compliance with regulations such as GDPR and HIPAA. Additionally, blockchain can facilitate secure sharing of medical research data, accelerating the development of treatments and fostering collaboration among researchers.

In the realm of digital identity, blockchain offers a solution to the problem of identity theft and data breaches. By providing a decentralized and secure way to manage digital identities, individuals can have greater control over their personal information and reduce the risk of unauthorized access.

Overall, the application domain of blockchain technology is vast and growing. Its ability to provide secure, transparent, and efficient solutions has the potential to disrupt and enhance various sectors, driving innovation and creating new opportunities for businesses and individuals alike.

3 Context Presentation

The primary aim of our decentralized application (DApp) is to create an engaging and rewarding platform that combines gaming with blockchain technology. By integrating classic mini-games such as Tetris, Minesweeper, and Snake, the DApp not only provides entertainment but also incentivizes player participation through a unique token economy.

The DApp allows players to earn Donuts (DNT) tokens based on their performance in these games. These tokens can then be used to purchase exclusive NFTs, which represent unique digital assets within the platform. Additionally, players have the option to trade DNT tokens for Ethereum (ETH), thereby bridging the gap between virtual rewards and real-world value. Another significant feature of the DApp is the inclusion of quizzes related to blockchain technology. Players can earn DNT tokens by correctly answering questions on Blockchain, Smart Contracts, and Ethereum, further enhancing their engagement and knowledge.

By combining gaming with a blockchain-based reward system, the DApp aims to:

- **Engage Users**: Provide an interactive gaming experience that keeps users entertained while incentivizing their participation with valuable rewards.
- **Educate Users**: Offer educational content in the form of quizzes to improve users' understanding of blockchain technology.
- **Create Value**: Enable users to earn and trade digital assets, adding real-world value to their achievements within the platform.

Overall, the DApp seeks to merge fun and functionality, creating a compelling platform that not only entertains but also educates and rewards its users.

3.1 Why Using a Blockchain, and What Type Thereof to Use in Production

Blockchain technology is central to the functionality and value proposition of our DApp. The decision to use a blockchain was driven by several key factors:

- **Decentralization**: Blockchain provides a decentralized framework, ensuring that the game data and token transactions are not controlled by a single entity. This decentralization enhances transparency and reduces the risk of fraud or manipulation.
- **Security**: Blockchain's cryptographic nature ensures that transactions are secure and tamper-proof. Each transaction is recorded in a block and linked to previous transactions, making it nearly impossible to alter past records.

- **Transparency**: All transactions and token transfers are publicly recorded on the blockchain, allowing for full transparency. This transparency builds trust among users and ensures the integrity of the reward system.
- **Token Economy**: Blockchain enables the creation and management of digital tokens (DNT) that can be used within the platform. These tokens can be traded or redeemed for real-world value, providing users with tangible benefits.

When choosing the type of blockchain for production, several factors need to be considered:

- **Public vs. Private Blockchains**: For our DApp, a public blockchain like Ethereum is preferred due to its widespread adoption, security features, and support for smart contracts. Public blockchains offer greater transparency and are more suitable for applications that require open and trustless interactions.
- **Scalability and Cost**: While public blockchains provide numerous benefits, they may face issues related to scalability and transaction costs. To address these challenges, Layer 2 solutions such as rollups or sidechains can be considered to enhance scalability and reduce costs without compromising security.
- **Smart Contract Support**: The chosen blockchain must support smart contracts, which are essential for automating token transactions and implementing game logic. Ethereum, with its robust support for smart contracts, is a suitable choice for this purpose.

In conclusion, the use of blockchain technology is pivotal for achieving the goals of our DApp, providing a secure, transparent, and decentralized platform. Ethereum, with its support for smart contracts and its established ecosystem, is the chosen blockchain for production, ensuring that the DApp meets its objectives effectively and efficiently.

4 Software Architecture

4.1 Deployment Diagram

The deployment diagram provides an overview of the distribution and interaction of the components within our decentralized application (dApp). This visual representation is crucial for understanding how the different parts of the system connect and collaborate to deliver a functional and cohesive application.

