Bilkent University
Department of Computer Engineering

Senior Design Project

T-2428
Satonic

Analysis and Requirement Report

Mehmet Berşan Özgür - 21902246 - bersan.ozgur@ug.bilkent.edu.tr
Ali Kaan Şahin - 22002932 - ksahin@ug.bilkent.edu.tr

5.12.2024

This report is submitted to the Department of Computer Engineering of Bilkent University in partial fulfilment of the requirements of the Senior Design Project course CS491/2.

Contents

Analysis and Requirement Report

Project Short-Name: Project Satonic

1 Introduction

The Ordinals Auction System, Satonic project aims to develop an innovative marketplace for Bitcoin Ordinals, leveraging Citrea, a Bitcoin rollup with a trust-minimized bridge. Ordinals function similarly to NFTs, tied to satoshis on the Bitcoin blockchain, but existing auction systems for them face usability challenges due to Bitcoin's script limitations. This project seeks to overcome those limitations by integrating the EVM ecosystem through Citrea, enabling seamless and efficient trading for collectors and traders. With a full-stack development approach, the project holds the potential to not only simplify Ordinals trading but also set the foundation for future innovation in Bitcoin-based digital assets.

2 Current System

Current platforms like Magic Eden allow users to trade Bitcoin Ordinals, but they face major challenges because they rely on Bitcoin's Script, which is very limited. Bitcoin Script cannot handle loops and other advanced operations, which makes it slow and expensive for activities like auctions. Transactions on these platforms often take a long time to process and cost a lot compared to other networks.

Satonic will solve these problems by using Citrea, a system that works alongside Bitcoin but handles most operations off-chain. Citrea uses Ethereum Virtual Machine (EVM) technologies to do the heavy work off-chain. This makes transactions much faster and cheaper. By also using zero-knowledge proofs for security, Satonic will provide a smoother, faster, and more affordable way to trade Bitcoin Ordinals.

3 Proposed System

The proposed system aims to create a user-friendly and efficient marketplace for trading Bitcoin Ordinals using Citrea, a Bitcoin rollup with EVM support. The platform will overcome the limitations of Bitcoin Script by handling operations off-chain, ensuring faster transactions and lower costs compared to existing solutions like Magic Eden. Users will be able to connect their wallets, view their NFTs, and participate in auctions seamlessly. The system will prioritize security with features like encryption and zero-knowledge proofs, ensuring user data and transactions remain private. The system will provide a scalable, reliable, and cost-effective solution tailored for the Bitcoin Ordinals community.

3.1 Overview

Satonic is a marketplace for Bitcoin Ordinals, created to solve the problems of current platforms by using Citrea, a Bitcoin rollup with EVM support. It helps users trade Ordinals faster and cheaper by handling operations off-chain while keeping transactions secure and private with zero-knowledge proofs. Satonic makes it easy for users to start auctions, place bids, and manage their NFTs with a simple and user-friendly design. By fixing the issues of Bitcoin Script and using modern technologies, Satonic offers a reliable and innovative solution for the growing Ordinals community.

3.2 Functional Requirements

- **User Authentication and Wallet Integration:** The system must allow users to link their Bitcoin wallets. As Ordinals NFTs are stored on-chain, with linking their wallet users will be able to display their owned NFTs.
- **Auction System for Ordinals:** Users must be able to list their Ordinals NFTs in the marketplace with configurable parameters(e.g., starting price, duration). The system must make real-time updates to ensure auction works as desired.
- **Transaction Management:** The platform must execute secure transactions when auctions end, transferring ownership of Ordinals. To ensure this system will use PSBT(Partially Signed Bitcoin Transaction) so that when the auction ends, the new owner will sign this PSBT, which is sector standart.
- **Marketplace Features**: Enable users to browse and search for desired Ordinals using filters. Each Ordinals NFT auction will possess its own page displaying detailed asset information
- **Administrative Panel:** Admins will be able to monitor transactions and users so that security can be ensured throughout the system.

3.3 Non-functional Requirements

- **Usability:** The platform will provide an easy user interface with clear navigation, allowing users to easily navigate and find what they want. User Interface will clearly indicate how to create an account, link wallet and participate in auctions
- **Reliability:** The system will unlikely to face problems as with using Citrea, the transactions and operations will be done off-chain on EVM. With doing that instead of running that operation on that local computer, the system will run it on EVM (Ethereum Virtual Machine).This approach minimizes dependency on local computing resources and ensures consistent and predictable outcomes.
- **Performance:** The platform will support real-time updates for bidding and auction states visible to all participants. Also as this platform uses Citrea, it will handle transactions off-chain using EVM technologies which fasten the process as transactions are too slow in Bitcoin blockchain. Citrea allows ZK (zero-knowledge) proof, significantly shortens the metadata to be written on transaction results in reduced gas fees.
- **Supportability:** The system will use modular architecture to facilitate easy updates, troubleshooting and integration of new features in the future. This will ensure, system is approached professionally.
- **Scalability:** The system will be designed to handle growth in user number. The system will have the ability to expand transaction processing capabilities as demand increases.

- **Security:** The system will leverage Zero-Knowledge (ZK) technology, ensuring high-level security without exposing sensitive details. This approach minimizes risks of data breaches.
- **Safety:** The system ensures safety by processing transactions off-chain using Citrea's ZK Rollup, which minimizes the risk of vulnerabilities. This approach ensures safety on transactions as sensitive data is not being exposed on-chain.

3.4 Pseudo Requirements (for devs (derived requirements))

- **Platform Accessibility:** The platform must be accessible through modern web browsers without requiring users to download any additional software or plugins. This ensures ease of use for traders.
- **Integration with Citrea:** The system must be compatible with Citrea's off-chain architecture to handle transactions efficiently and securely.
- **Scalability:** The platform should be designed to accommodate future growth, including an increase in the number of users and Ordinals traded.
- **User Security:** Basic user security measures, like encryption for transactions and secure user login, will be used. Zero-knowledge technology will also help keep user information private and secure by allowing transactions to be verified without sharing sensitive details. This will make the platform safer and more trustworthy.
- **Cost Efficiency:** The platform must maintain low operational costs for users, emphasizing its advantage over competitors like Magic Eden.

3.5 System Models

3.5.1 Scenarios

- **Create an Auction:** A trader wants to auction an Ordinal. They connect their wallet to the platform and click the "Create Auction" button. The trader selects the Ordinal from their wallet, sets the starting price, auction duration, and minimum bid increment. Once all details are confirmed, the trader submits the auction and the auction starts.
- **Bidding on an Auction:** A user browses the active auctions and finds an Ordinal they want to bid on. User clicks on the enter to auction button, and the system checks whether this user connected its wallet to the system. After the user is connected, they review the current highest bid and place a new bid that meets the minimum increment. The platform validates the bid, processes it, and updates the auction status instantly. The user receives a confirmation that their bid has been recorded.
- **Completing a Transaction:** When an auction ends, the platform determines the highest bidder and notifies both the seller and the winning bidder. The winning bidder sends payment through the platform, which finalizes the transaction. The Ordinal is then transferred to the winner's wallet, and the seller receives the payment, minus platform fees.

- **Displaying owned NFTs:** A user connects their wallet to the platform using the "Connect Wallet" button on the homepage. After successful connection, the platform retrieves the NFTs associated with the user's wallet. The NFTs are displayed on the user's profile page. Each NFT is shown with relevant details like metadata, ownership status providing the user with a clear view of their assets.

