DarkSwap Whitepaper

DarkSwap Team

April 30, 2025

1 Introduction

The burgeoning digital asset landscape necessitates trading platforms that uphold the core tenets of decentralization: security, privacy, and censorship resistance. Conventional centralized exchanges, despite their current dominance in liquidity and accessibility, are fundamentally antithetical to these principles. Their centralized control points represent attractive targets for malicious actors and regulatory pressures, introducing significant counterparty risk and eroding user autonomy. The inherent opacity of such platforms further contradicts the transparency that blockchain technology promises.

While various decentralized trading approaches have been explored, they often grapple with complexities that hinder widespread adoption, including challenges in achieving sufficient liquidity and providing a seamless user experience. This whitepaper introduces DarkSwap, a groundbreaking decentralized peer-to-peer trading platform meticulously engineered for the trustless exchange of Bitcoin, Runes, and Alkanes directly between participants. DarkSwap distinguishes itself by employing a sophisticated modular architecture and advanced P2P networking protocols to effectively eliminate counterparty risk, bolster censorship resistance, and return complete control of assets to the users throughout the trading process. This document provides a comprehensive exposition of DarkSwap's technical architecture, communication protocols, salient features, robust security framework, performance considerations, and strategic future development roadmap, positioning DarkSwap as a leading-edge, secure, and highly efficient decentralized trading solution within the Bitcoin ecosystem.

2 Architecture

The architectural design of DarkSwap is predicated on principles of decentralization, modularity, and robustness, specifically tailored to enable trustless peer-to-peer trading of Bitcoin, Runes, and Alkanes. The system is logically partitioned into several interconnected components, each assigned distinct responsibilities within the overall trading ecosystem and network topology.

At the core of the platform resides the DarkSwap SDK (`darkswap-sdk`), implemented as a Rust library. The selection of Rust is motivated by its strong emphasis on memory safety, performance, and concurrency, which are critical for building reliable and efficient decentralized applications. The SDK encapsulates the fundamental logic underpinning the DarkSwap protocol, including sophisticated modules for distributed orderbook management, secure trade execution, and seamless integration with various wallet implementations.

Building upon the solid foundation of the SDK are the user-facing interfaces and background services. The DarkSwap CLI (`darkswap-cli`) provides a powerful and flexible command-line interface, allowing technical users to interact directly with the DarkSwap network and execute trading operations. For continuous participation in the decentralized network and automated trading strategies, the DarkSwap Daemon (`darkswap-daemon`) operates as a persistent background service. The web interface (`web`), constructed using modern web technologies like TypeScript and React, offers an intuitive graphical user interface, communicating with the core SDK functionalities through WebAssembly bindings. This approach leverages the performance benefits of the Rust-based SDK while providing broad accessibility through standard web browsers. Supporting libraries such as `darkswap-lib`, `darkswap-support`, `darkswap-web-sys`, and `darkswap-wasm` provide common utilities, shared functionalities, and facilitate the WebAssembly integration.

The decentralized network communication layer is powered by the versatile `libp2p` framework. `libp2p` was chosen for its modularity, extensibility, and native support for various transport protocols, making it ideal for constructing a resilient and adaptable P2P network. WebRTC is specifically employed to enable direct peer-to-peer connections for browser-based clients, optimizing data transfer efficiency. To overcome the challenges posed by Network Address Translation (NAT) and ensure connectivity for peers behind firewalls, DarkSwap incorporates a Circuit Relay mechanism, facilitated by a dedicated DarkSwap Relay Server (`darkswap-relay`). This server assists peers in discovering each other and establishing relayed connections when direct connections are not possible.

The distributed orderbook is a key architectural element, managing buy and sell orders across the decentralized network. Orders are propagated among peers, each maintaining and updating their local copy of the orderbook. This distributed approach enhances transparency and resilience compared to centralized orderbook systems. The secure trading protocol, built upon Partially Signed Bitcoin Transactions (PSBTs), is integral to the architecture, ensuring atomic and trustless execution of asset swaps directly between trading peers. Finally, robust wallet integration, including support for the Bitcoin Development Kit (BDK), is a critical component, enabling users to securely manage their Bitcoin, Rune, and Alkane balances and authorize transactions necessary for trading directly within the DarkSwap environment.