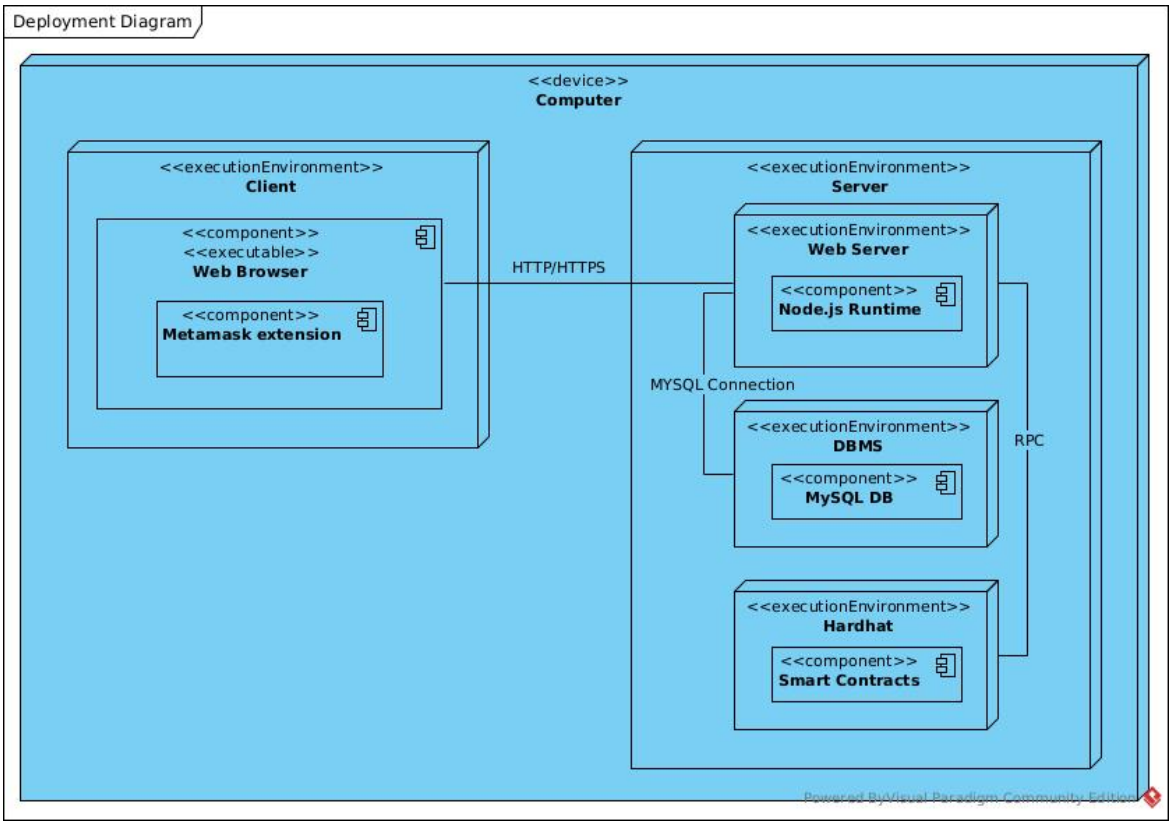

Figure 1: dApp Deployment Diagram

Our dApp is designed as a web application using JavaScript and Handlebars (hbs). Users interact with the dApp through this web interface, which is supported by client libraries such as Web3.js or Ethers.js for blockchain interactions and MetaMask for transaction management.

The blockchain management is facilitated by smart contracts deployed on the Ethereum network. These smart contracts handle the management of tokens (DNT), processing of NFT transactions, and recording of game scores. Hardhat, a development environment for Ethereum, is utilized for deploying and testing these smart contracts.

Hardhat streamlines the development process by providing local blockchain environments,

debugging tools, and integration with the Ethereum network.

MetaMask, a browser extension wallet, allows users to connect their Ethereum wallets to the dApp securely. It provides a user-friendly interface for managing private keys and interacting with smart contracts on the Ethereum network.

The backend includes a Node.js API server and a MySQL database, managed via phpMyAdmin, to store essential data such as wallet-username associations and game scores. All components are hosted on cloud platforms, ensuring both scalability and availability.

This diagram offers a clear depiction of the connections and dependencies among these elements, aiding in the understanding of the architecture and supporting effective system management throughout the development and production phases.

4.2 Use Case Diagram

The use case diagram outlines key blockchain-driven interactions within the dApp, such as connecting the wallet via MetaMask, registering, participating in mini-games to earn tokens (DNT) by placing in the top three, and completing quizzes for token rewards. It also includes token transactions for buying and selling, all securely facilitated through smart contracts.

