BILKENT UNIVERSITY
ENGINEERING FACULTY
DEPARTMENT OF COMPUTER ENGINEERING

T-2428 Project Satonic
Project Specification Document

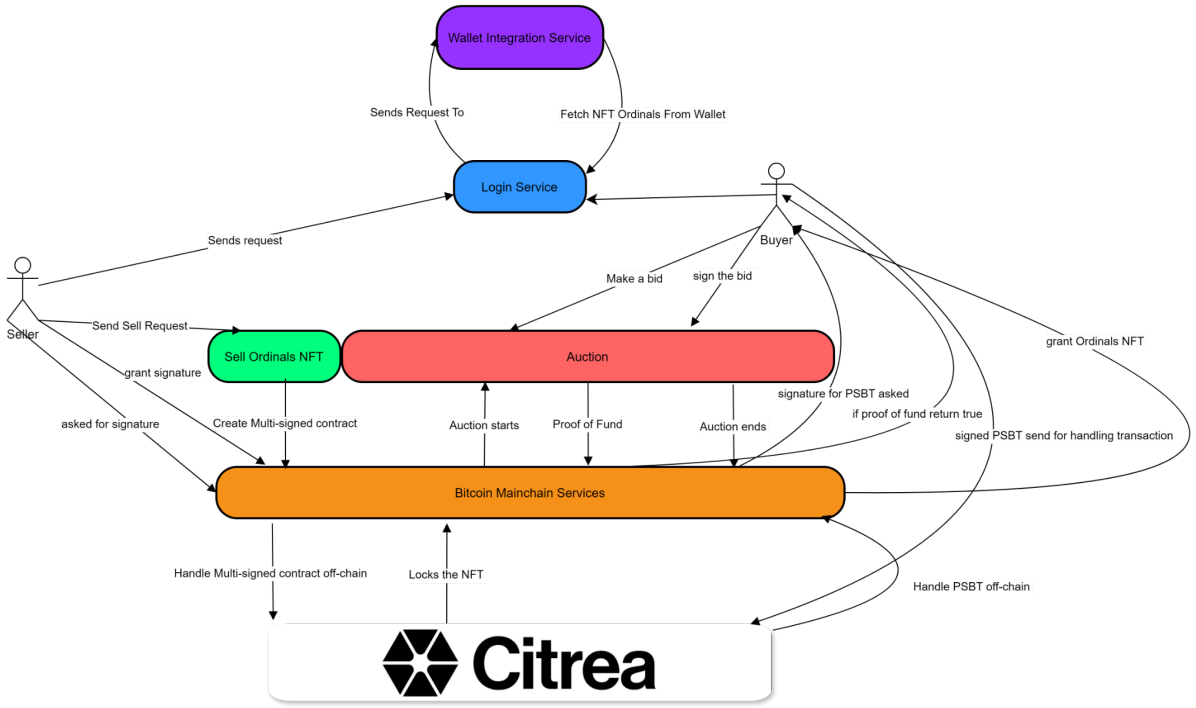
Mehmet Berşan Özgür - 21902246
Ali Kaan Şahin - 22002932

1. Introduction

1.1 Description

The Ordinals Auction System 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.

1.2 High Level System Architecture & Components of Proposed Solution



1.3 Constraints

1.3.1. Implementation Constraints

1. 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.

Offloading auction logic to the EVM ecosystem must be done carefully to ensure security and minimize transaction overhead.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. Full-Stack Development Requirements

The project involves building:
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.

9. 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.

10. 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.

11. 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.

12. 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.

1.3.2. Economic Constraints

1. Development Costs

Building a full-stack platform that integrates Bitcoin and EVM technologies requires significant investment in development, testing, and deployment.
Hiring specialized talent for Bitcoin Script, Solidity, and cross-chain development can be expensive.

2. 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.

3. 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.

4. 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.

5. Revenue Model Constraints

Establishing a sustainable revenue model (e.g., platform fees, listing fees) must strike a balance between profitability and affordability for users.

6. 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.

7. 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.

8. 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.

1.3.3. Ethical Constraints

1. 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.

2. 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.

3. Fraud Prevention

The platform must ensure robust measures against scams, fraudulent listings, and manipulative practices like wash trading or bid rigging.

4. 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.

5. 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.

6. 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.

7. 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.

8. Cross-Chain Risks

The trust-minimized bridge must ensure integrity; any failure could result in lost user funds, undermining trust and violating ethical responsibility.

9. Transparency in Auctions

Ethical challenges arise if the auction process is not transparent, leading to user mistrust or allegations of unfair practices.