3.5.2 Use-Case Model

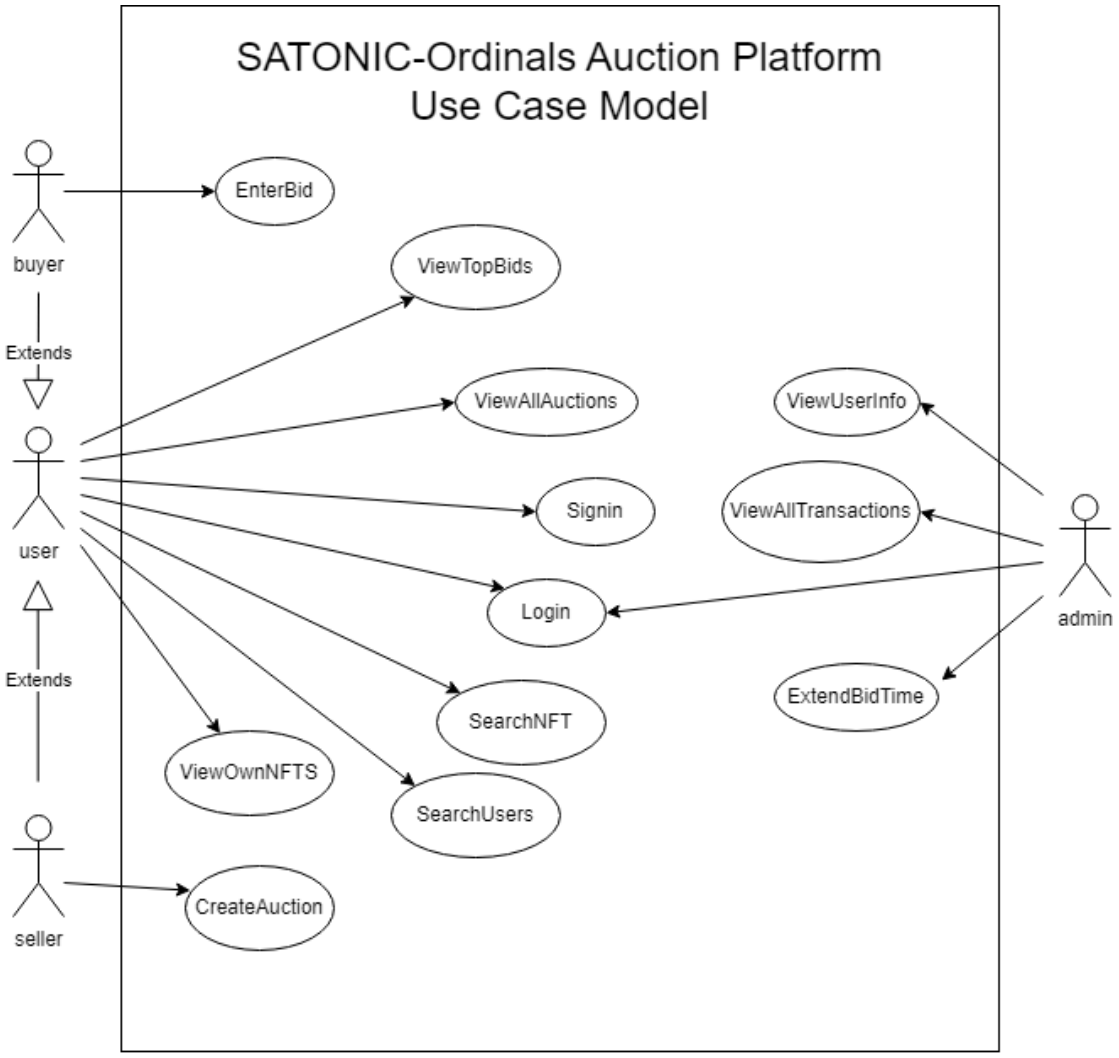

Figure 1. Use Case Model of Satonic

3.5.3 Object and Class Model

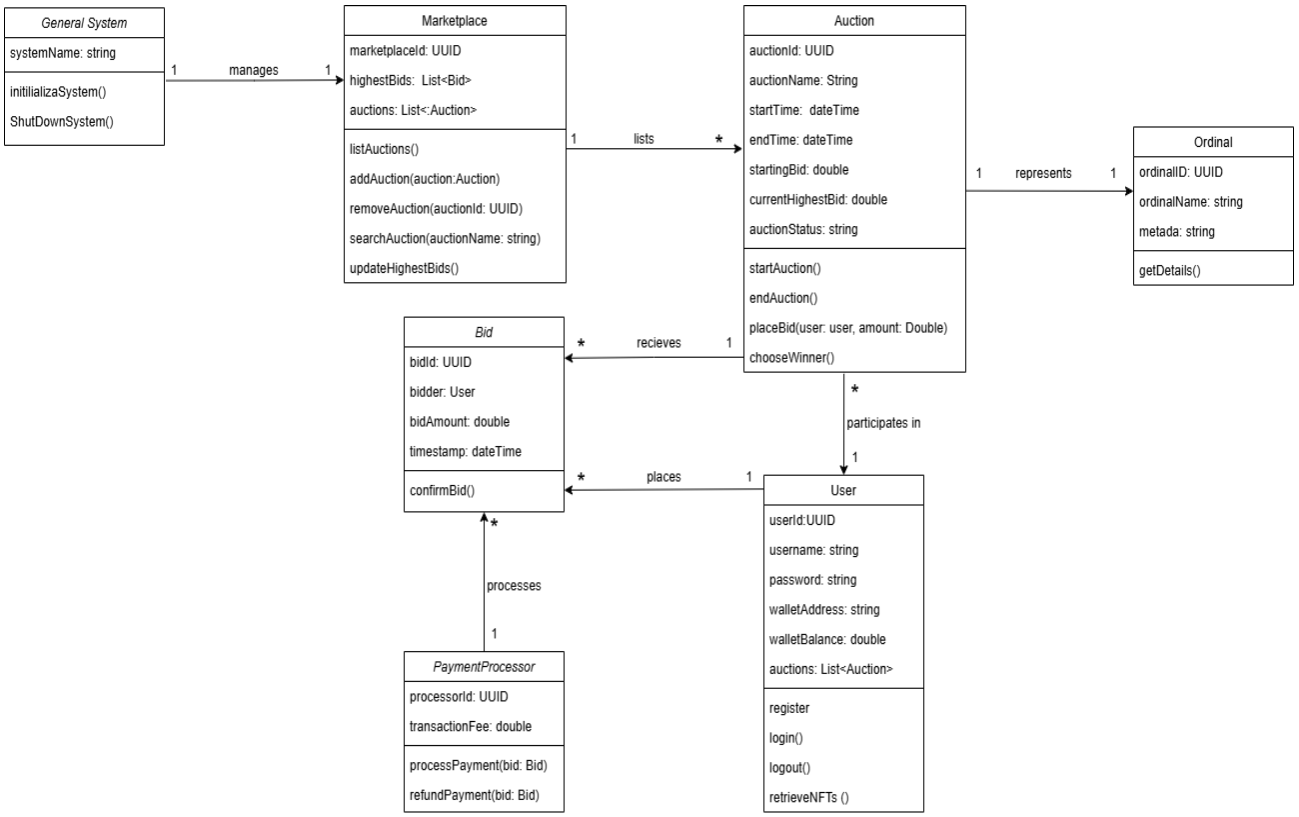

Figure 2. UML Class Diagram of Satonic

3.5.4 Dynamic Models

3.5.4.1 Sequence Diagram

3.5.4.1.1 Create an Auction

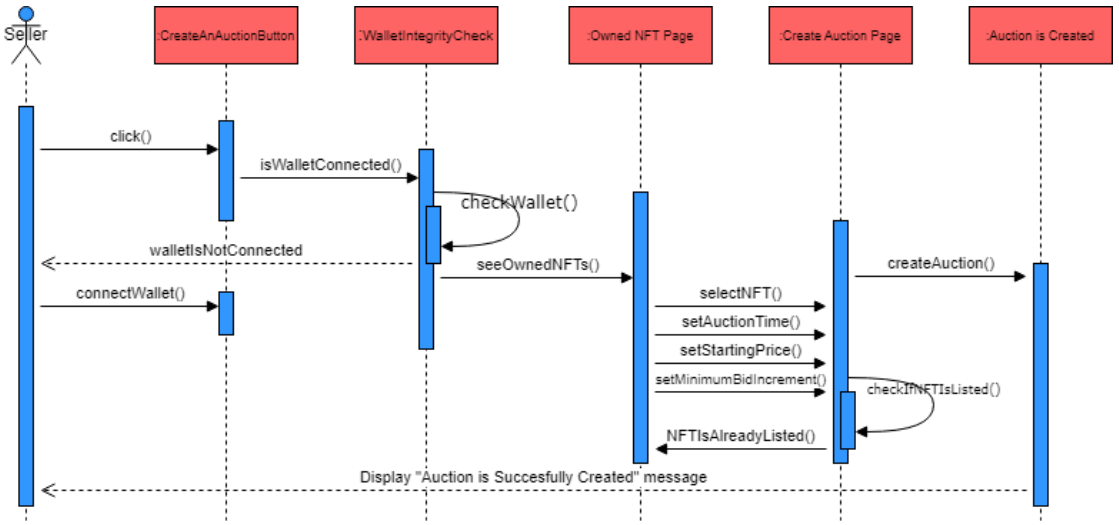

Figure 3. Auction Phase Sequence Model of Satonic

3.5.4.1.2 Bidding on an Auction

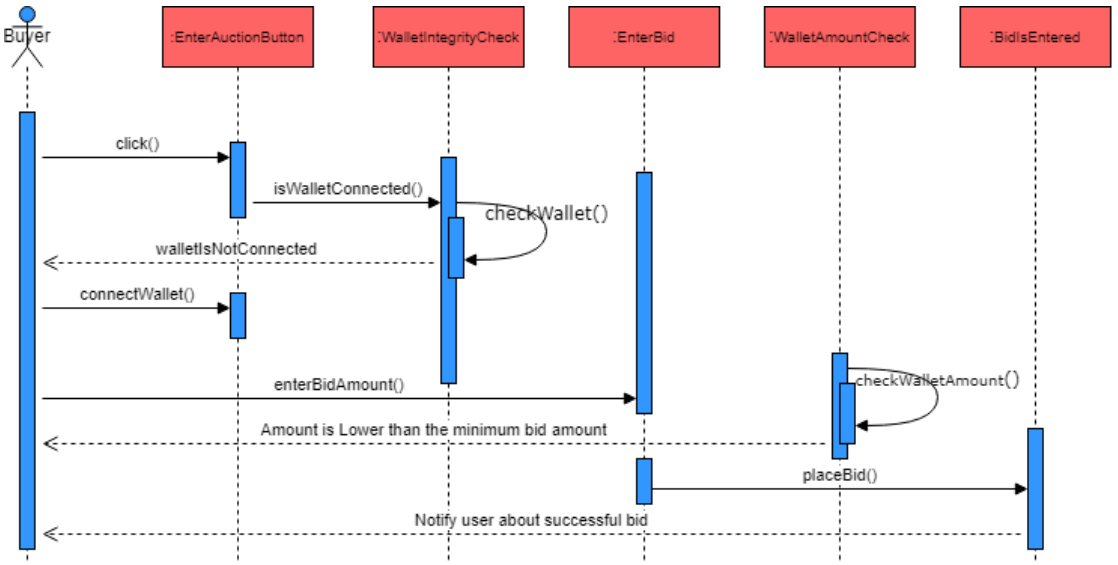

Figure 4. Bidding Phase Sequence Model of Satonic

3.5.4.1.3 Completing a Transaction