2.1 P2P Protocol

The peer-to-peer (P2P) communication layer is a cornerstone of the DarkSwap architecture, enabling decentralized interaction among participants without re-

Figure 1: Overall Architecture of the DarkSwap Platform. This diagram should illustrate the main components (SDK, CLI, Daemon, Web, Relay Server) and their interactions, including the P2P Network, User Wallets, and the Bitcoin Blockchain.

liance on a central authority. This layer is built upon the `libp2p` framework, a sophisticated and modular networking stack chosen for its adaptability, extensibility, and native support for diverse transport protocols. The selection of `libp2p` provides DarkSwap with the flexibility to operate across various environments, from command-line interfaces and background daemons to web browsers.

Peer discovery within the DarkSwap network is a critical function facilitated by `libp2p`'s integrated mechanisms. These include Multicast DNS (mDNS) for efficient and automatic discovery of peers within local network segments, and the Kademlia Distributed Hash Table (DHT) for scalable peer discovery across a wider, geographically dispersed network by decentralizing the storage and retrieval of peer addressing information. The network also utilizes a set of predefined bootstrap nodes, which serve as initial connection points for new peers to join the network and subsequently discover other participants through the DHT.

Once peers have discovered each other, `libp2p` supports the establishment of direct connections using a variety of transport protocols. DarkSwap leverages TCP for reliable, stream-oriented communication between traditional nodes and WebSockets to enable seamless connectivity for browser-based clients. Crucially, WebRTC is employed to facilitate direct peer-to-peer connections between web browsers, significantly reducing latency and optimizing data transfer efficiency by bypassing intermediate servers after the initial connection setup. Acknowledging the prevalent challenges posed by Network Address Translation (NAT) and firewalls, DarkSwap incorporates a Circuit Relay mechanism. This allows peers situated behind restrictive network configurations to establish connections by relaying their traffic through a publicly accessible DarkSwap Relay Server, thereby enhancing network reachability and resilience.

Message exchange between connected peers occurs over secure channels established by `libp2p`, utilizing application-level protocols tailored to DarkSwap's needs. The GossipSub protocol, a robust and scalable publish/subscribe mechanism, is effectively utilized for the efficient dissemination of information such as new trading orders and updates across the network. This ensures that all interested peers receive relevant orderbook information in a timely manner. Additionally, a request-response pattern is implemented for direct, point-to-point communication between two peers, facilitating specific interactions such as requesting detailed information about a particular order or engaging in the step-by-step negotiation process of a trade. Maintaining a consistent view of the distributed orderbook across all peers in the face of network latency and churn is a key challenge addressed through careful design and ongoing optimization of the message propagation and validation mechanisms.

Figure 2: DarkSwap P2P Network Connectivity. This diagram should illustrate how different types of peers (e.g., CLI, Daemon, Browser) connect to each other, showing the role of libp2p, WebRTC, and the relay server in facilitating connections, including NAT traversal.

2.2 Trading Protocol

The DarkSwap trading protocol orchestrates the process of exchanging assets between peers in a trustless and atomic fashion. Engineered for security and reliability, this protocol guarantees that asset swaps are executed such that either both sides of the trade are successfully completed on the Bitcoin blockchain, or neither is, thereby effectively eliminating counterparty risk.

The lifecycle of a trade within DarkSwap commences with the creation and propagation of trading orders. Users specify the parameters of their desired exchange, including the asset to be sold, the asset to be acquired, and the terms of the trade (e.g., price and quantity). These orders are cryptographically signed by the user's wallet to ensure authenticity and integrity, and are then disseminated across the decentralized P2P network. The efficient propagation of these orders is facilitated by the GossipSub protocol, enabling peers to receive and validate new orders and update their local copies of the distributed orderbook.

Order matching is a continuous and decentralized process. Peers actively monitor their local orderbooks for compatible buy and sell orders. A match is identified when the terms of a buy order for a specific asset pair align with or exceed the terms of a sell order for the same pair. Matching can occur directly between any two peers on the network that discover a compatible order.