10. 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.

1.4 Professional and Ethical Issues

1. Platform Reliability and Uptime

Ensuring the platform is consistently operational is a professional obligation. Downtime or system failures can damage the platform’s reputation and erode user trust.

2. Code Quality and Security

Poorly written or inadequately tested code can lead to vulnerabilities, exploits, or operational failures, impacting users and the project's credibility.
Regular audits of smart contracts and cross-chain protocols are essential to maintain professional standards.

3. Cross-Chain Integration Challenges

Interoperability between Bitcoin and the EVM ecosystem involves complex technologies that require high levels of expertise. A lack of skilled personnel could lead to integration issues.

4. Knowledge and Competence

Developers must possess a deep understanding of Bitcoin Ordinals, Ethereum smart contracts, and rollup technology to deliver a robust product.
Misrepresentation of technical capabilities to stakeholders can harm project outcomes and credibility.

5. User Support and Documentation

Providing comprehensive documentation, tutorials, and responsive support channels is a professional responsibility to ensure users can navigate the platform effectively.

6. Regulatory Expertise

Professionals involved must stay informed about cryptocurrency regulations and ensure the platform complies with applicable laws.
Failure to do so could lead to fines, shutdowns, or loss of user trust.

7. Intellectual Property and Licensing

Respecting intellectual property rights for any third-party tools, APIs, or frameworks used is essential.
Licensing terms for the platform must be clear and enforceable.

8. User Protection

The platform must prioritize the safety of user funds and personal data, implementing measures against fraud, scams, and unauthorized access.

9. Fair Access

Ethical challenges arise if wealthier participants gain unfair advantages, such as bypassing auction limits or manipulating bids. Mechanisms should be in place to ensure fairness for all users.

10. Transparency and Trust

Ensuring that auction processes, fees, and platform policies are transparent is critical to maintaining ethical standards.
Any hidden fees, unclear terms, or ambiguous practices could erode user trust.

11. Environmental Responsibility

Bitcoin's energy-intensive mining has environmental implications, and integrating with Bitcoin requires careful consideration of these impacts.
Ethically, the platform could explore ways to offset its carbon footprint.

12. Market Speculation Risks

By enabling auctions for Bitcoin Ordinals, the platform might encourage speculative behavior, leading to potential financial losses for uninformed or inexperienced users.

13. Privacy Concerns

Users' identities and transactions must be handled with utmost care to avoid misuse or exposure of personal information.

14. Potential for Exploitation

Auction dynamics might enable practices like wash trading or price manipulation, which could mislead participants and inflate prices unethically.

15. Censorship Resistance vs. Compliance

Striking a balance between regulatory compliance (e.g., KYC, AML) and maintaining the decentralized ethos of cryptocurrency is an ethical challenge.

Excessive compliance measures could alienate users who value privacy, while insufficient measures could attract illicit activities.

16. Social Responsibility

The platform must consider its broader societal impact, such as promoting inclusivity, reducing barriers to entry, and educating users about risks involved in trading digital assets.

17. Responsibility for Losses

If users lose funds due to platform bugs, hacks, or cross-chain failures, there is an ethical obligation to provide remedies or compensations where feasible.

1.5 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.

2. Design Requirements

2.1. 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.

2.2. Non-Functional Requirements

2.2.1. 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.

2.2.2. 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.

2.2.3. 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.

2.2.4. 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.

2.2.5. 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.

2.2.6 Security

The system will leverage Zero-Knowledge (ZK) technology, ensuring high-level security without exposing sensitive details. This approach minimizes risks of data breaches.

2.2.7 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. Feasibility Discussions