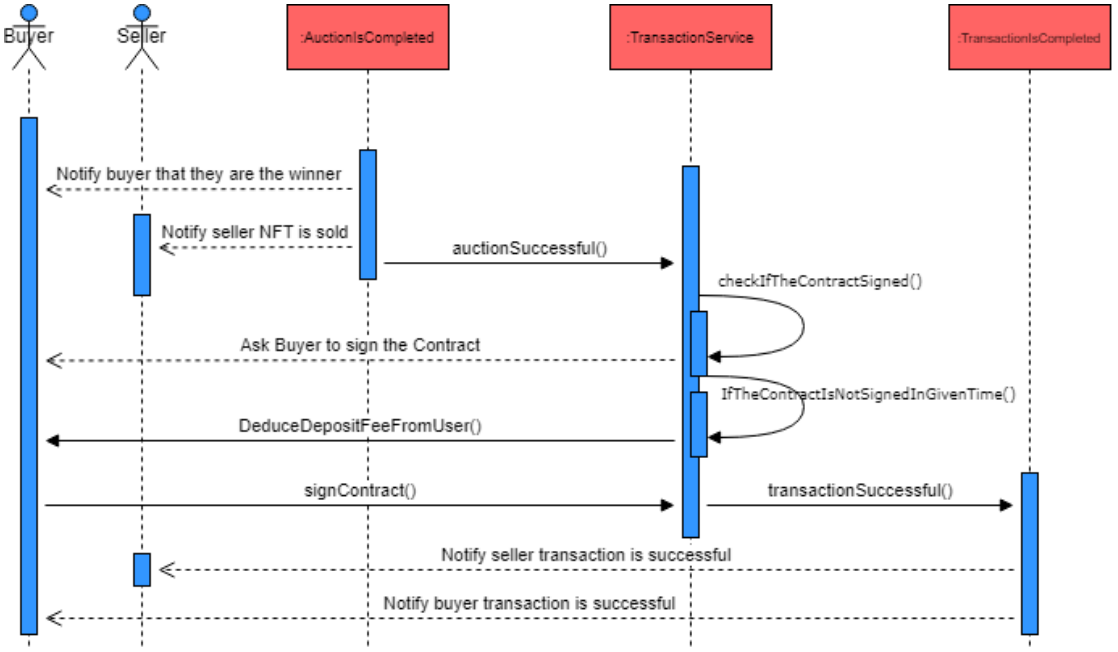

Figure 5. Transaction Phase Sequence Model of Satonic

3.5.4.1.4 Displaying owned NFTs

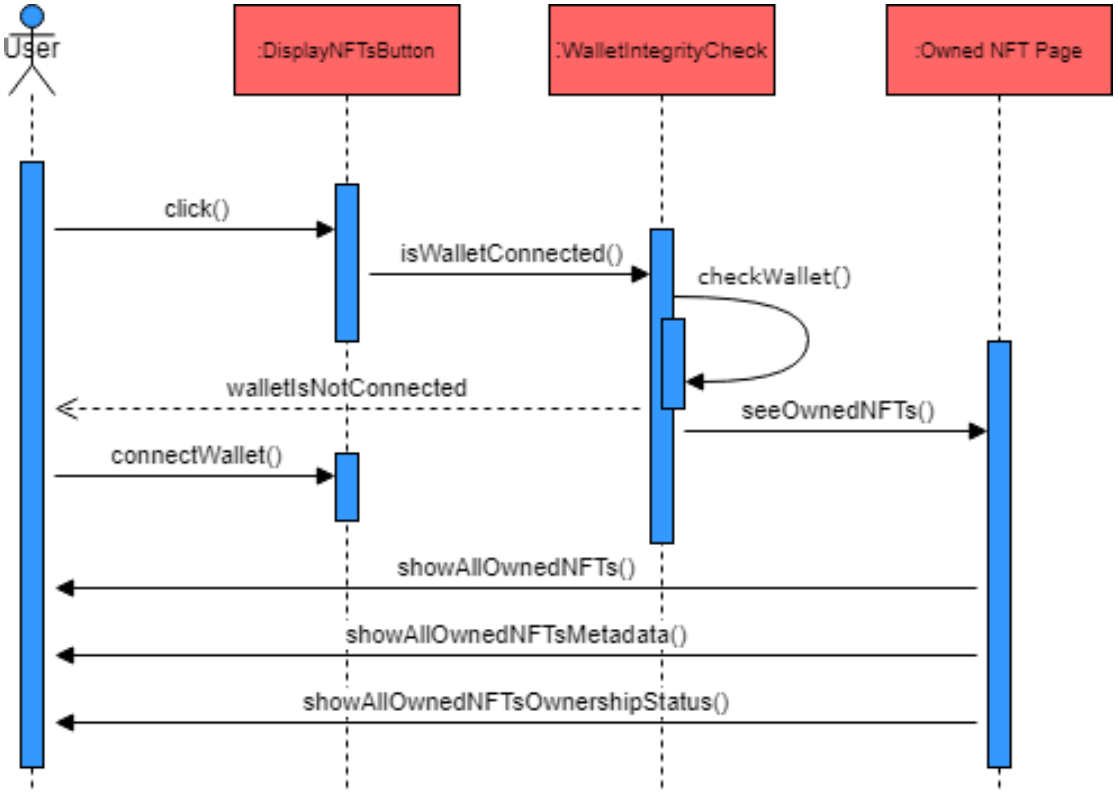

Figure 6. Sequence Model of Displaying NFT's in Satonic

3.5.4.2 State Diagram

3.5.4.2.1 Create an Auction

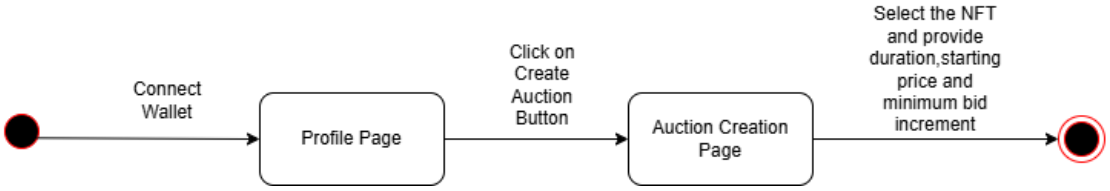

Figure 7. Auction Phase State Diagram of Satonic

3.5.4.2.2 Bidding on an Auction

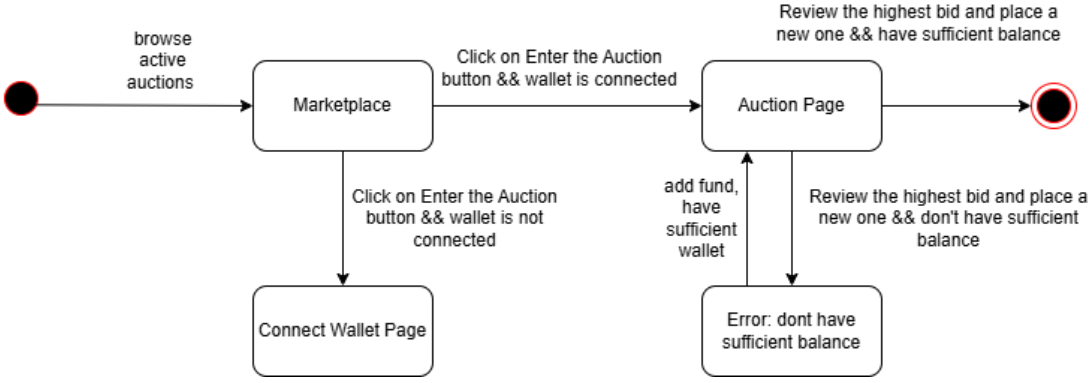

Figure 8. Bidding Phase State Diagram of Satonic