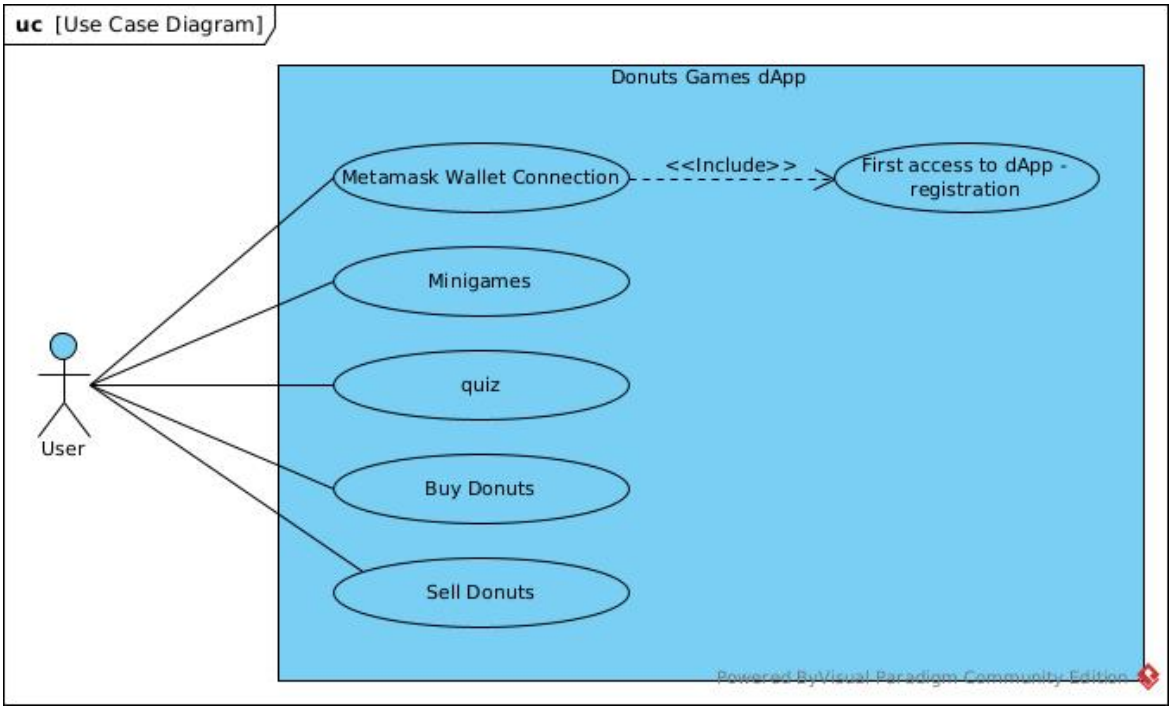

Figure 2: dApp Use Case Diagram

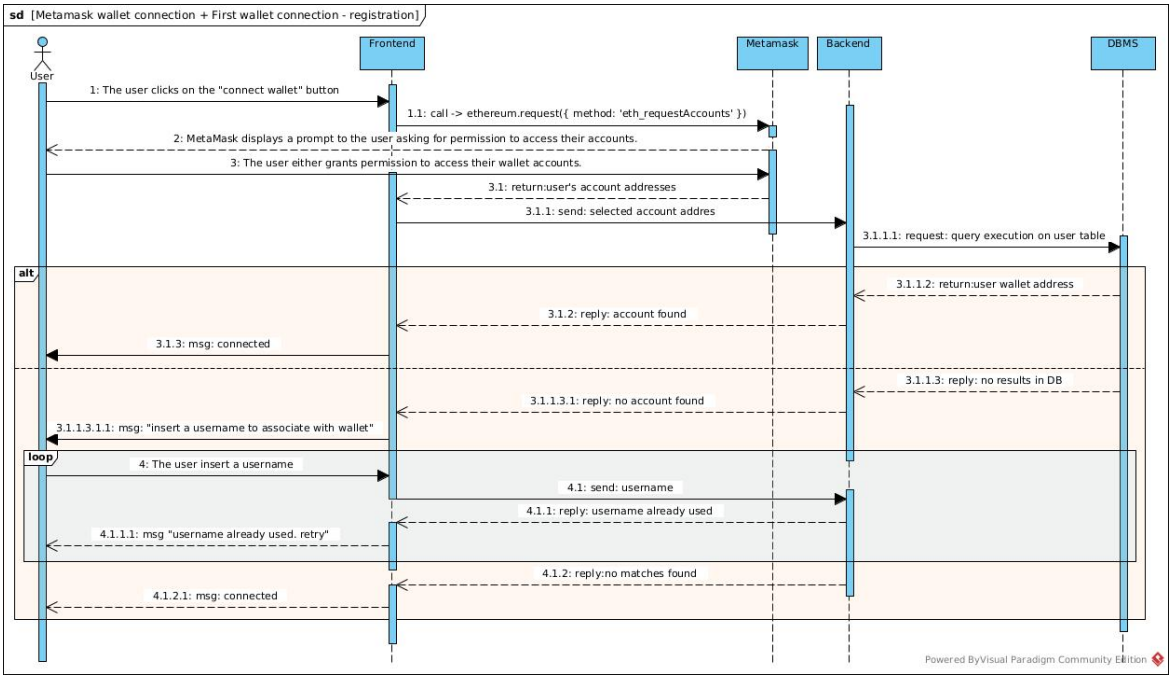

Figure 3: Wallet connection sequence diagram

5 Implementation

In the ever-changing digital landscape, we are witnessing a technology that has captured the attention of experts, media, and users worldwide: deepfakes...

6 Known Issues and Limitations

In the ever-changing digital landscape, we are witnessing a technology that has captured the attention of experts, media, and users worldwide: deepfakes...

7 Conclusions and Future Remarks

In the ever-changing digital landscape, we are witnessing a technology that has captured the attention of experts, media, and users worldwide: deepfakes...

References