Upon identifying a match, the involved peers engage in a structured trade negotiation phase. This phase involves the secure exchange of information necessary to construct a Partially Signed Bitcoin Transaction (PSBT). The PSBT format is a standardized and widely adopted method that allows multiple participants to collaborate in building and signing a complex Bitcoin transaction without exposing their private keys to one another. The atomic execution of the trade is enforced through the PSBT mechanism, requiring both the maker and the taker to apply their digital signatures to the transaction. The trade is only considered valid and broadcastable to the Bitcoin network if all required signatures are present. This design inherently handles potential edge cases such as one party going offline or refusing to sign; in such scenarios, the PSBT remains incomplete, the transaction is not broadcast, and the assets remain unspent in the participants' wallets. The typical flow of trade negotiation and execution involves the maker sending an initial trade proposal (encapsulating their desired terms and initial PSBT data) to the taker. The taker validates this proposal and, if acceptable, contributes their necessary inputs and outputs to the PSBT and applies their signature. The partially signed PSBT is then returned to the maker, who performs a final validation, adds their own inputs and outputs, and applies their signature. The now fully signed PSBT represents the atomic swap transaction and is broadcast to the Bitcoin network for confirmation. The successful inclusion of this transaction in a Bitcoin block signifies the completion of the trustless atomic swap. This reliance on native Bitcoin scripting capabilities and the PSBT standard, rather than complex smart contracts, enhances the security and simplicity of the trading protocol.

Figure 3: DarkSwap Trading Protocol Flow. This diagram should illustrate the sequence of events in a trustless atomic swap, from order creation and propagation to matching, negotiation, PSBT exchange, and broadcasting the final transaction.

2.3 Signaling Protocol

The signaling protocol is an indispensable component of the DarkSwap network, specifically facilitating the establishment of WebRTC connections between peers, a requirement particularly pronounced for clients operating within web browser environments. As WebRTC is fundamentally a peer-to-peer communication technology, it mandates an initial signaling phase to enable the exchange of crucial network configuration and session capabilities information between the peers intending to establish a direct connection.

This signaling process involves a dedicated signaling server, which can be deployed as a standalone service or integrated into the DarkSwap Relay Server infrastructure, and the individual peers seeking to form a WebRTC connection. The typical sequence of events in the signaling exchange is as follows: An initiating peer, acting as the offerer, generates a WebRTC offer. This offer is formatted as a Session Description Protocol (SDP) message, containing essential details about the offerer's media capabilities, supported codecs, and potential network addresses. The offerer securely transmits this SDP offer to the signaling server, specifying the unique identifier of the intended recipient peer. The signaling server acts as a secure intermediary, responsible for reliably forwarding the received SDP offer to the designated answerer peer. Upon receiving the offer, the answerer processes the information and generates a compatible WebRTC answer, also encapsulated within an SDP message. This answer is then transmitted back to the signaling server, again specifying the target peer. The signaling server subsequently delivers the SDP answer to the original offerer.

Concurrently with the exchange of SDP offers and answers, both peers engage in the process of gathering ICE (Interactive Connectivity Establishment) candidates. ICE candidates represent potential network transport addresses and protocols (e.g., IP addresses, ports, TURN/STUN relay information) that the peers can use to establish a direct connection. These ICE candidates are also exchanged between the peers via the signaling server. The signaling server's role in this phase is purely facilitative, ensuring the secure and timely delivery of signaling messages between the peers. Security considerations for the signaling server include implementing robust authentication and authorization mechanisms to prevent unauthorized access and message manipulation. The signaling server should also employ secure communication channels (e.g., WSS for WebSockets) to protect the confidentiality and integrity of the signaling data.

Once both peers have successfully exchanged sufficient SDP and ICE information, they possess the necessary data to traverse NATs and firewalls and attempt to establish a direct peer-to-peer connection using the gathered candidates. The signaling server's involvement concludes once the direct WebRTC connection is successfully established, with subsequent data communication flowing directly between the peers, bypassing the signaling infrastructure.

3 Key Features

DarkSwap is distinguished by a suite of key features meticulously designed to deliver a truly decentralized, secure, and user-centric trading experience within the Bitcoin ecosystem.

A fundamental feature is the platform's decentralized peer-to-peer trading capability. Unlike centralized exchanges where users relinquish control of their assets to a third party, DarkSwap enables direct trading between users. This architecture significantly reduces counterparty risk and enhances censorship resistance, aligning with the core principles of decentralized finance.

DarkSwap is engineered to provide comprehensive support for trading native Bitcoin alongside emerging assets on the Bitcoin blockchain, specifically Runes and Alkanes. This broad asset support positions DarkSwap as a versatile platform for the evolving Bitcoin asset landscape.