3.5.4.2.3 Completing a Transaction

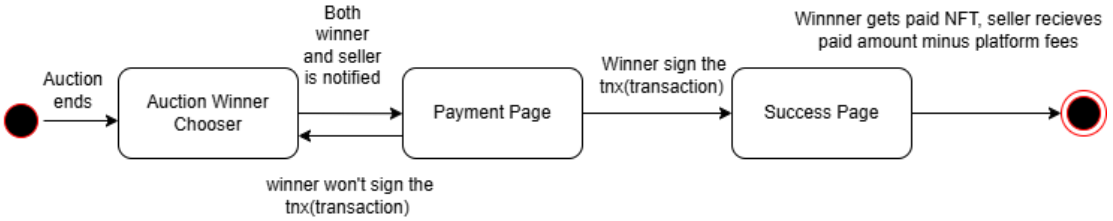

Figure 9. Transaction Phase State Diagram of Satonic

3.5.4.2.4 Displaying owned NFTs

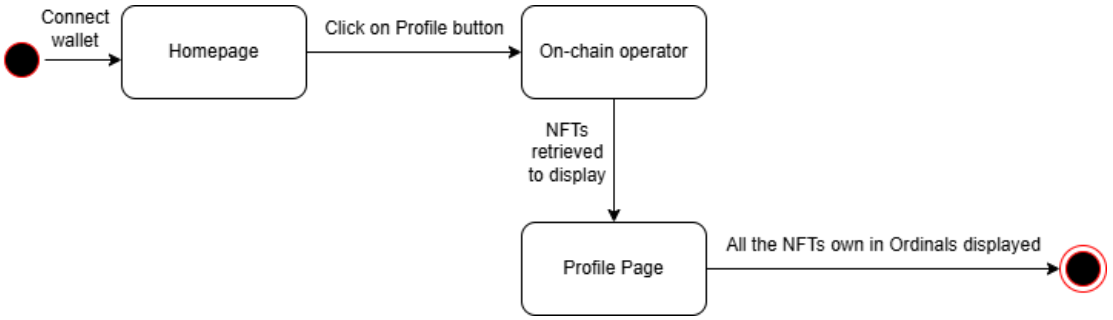

Figure 10. State Diagram of Displaying NFT's in Satonic

3.5.4.3 Activity Diagram

3.5.4.3.1 Create an Auction

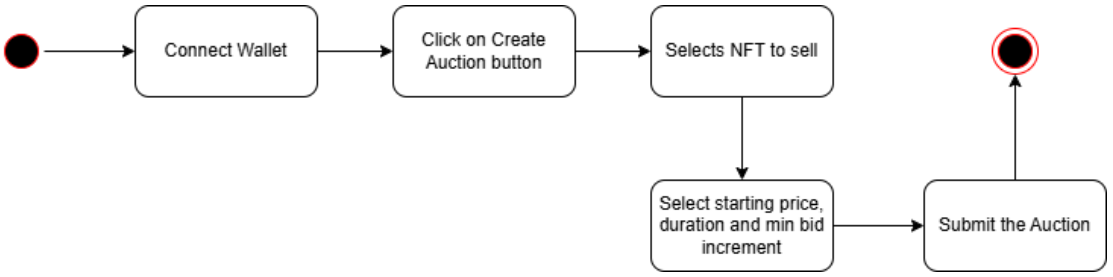

Figure 11. Auction Phase Activity Diagram of Satonic

3.5.4.3.2 Bidding on an Auction

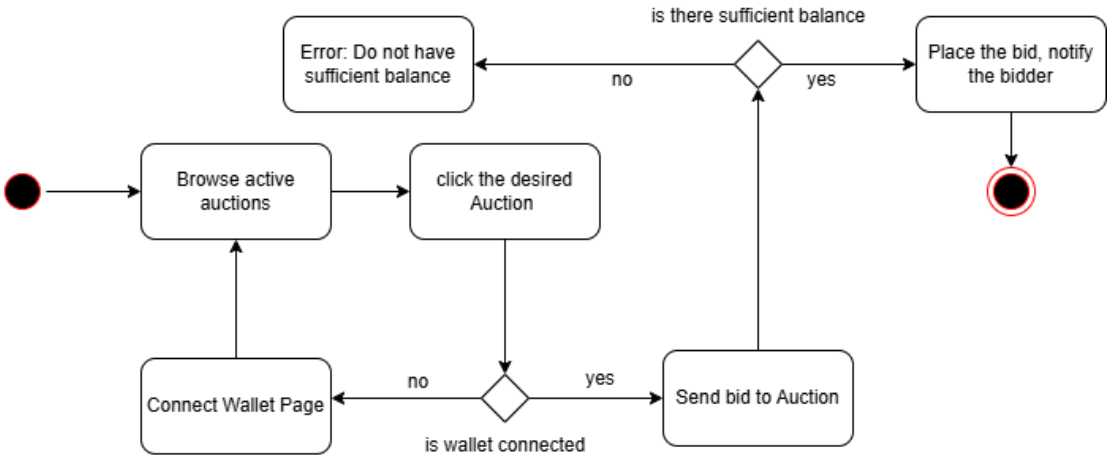

Figure 12. Bidding Phase Activity Diagram of Satonic