3.1. Market & Competitive Analysis

3.1.1 Market Analysis

1. **Magic Eden:**
    - **Main Features:** Magic Eden started as a marketplace for Solana NFTs and now supports Bitcoin Ordinals. It's easy to use and has tools for buying, selling, and browsing Ordinals.
    - **How it serves the Ordinals Market:** Magic Eden uses its well-known brand to create a familiar place for trading Bitcoin Ordinals, ideal for users who want a simple and reliable platform.
    - **Website Link:** https://magiceden.io/
2. **Gamma**
    - **Main Features:** Gamma is a marketplace focused on Bitcoin Ordinals. It offers tools for creators to mint and list their digital items, making it easy for users to manage their Ordinals.
    - **How it serves the Ordinals Market:** Gamma makes Ordinals more accessible by providing tools for creators to make new items and for collectors to easily find and buy them.
    - **Website Link:** https://gamma.io/
3. **Ordswap**
    - **Main Features:** Ordswap is the first trustless marketplace for Ordinals, focusing on secure and direct trading without middlemen.
    - **How it serves the Ordinals Market:** Ordswap appeals to users who value security and control, allowing them to trade Ordinals directly on Bitcoin without centralized systems.
    - **Website Link:** https://ordinals-ecosystem.com/ecosystem/ordswap/
4. **UniSat**
    - **Main Features:** UniSat is a decentralized app for creating, trading, and managing Bitcoin Ordinals. It supports over 1,500 Ordinals collections.
    - **How it serves the Ordinals Market:** UniSat gives users access to a wide variety of Ordinals in a decentralized way, good for both creators and collectors who want full control over their assets.
    - **Website Link:** https://unisat.io/
5. **Ordinals Wallet**
    - **Main Features:** Ordinals Wallet is mainly a wallet for securely storing and managing Ordinals, letting users view and manage their Bitcoin-based NFTs.
    - **How it serves the Ordinals Market:** While it's not a full marketplace, Ordinals Wallet offers a safe place for users to manage their Ordinals, especially useful for those new to Ordinals or who only need storage.
    - **Website Link:** https://ordinalswallet.com/

3.1.2 Difference of Satonic:

- **Auction Based Model:** Unlike other marketplaces, this platform uses an auction system where the highest bid wins unlike Dutch Auction. This creates flexible pricing and makes the trading experience more exciting for users.

- **Fast Transactions with low fees:** By using Citrea, transactions here are faster and cheaper than those on traditional Ordinals platforms, which rely on Bitcoin's slower mainnet. Citrea also uses zero-knowledge proofs, which reduce the amount of data sent on the blockchain, saving space and cutting fees while keeping interactions quick and safe.

- **Enhanced Security with Zero-Knowledge Proof:** Citrea employs zero-knowledge (ZK) proofs, ensuring secure transactions with minimal on-chain data exposure, which both lowers fees and maintains user privacy.

3.1.3 Comparison Table:

Name	Auction Model	Transaction Speed	Fees	Security
Satonic	Yes	Fast	Low	High
Magic Eden	No	Slow	High	Moderate
Ordswap	No	Slow	High	High
Unisat	No	Slow	High	Moderate
Ordinals Wallet	No	Slow	High	High

3.2. Academic Analysis

The auction system for Ordinals NFTs uses Bitcoin's UTXO model and Citrea's technology to ensure security, efficiency, and scalability. At the beginning of the auction, the Ordinal NFT is locked in a multi-signature contract on the Bitcoin blockchain, preventing it from being moved or changed until the auction ends. During the bidding process, participants submit bids that are signed using their private keys, providing proof of their intent to pay. Proof of sufficient Bitcoin funds are verified and handled through proof of funds using Blockchain's REST API. These bids are handled off-chain through Citrea, reducing transaction costs and improving speed. After the auction ends, the highest bidder signs a Partially Signed Bitcoin Transaction (PSBT) to transfer the payment to the seller. Once the transaction is complete, the Ordinal NFT is released from the multi-signature contract and

transferred to the buyer. The UTXO model ensures that each bid is linked to funds in the bidder's wallet, and the final transaction consumes those funds to complete the payment. This design maintains security, efficiency, and transparency while minimizing costs.

Research has been done on Partially Signed Bitcoin Transactions (PSBT), UTXOs, multi-signature contracts, and proof-of-funds to design a secure and simple system. PSBT allows transactions to be signed by more than one person before they are sent, and multi-signature contracts help lock assets safely. Proof-of-funds and UTXOs have been studied to ensure bids are reliable and transactions are traceable.

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

1. Citrea. (n.d.). *Getting started*. Retrieved November 19, 2024, from https://docs.citrea.xyz/

2. Bitcoin Improvement Proposals (BIPs). (n.d.). *GitHub repository.* Retrieved November 19, 2024, from https://github.com/bitcoin/bips

3. 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

5. Gamma.io. (n.d.). *What is a PSBT?* Retrieved November 19, 2024, from https://gamma.io/learn/blockchain/bitcoin/what-is-a-psbt

6. Alchemy. (n.d.). *Multi-sig contracts*. Retrieved November 19, 2024, from https://docs.alchemy.com/docs/multi-sig-contracts

7. Blockchain.com. (n.d.). *Blockchain API v3: Get accounts*. Retrieved November 19, 2024, from https://api.blockchain.com/v3/#getaccounts