The implementation of trustless atomic swaps, facilitated by Partially Signed Bitcoin Transactions (PSBTs), is a cornerstone of DarkSwap's security model. This feature ensures that trades are executed atomically, meaning either both legs of the swap are successfully completed on the blockchain, or neither is. This cryptographic guarantee eliminates the possibility of one party failing to uphold their end of the trade after the other has committed, thereby removing the need for trust between trading partners.

The distributed orderbook is another salient feature contributing to the platform's transparency and resilience. Instead of a single, centralized orderbook, order information is propagated and maintained across the decentralized network of peers. Users have access to their local copy of the orderbook and can directly identify and match with compatible orders from other participants. This distributed approach enhances the platform's resistance to manipulation and single points of failure.

Seamless wallet integration is crucial for a user-friendly decentralized trading experience. DarkSwap provides robust integration with compatible Bitcoin wallets, including those built using the Bitcoin Development Kit (BDK). This allows users to manage their Bitcoin, Rune, and Alkane balances and securely sign transactions required for trading directly within the DarkSwap environment, without exposing their private keys to the trading platform itself.

Browser compatibility, achieved through the strategic use of WebRTC and WebAssembly, significantly enhances the accessibility of DarkSwap. Users can access and utilize the full functionality of the platform directly within a standard web browser, eliminating the need for dedicated software installations and lowering the barrier to entry for new users.

Finally, DarkSwap's commitment to being open source is a key feature that fosters transparency, community engagement, and security. The entire codebase is publicly available, allowing for independent security audits, community contributions, and ensuring that the platform operates as described without hidden backdoors or vulnerabilities. This open approach builds trust and accelerates the development and improvement of the platform.

4 Security

Security is a foundational pillar of the DarkSwap platform, with meticulous attention paid to safeguarding user assets and ensuring the integrity of all trading operations. The decentralized nature of DarkSwap inherently provides significant security advantages over centralized alternatives by eliminating single points of failure and reducing susceptibility to censorship and malicious attacks targeting a central authority.

A cornerstone of DarkSwap's security framework is the implementation of trustless atomic swaps, facilitated by the strategic use of Partially Signed Bitcoin Transactions (PSBTs). As elaborated in the Trading Protocol section, this mechanism ensures that the exchange of assets is atomic: either both legs of the trade are successfully executed on the Bitcoin blockchain, or neither is. This cryptographic guarantee is paramount, as it removes the necessity for trust between trading participants and effectively prevents scenarios such as one party absconding with funds without completing their side of the swap. The reliance on native Bitcoin scripting capabilities and the well-audited PSBT standard, rather than introducing complex and potentially vulnerable smart contracts, further enhances the security posture of the trading process.

Cryptographic signatures are employed extensively throughout the DarkSwap network to ensure the authenticity and integrity of data. All trading orders and protocol-specific messages are cryptographically signed using the user's private keys. This process verifies the origin of messages and guarantees that they have not been tampered with in transit, thereby preventing unauthorized order manipulation or fraudulent trade initiation.

Robust wallet integration is another critical security consideration. DarkSwap integrates with reputable and security-focused Bitcoin wallet libraries, such as the Bitcoin Development Kit (BDK). By leveraging these established and audited solutions for key management and transaction signing, DarkSwap avoids the complexities and potential vulnerabilities associated with implementing custom wallet functionality. Users retain full control over their private keys, which never leave their local environment, significantly mitigating the risk of asset theft due to platform compromise.

The open-source nature of the entire DarkSwap codebase is a deliberate security measure. Public availability of the code allows for continuous scrutiny and independent security audits by the broader community and cybersecurity experts. This transparency fosters trust and facilitates the proactive identification and remediation of potential vulnerabilities, contributing to the long-term security and stability of the platform.

Furthermore, rigorous input validation and comprehensive error handling are implemented throughout the DarkSwap codebase. This defensive programming approach is essential for preventing unexpected behavior, mitigating potential attack vectors, and ensuring the platform's resilience in the face of malformed or malicious inputs.

While DarkSwap is designed to provide a highly secure trading environment, it is crucial to emphasize that users remain responsible for the security of their own wallets and the diligent management of their private keys. Adhering to best practices for personal wallet security, including the use of strong, unique passwords, enabling two-factor authentication where applicable, and securely backing up recovery phrases, is indispensable for protecting assets within the decentralized ecosystem. Compared to centralized exchanges, where users deposit funds into exchange-controlled wallets, DarkSwap's non-custodial approach fundamentally shifts control and responsibility to the user, representing a significant security advantage for those prioritizing self-custody.