3.5.4.3.3 Completing a Transaction

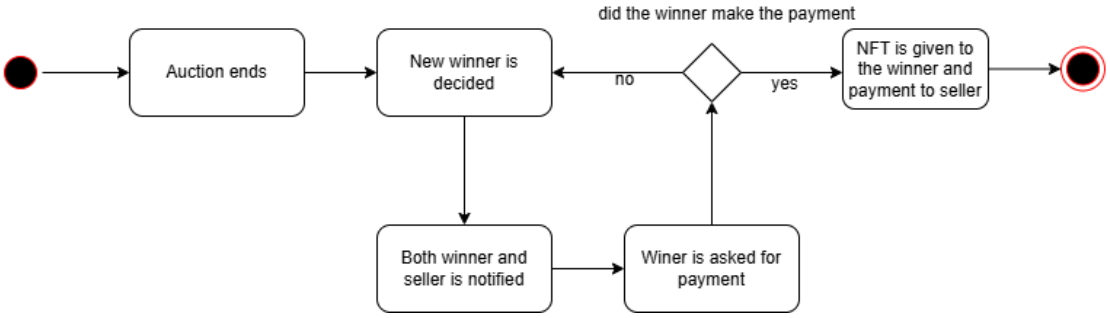

Figure 13. Transaction Phase Activity Diagram of Satonic

3.5.4.3.4 Displaying owned NFTs

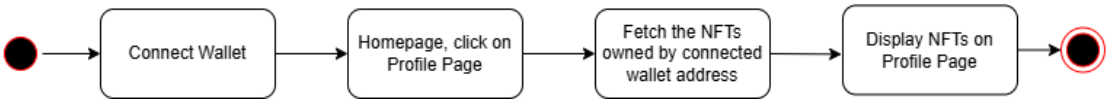

Figure 14. Activity Diagram of Displaying NFT's in Satonic

3.5.5 User Interface

Active Auctions Page:

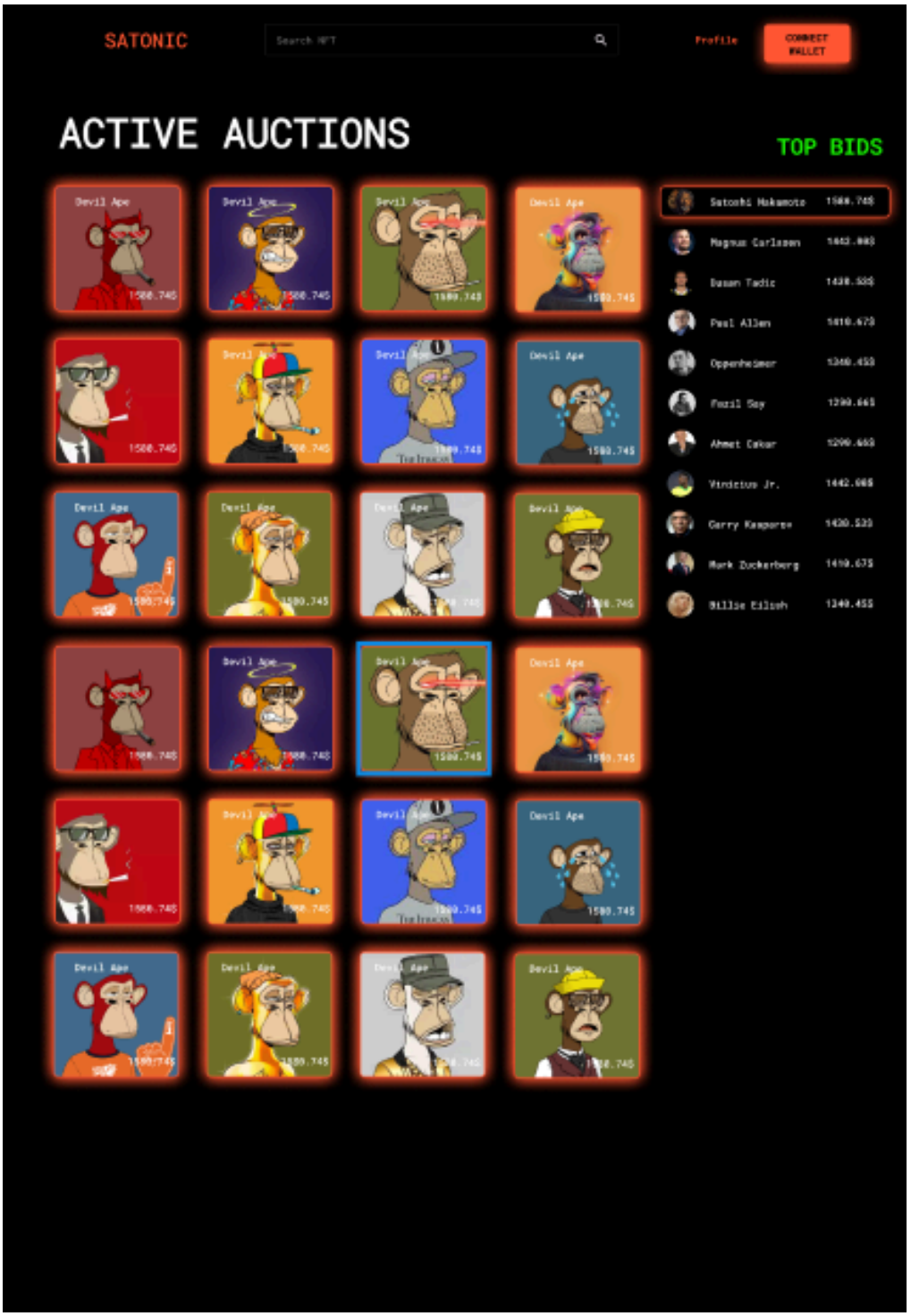

Figure 15. User's main auction page view in Satonic

Auction Page:

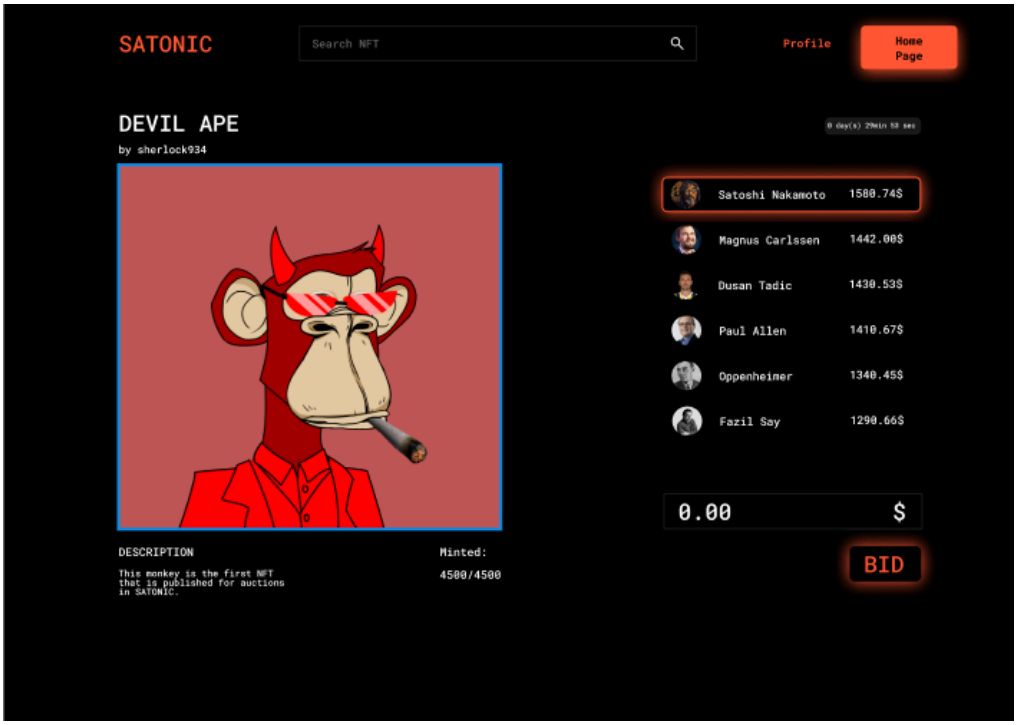

Figure 16. Auction Page of NFT in Satonic

Profile Page:

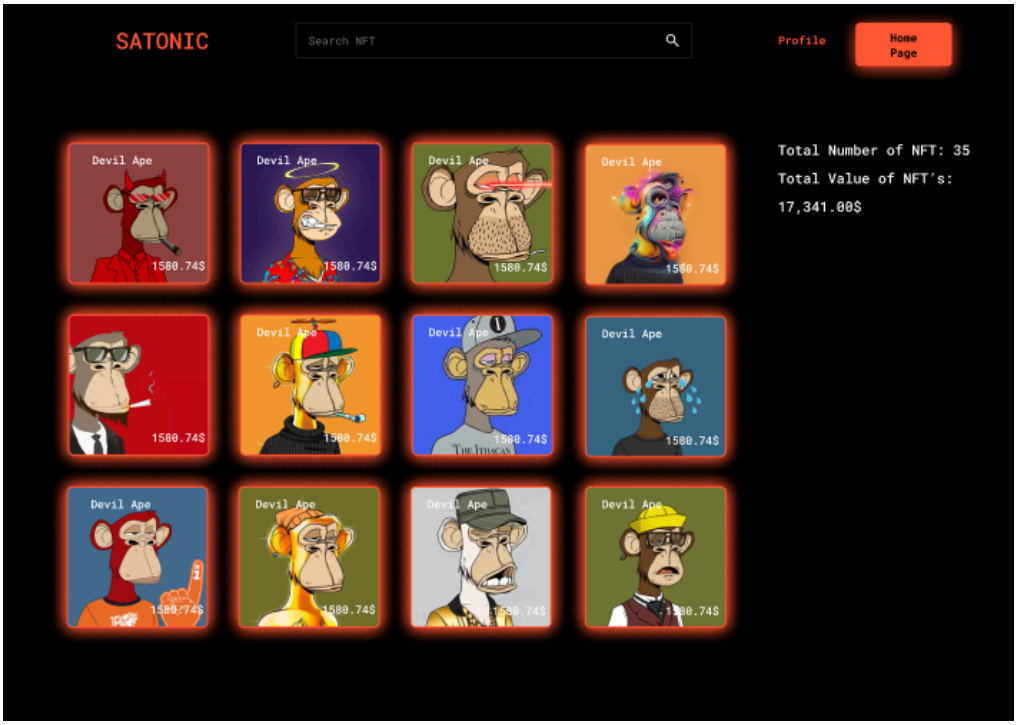

Figure 17. Profile Page of an User in Satonic

4 Other Analysis Elements

4.1 Consideration of Various Factors in Engineering Design

4.1.1 Constraints

4.1.1.1 . Implementation Constraints

- **Bitcoin Script Limitations:** Bitcoin's script language is non-Turing complete, which imposes strict constraints on transaction logic. Limited scripting makes it challenging to implement complex auction logic natively on Bitcoin. 2 Offloading auction logic to the EVM ecosystem must be done carefully to ensure security and minimize transaction overhead.

- **Trust-Minimized Bridge (Citrea):** Citrea's bridge requires robust security measures to prevent exploits such as double-spending or malicious attacks on cross-chain transactions. Any vulnerabilities in the bridge could compromise the integrity of the auction system and user funds.

- **Scalability and Transaction Fees:** Bitcoin Ordinals trading can be costly due to high fees during network congestion. The system must balance on-chain Bitcoin transactions and off-chain EVM transactions to maintain cost-effectiveness while ensuring reliability.

- **Latency in Cross-Chain Transactions:** Transferring data and assets between Bitcoin and the EVM ecosystem can introduce delays. Auctions rely on timing and precision, so latency could affect user experience and trust.

- **User Experience (UX):** Users accustomed to Ethereum-based NFTs might find Bitcoin-based Ordinals more complex due to differences in wallet management, UTXO model, and transaction workflows. The auction platform must simplify these processes to appeal to a broad audience.

- **Regulatory and Compliance Considerations:** Cross-chain systems are often scrutinized for potential regulatory violations (e.g., money laundering, tax evasion). The project needs to ensure compliance with local and international laws regarding digital assets and trading platforms.

- **Security Challenges:** Both the Bitcoin and Ethereum ecosystems are frequent targets for hackers. Multi-signature schemes, smart contract audits, and strong key management are necessary to ensure platform safety.

- **Full-Stack Development Requirements:**

  Frontend: A user-friendly interface for browsing, bidding, and managing Ordinals.

  Backend: Auction logic, payment processing, and bridge operations.

  Blockchain Integration: Smart contracts, Bitcoin UTXO handling, and EVM compatibility. Coordination across these layers requires expertise in both Bitcoin and Ethereum ecosystems.

- **Compatibility and Interoperability:** Ensuring that wallets supporting Bitcoin Ordinals can interact seamlessly with the system. Integration with existing Bitcoin Ordinals protocols and Bitcoin tools (e.g., Unisat) is crucial.
- **Auction System Design:** Designing auction mechanisms that accommodate Bitcoin Ordinals' unique nature (e.g., tied to specific satoshis). Preventing sniping, front-running, and other unfair practices in an auction environment.
- **Market Adoption and Liquidity:** Attracting sufficient buyers and sellers to create a liquid marketplace for Ordinals. Addressing potential resistance from Bitcoin maximalists who may oppose EVM integration.
- **Testing and Deployment:** Extensive testing is necessary for both the smart contracts and the Bitcoin bridge to ensure robustness and reliability. Deployment must include fallback mechanisms in case of system failures or bridge issues.

4.1.1.2 Economic Constraints

- **Development Costs:** Building a full-stack platform that integrates Bitcoin and EVM technologies requires significant investment in development, testing, and deployment.
- **Infrastructure Expenses:** Running Bitcoin and Ethereum nodes, as well as the infrastructure for the Citrea rollup, involves ongoing costs for server hosting, bandwidth, and maintenance.
- **Transaction Costs:** High Bitcoin and Ethereum transaction fees during periods of network congestion could deter users or inflate operational costs. Users may avoid using the platform if fees for bidding, transferring, or settlement become excessive.
- **Liquidity Challenges:** Attracting enough buyers and sellers to ensure a liquid marketplace can require incentives such as marketing campaigns, fee discounts, or rewards, which come at a cost.
- **Revenue Model Constraints:** Establishing a sustainable revenue model (e.g., platform fees, listing fees) must strike a balance between profitability and affordability for users.
- **Volatility in Cryptocurrency Prices:** Rapid fluctuations in Bitcoin and Ethereum prices could affect user behavior and platform costs. Holding cryptocurrencies in the platform’s treasury poses financial risk.
- **Economic Accessibility:** Many potential users might find Bitcoin Ordinals trading inaccessible due to high entry costs for Bitcoin or the technical knowledge required to participate.
- **Funding and Investment:** Limited access to funding for the project could constrain the scope of development, marketing, and expansion. Attracting investors might require demonstrating a clear path to profitability, which can be challenging in the early stages.