5 Performance

The performance characteristics of DarkSwap are intrinsically linked to its decentralized architecture and the underlying networking and processing technologies employed. Key considerations for performance include the platform's scalability, the efficiency of order propagation across the P2P network, and the speed of trade execution.

Scalability is a significant advantage of DarkSwap's P2P architecture with a distributed orderbook. As the number of users and trading activity increase, the platform can scale horizontally by distributing the load of order processing and storage across a larger number of peers. This contrasts with centralized exchanges, which can experience performance bottlenecks under high load due to their centralized infrastructure. However, the efficiency of order propagation via the GossipSub protocol in a very large and dynamic network presents a continuous area for monitoring and optimization. Factors such as network latency, peer churn (peers frequently joining and leaving the network), and the sheer volume of orders can impact the speed at which orderbook updates are disseminated and the consistency of the orderbook view across all participating peers. Ongoing efforts in optimizing message serialization, compression techniques, and network topology management are crucial for maintaining a responsive and synchronized distributed orderbook.

The speed of trade execution in DarkSwap is primarily determined by two factors: the latency of the direct P2P connection established between the trading peers for negotiation and the confirmation times on the Bitcoin blockchain for the final atomic swap transaction. While the P2P negotiation phase is typically fast, occurring directly between peers, the ultimate finality of the trade is contingent upon the inclusion of the resulting PSBT in a Bitcoin block. Bitcoin block confirmation times are inherently variable and outside the direct control of the DarkSwap platform.

Resource utilization is another important performance aspect. The core logic of the DarkSwap SDK is implemented in Rust, a language known for its performance and efficiency. The use of optimized data structures and algorithms for critical operations such as orderbook management and trade processing contributes to minimizing resource consumption. For browser-based clients utilizing the web interface, the performance of WebAssembly bindings, which allow the Rust-based SDK to run in the browser, and the efficiency of WebRTC data channels for direct peer-to-peer communication are key factors influencing the user experience.

Continuous performance testing, profiling, and optimization efforts are integral to the DarkSwap development process. These activities aim to identify and address potential performance bottlenecks as the network grows and trading volume increases, ensuring that DarkSwap remains a fast, responsive, and efficient trading platform.

6 Future Development

The DarkSwap project is committed to continuous evolution and improvement, guided by a strategic roadmap focused on expanding its capabilities, refining the user experience, and broadening its impact within the decentralized trading landscape. Future development efforts are prioritized to address key areas identified for enhancing the platform's functionality, performance, and accessibility.

Key areas for future development include the implementation of more advanced trading features. This encompasses the introduction of sophisticated order types beyond basic market orders, such as limit orders and stop orders, to provide users with greater control and flexibility over their trading strategies. Exploration into more complex atomic swap types may also be pursued to support a wider range of cross-asset exchanges.

Further optimization of the P2P network efficiency is a critical focus area. Efforts will be directed towards enhancing the speed and reliability of order propagation and overall network resilience. This may involve exploring alternative or complementary network protocols and optimizing existing mechanisms to ensure efficient data dissemination in a growing network.

Expanding enhanced wallet support is another priority to improve user accessibility and convenience. Plans include integrating with a wider array of compatible Bitcoin wallets to offer users more choices and potentially exploring support for assets on other blockchain networks in the future, contingent upon thorough technical evaluation and user demand.

Continuous user interface enhancements for the web platform are planned, driven by user feedback. The focus will be on improving usability, optimizing performance, and providing more comprehensive trading tools, charts, and visualizations to create a more engaging and efficient trading experience.

To cater to the growing mobile user base, the development of native mobile applications for iOS and Android is a key future objective. These applications will aim to provide a seamless and optimized DarkSwap trading experience on mobile devices.

Increasing asset support is a potential area for expansion, involving the careful evaluation and integration of additional Bitcoin-based assets or assets residing on other compatible blockchains, based on their technical specifications and security implications.

Finally, the project intends to establish a framework for community governance, enabling greater involvement of the DarkSwap community in the project's direction and key decision-making processes, fostering a truly decentralized and community-driven platform.

The DarkSwap team remains dedicated to building a robust, decentralized, and user-centric trading platform that serves the evolving needs of the Bitcoin ecosystem.