4.1.1.3 Ethical Constraints

- **Inclusivity and Accessibility:** The platform must ensure equal access to auctions, avoiding favoritism or unfair advantages for certain users or entities. Complex interfaces or high fees could exclude less technically proficient or economically disadvantaged users.
- **Environmental Concerns:** Bitcoin and Ethereum's proof-of-work energy consumption may raise ethical concerns about the environmental impact of trading Ordinals. Although Ethereum has transitioned to proof-of-stake, the Bitcoin aspect still carries this concern.
- **Fraud Prevention:** The platform must ensure robust measures against scams, fraudulent listings, and manipulative practices like wash trading or bid rigging.
- **Privacy and Data Security:** Ethical handling of user data is critical to maintaining trust. Any compromise in privacy or data leaks could harm users and the platform's reputation.
- **Market Manipulation:** Mechanisms must be in place to prevent wealthier participants from manipulating the auction process or dominating the market, creating unfair conditions for smaller participants.
- **Regulatory Compliance:** Operating in jurisdictions with unclear or evolving cryptocurrency regulations presents ethical challenges, as failure to comply could harm users. Transparent operations must ensure compliance with anti-money laundering (AML) and know-your-customer (KYC) requirements without compromising user privacy excessively.
- **Economic Inequality:** By tying assets to Bitcoin Ordinals, the platform risks further concentrating digital wealth among already affluent cryptocurrency holders. Ethical considerations should include mechanisms to broaden access and participation.
- **Cross-Chain Risks:** The trust-minimized bridge must ensure integrity; any failure could result in lost user funds, undermining trust and violating ethical responsibility.
- **Transparency in Auctions:** Ethical challenges arise if the auction process is not transparent, leading to user mistrust or allegations of unfair practices.
- **Encouragement of Speculation:** By focusing on auctions for Bitcoin Ordinals, the platform may inadvertently promote speculative behavior, leading to financial harm for less-informed participants.

4.1.2 Standards

Bitcoin Improvement Proposals (BIPs) are formal documents that define standards and enhancements to the Bitcoin protocol, ensuring consistent functionality across the network. Several BIPs are directly relevant to the auction system for Ordinals NFTs. Partially Signed Bitcoin Transactions (PSBT), defined in BIP 174, provide a standard for creating, signing, and finalizing transactions collaboratively, ensuring flexibility and security in the auction's settlement phase. Multi-signature contracts, outlined in BIP 11, are used to lock the Ordinal NFT securely on the Bitcoin blockchain, requiring signatures from multiple parties to authorize its transfer. The UTXO (Unspent Transaction Output) model, which is a core feature of Bitcoin, ensures

traceable and verifiable transactions by linking each bid to the bidder's available funds. Additionally, proof-of-funds mechanisms, while not formally defined in a specific BIP, are an industry practice that helps confirm a bidder's financial capacity to complete the purchase. These standards collectively ensure the system is secure, efficient, and aligned with best practices in blockchain technology.

4.2 Risks and Alternatives

- **Technical Challenges with Citrea Integration:** Citrea is a new rollup platform and its integration may pose unforeseen technical challenges, such as compatibility issues or documentation gaps.

  Alternative: Seek direct assistance from the Citrea team as they are willing to help the team. Simplify features if necessary, or temporarily use a simulated environment to continue development while resolving integration issues.

- **Smart Contract Errors:** Smart contracts may contain bugs or vulnerabilities that could lead to transaction errors or security issues.

  Alternative: Considering past incidents in the blockchain sector, smart contracts can be developed using established industry standards to minimize vulnerabilities.

- **Delayed Development Timeline:** A two-person team may face time constraints, leading to delays in project milestones.

  Alternative: Prioritize core features for an MVP (Minimum Viable Product) and use agile methods to deliver smaller, functional components on time.

- **Lack of User Adoption:** The platform might struggle to attract Bitcoin Ordinals traders and hobbyists due to strong competition from Magic Eden and a possible drop in interest in Ordinals. Success depends on keeping the hype alive and encouraging more users to adopt Ordinals.

  Alternative: Conduct market research to understand user needs, emphasize faster and cheaper transactions compared to competitors like Magic Eden, collaborate with Ordinals communities, and seek support from the Citrea team to grow and overcome competition

4.3 Project Plan

Table 1: Factors that can affect analysis and design.

Factors	Effect level	Effect
Public health	low	Minimal impact unless tied to physical events or facilities, as NFTs are digital assets.
Public safety	low	Rarely relevant unless our platform involves physical NFT-related goods or in-person auctions.
Public welfare	moderate	May face criticism if NFTs are associated with speculative bubbles or scams that harm users financially.

Global factors	high	Geopolitical events, international regulations, and currency exchange rates can significantly impact market activity.
Cultural factors	moderate	Cultural acceptance or rejection of NFTs can influence platform adoption across different regions.
Social factors	moderate	Public perception of NFTs as either innovative or exploitative may affect user trust and engagement.
Environmental factors	high	Environmental concerns about blockchain energy consumption could deter eco-conscious users.
Economic factors	high	Economic downturns or instability can reduce discretionary spending on digital collectibles like NFTs.

Table 2: Risks

Risks	Likelihood	Effect on the project	B Plan Summary
Public Welfare	Moderate	Users may face financial harm from scams or speculative losses.	Implementing strict fraud detection and clear user guidelines.
Global Regulations	High	Compliance issues may hinder global operations.	To engage legal advisors for each target region.
Economic Downturn	High	Reduced activity as users prioritize essential spending.	Offering flexible pricing and alternative auction models
Security Breaches	Moderate	Loss of trust and assets due to cyberattacks.	Regularly updating security protocols and conducting audits.
Platform Downtime	Low	Revenue loss and user dissatisfaction.	To invest in reliable hosting and failover systems.
Volatility in Crypto	High	Sudden value changes may disrupt auctions.	Integrating stablecoin options for transactions.

Table 3: List of work packages

WP#	Work package title	Leader	Members involved
WP1	Creating and developing the codebase of the project	Ali Kaan Şahin	Ali Kaan Şahin Mehmet Berşan Özgür
WP2	Writing reports of the project	Mehmet Berşan Özgür	Ali Kaan Şahin Mehmet Berşan Özgür
WP 1: Creating and developing the codebase of the project			
Start date: 01.11.2024 **End date:** Ongoing			
Leader:	Ali Kaan Şahin	**Members involved:**	Mehmet Berşan Özgür

Objectives: The objective of this work package is to design, develop, and establish a scalable and efficient codebase for the project. This includes creating a robust architecture, implementing core functionalities, and ensuring the maintainability of the code. The goal is to deliver a system that meets the project requirements while enabling smooth future development and feature enhancements.			
Tasks: **Task 1.1 Designing the System Architecture :** Develop a modular and scalable architecture that outlines the core components and their interactions. Ensure the design aligns with the project's objectives and technological stack **Task 1.2 Implementing Core Functionalities :** Write and test the core modules and features of the project. Emphasize clean coding practices, performance optimization, and adherence to coding standards.			
Deliverables **D1.1:** System architecture documentation **D1.2:** Initial codebase with core features implemented			
WP 2: Writing reports of the project			
Start date: 25.10.2024 **End date:** Ongoing			
Leader:	Mehmet Berşan Özgür	**Members involved:**	Ali Kaan Şahin
Objectives: The objective of this work package is to document the project's progress, methodologies, and outcomes comprehensively. These reports aim to ensure transparency, facilitate knowledge sharing among stakeholders, and serve as a reference for future development. Additionally, the reports will help assess whether the project is meeting its predefined objectives and timelines.			
Tasks: **Task 2.1 Project Information form :** Collect and compile key details about the project, including objectives, scope, stakeholders, and deliverables, into a standardized information form for consistent communication and record-keeping. **Task 2.2 Project Specification document :** Create a detailed specification document outlining the project's functional and technical requirements. Ensure clarity and precision to serve as a guideline for the development team. **Task 2.3 Analysis and Requirements Report :** Conduct a comprehensive analysis to gather and document the project's requirements. Highlight critical needs, constraints, and expected outcomes to ensure alignment with stakeholder expectations.			
Deliverables **D2.1 Project Information form** **D2.2 Project Specification document** **D2.3 Analysis and Requirements Report**			

4.4 Ensuring Proper Teamwork

The team consists of two members, which increases responsibilities and promotes closer collaboration. To maximize knowledge in both web development and blockchain technologies, tasks are divided based on strengths and expertise. One member focuses on frontend and backend development, ensuring a user-friendly interface and efficient system design, while the other handles blockchain integration, including smart contract development and interaction with Citrea. Tools such as GitHub are used for version control and task management, enabling organized progress and equal contributions. Regular meetings and open communication help maintain alignment and address issues promptly, ensuring effective teamwork.

4.5 Ethics and Professional Responsibilities

The project prioritizes transparency, user security, and data integrity, ensuring trust and accountability in financial transactions. Industry standards for blockchain and software development are followed, including proper documentation, reliable smart contracts, and thorough testing using testnet of Citrea. Citrea's guidance helps maintain professional quality, with a focus on inclusivity and accessibility for all users. These principles ensure an ethical and secure solution for the Bitcoin Ordinals community.

4.6 Planning for New Knowledge and Learning Strategies

The project requires a deep understanding of Citrea, a relatively new and innovative rollup platform. Learning its architecture, integration methods, and features will be a key focus. Throughout the process, the team will remain flexible and ready to adapt to challenges, instantly learning and applying new strategies as needed.

As blockchain technology is highly innovative and constantly evolving, new trends and tools are expected to emerge during the project. The team anticipates encountering these developments and will actively seek to incorporate them into the project to ensure it stays relevant and competitive. Strategies such as hands-on experimentation, consulting the Citrea team, and leveraging online resources will be employed to acquire and apply the necessary knowledge effectively.

5 Glossary

Bitcoin: A digital currency and payment system that operates without a central authority. Bitcoin transactions are recorded on a blockchain, a public ledger

Ordinals: Digital assets like NFTs that are inscribed directly onto satoshis (the smallest unit of Bitcoin) and stored on the Bitcoin blockchain.

Citrea: A Bitcoin rollup platform that enables EVM technologies on Bitcoin, like Ethereum, using a trust-minimized bridge for cross-chain functionality.

Rollup: A blockchain scalability solution that processes many transactions off the main blockchain and later submits them as a single batch to reduce costs and congestion.

NFT (Non-Fungible Token): A unique digital asset that represents ownership of items like art, music, or collectibles, often stored on a blockchain.

Satoshi: The smallest unit of Bitcoin, equal to 0.00000001 BTC, named after Bitcoin's creator, Satoshi Nakamoto.

Bitcoin's Script Limitations: Bitcoin uses a simple programming language called Bitcoin Script, which lacks complex features such as loops and advanced computational capabilities, making it difficult to create advanced applications like auctions.

EVM (Ethereum Virtual Machine): A technology that runs smart contracts on Ethereum. It allows developers to build decentralized applications (dApps).

Non-Turing Complete: A system or programming language that cannot perform all possible computations, as is the case with Bitcoin's Script. This keeps Bitcoin secure but limits flexibility.

Transaction Overhead: Extra costs and time required for processing transactions, often due to fees or technical inefficiencies.

Cross-Chain Transactions: The transfer of assets or data between two different blockchains, such as Bitcoin and Ethereum.

On-Chain Transactions: Transactions that are recorded directly on the blockchain. These are transparent and immutable but may incur higher fees.

Off-Chain Transactions: Transactions that occur outside the blockchain, reducing costs and speeding up processing but relying on external systems for trust.

Wallet: A digital tool for storing and managing cryptocurrency. Wallets can be software-based (apps) or hardware-based (physical devices).

Bitcoin UTXO (Unspent Transaction Output): A method used by Bitcoin to track and spend funds. It ensures that all inputs (money spent) match outputs (money received) without errors.

Multi-Signature Schemes: A security feature requiring multiple signatures from different parties to approve a transaction, making it harder for hackers to steal funds.

Smart Contract Audits: A review process to ensure that blockchain programs (smart contracts) are secure and free from vulnerabilities.

Unisat: A wallet or platform for managing and trading Bitcoin Ordinals and other blockchain assets.

Hardware Wallets: Physical devices that store cryptocurrency offline, protecting them from hacks and cyber-attacks.

Sniping: A practice in auctions where a participant places a bid at the last second to win without giving others time to respond.

Front-Running: Exploiting knowledge of a pending transaction to act before it and gain an unfair advantage, often seen in blockchain trading.

Liquid Marketplace: A market where assets can be easily bought or sold without affecting their price significantly.

Bitcoin Maximalists: People who believe Bitcoin is the best and only true cryptocurrency, often critical of other projects like Ethereum or NFTs.

Solidity: A programming language used to create smart contracts on Ethereum and other compatible blockchains.

Proof-of-Work (PoW): A consensus mechanism where miners solve complex problems to validate transactions and secure the blockchain. PoW is energy-intensive.

Proof-of-Stake (PoS): A consensus mechanism where validators are chosen based on how much cryptocurrency they own and "stake," using far less energy than PoW.

Wash Trading: A fraudulent practice where someone trades with themselves to create fake market activity, misleading others about an asset's value or demand.

Bid Rigging: An illegal practice where participants in an auction collude to manipulate the outcome, often to lower the final bid price.

Jurisdictions: Regions or countries with specific legal rules and regulations. Compliance with these is essential for operating legally.

Anti-Money Laundering (AML): Regulations aimed at preventing the use of cryptocurrency and other systems for illegal activities, like money laundering.

Know-Your-Customer (KYC): Rules requiring platforms to verify the identity of their users to ensure they are not engaging in illegal activities.

PSBT (Partially Signed Bitcoin Transaction): A Bitcoin transaction that is not yet finalized, allowing multiple parties to collaborate in signing it securely.

ZK (Zero-Knowledge) Proof: A cryptographic method that allows one party to prove they know certain information without revealing it, enhancing privacy.

Dutch Auction: An auction where the price starts high and decreases over time until a buyer accepts it. The first bid wins, making it quick and efficient for selling items.

Multi-Signature Contract: A type of Bitcoin transaction that requires signatures from multiple parties to authorize the transfer of assets, ensuring secure and controlled access to funds or NFTs during the auction process.

Signing a Bid: The process of cryptographically signing a bid using the bidder's private key to prove its authenticity and intent without requiring immediate fund transfer.

UTXO (Unspent Transaction Output): A Bitcoin transaction output that can be used as input in a new transaction, providing a traceable and secure way to manage and verify funds.

Proof of Funds: A method to verify that a bidder has sufficient Bitcoin in their wallet to honor their bid, ensuring reliability without locking funds upfront.

BIP (Bitcoin Improvement Proposal): A formal document that outlines proposed changes, features, or standards for the Bitcoin protocol, ensuring consistency and interoperability across the network. Examples include BIP 174 for Partially Signed Bitcoin Transactions and BIP 11 for multi-signature contracts.

6 References

- Object-Oriented Software Engineering, Using UML, Patterns, and Java, 2nd Edition, by Bernd Bruegge and Allen H. Dutoit, Prentice-Hall, 2004, ISBN: 0-13-047110-0.
- Citrea. (n.d.). Getting started. Retrieved November 19, 2024, from https://docs.citrea.xyz/
- Arkham Research Team. (2024, April 30). Bitcoin Ordinals for Beginners. Arkham Intelligence. Retrieved November 19, 2024, from https://www.arkhamintelligence.com/research/bitcoin-ordinals-for-beginners
- 4. Pontem Network. (n.d.). Bitcoin Ordinals 101. Retrieved November 19, 2024, from https://blog.pontem.network/bitcoin-ordinals-101-45a39d8c6002
- Gamma.io. (n.d.). What is a PSBT? Retrieved November 19, 2024, from https://gamma.io/learn/blockchain/bitcoin/what-is-a-psbt
- Alchemy. (n.d.). Multi-sig contracts. Retrieved November 19, 2024, from https://docs.alchemy.com/docs/multi-sig-contracts
- Blockchain.com. (n.d.). Blockchain API v3: Get accounts. Retrieved November 19, 2024, from https://api.blockchain.com/v3/#getaccounts