DarkSwap

A Decentralized Exchange for Bitcoin, Runes, and Alkanes

Whitepaper v1.0

DarkSwap Team

April 21, 2025

Contents

Abstract

DarkSwap is a decentralized exchange (DEX) platform designed specifically for Bitcoin, runes, and alkanes. Unlike traditional centralized exchanges, DarkSwap enables direct peer-to-peer trading without intermediaries, enhancing security, privacy, and user control. This whitepaper presents the architecture, technical components, and security model of DarkSwap, highlighting its innovative approach to decentralized trading on Bitcoin. By leveraging advanced peer-to-peer networking, WebRTC technology, and end-to-end encryption, DarkSwap provides a secure, private, and user-friendly platform for cryptocurrency trading without the risks associated with centralized exchanges.

1 Introduction

The cryptocurrency ecosystem has seen significant growth in decentralized finance (DeFi) applications, particularly decentralized exchanges. However, most existing DEX solutions focus on Ethereum and other smart contract platforms, with limited support for Bitcoin—the largest and most established cryptocurrency. Additionally, the emergence of runes and alkanes as new asset types on Bitcoin has created a need for specialized trading platforms.

DarkSwap addresses this gap by providing a decentralized exchange specifically designed for Bitcoin, runes, and alkanes. By enabling direct peer-to-peer trading without centralized intermediaries, DarkSwap eliminates the risks associated with centralized exchanges, such as hacks, asset freezes, and privacy concerns.

The key innovations of DarkSwap include:

- A pure peer-to-peer architecture with no central server or authority
- Advanced WebRTC-based networking for browser and desktop compatibility
- Circuit relay technology for reliable NAT traversal
- End-to-end encryption for secure communications
- Comprehensive authentication and authorization systems
- Efficient connection pooling and relay discovery mechanisms
- Cross-platform support across desktop and web environments

This whitepaper provides a detailed overview of DarkSwap's architecture, components, security model, and roadmap, demonstrating how it addresses the challenges of decentralized trading on Bitcoin.

2 Background and Problem Statement

2.1 Centralized Exchange Risks

Centralized cryptocurrency exchanges have been plagued by numerous issues:

- **Security Breaches**: Numerous high-profile hacks resulting in billions of dollars in losses
- **Asset Control**: Users must surrender control of their private keys
- **Counterparty Risk**: Exposure to exchange insolvency or mismanagement
- **Privacy Concerns**: KYC requirements and transaction monitoring
- **Censorship**: Ability to freeze assets or block transactions
- **Regulatory Uncertainty**: Vulnerability to changing regulations

2.2 Limitations of Existing DEX Solutions

While decentralized exchanges address many of these issues, they come with their own limitations:

- **Limited Bitcoin Support**: Most DEXs focus on Ethereum and other smart contract platforms

- **Complex User Experience**: Technical barriers for average users
- **Connectivity Issues**: P2P systems often struggle with NAT traversal
- **Limited Asset Support**: Few platforms support runes and alkanes
- **Performance Constraints**: Slower execution compared to centralized alternatives
- **Liquidity Challenges**: Fragmented liquidity across platforms

2.3 The Need for Bitcoin-Native DEX

Bitcoin's ecosystem has evolved with the introduction of runes and alkanes, creating new opportunities for asset creation and trading. However, these innovations lack dedicated trading infrastructure that preserves Bitcoin's core values of decentralization, security, and user sovereignty.

A Bitcoin-native DEX must address several unique challenges:

- Operating without smart contracts that are common on other platforms
- Ensuring secure peer-to-peer trading of Bitcoin and Bitcoin-based assets
- Providing reliable networking across diverse network conditions
- Maintaining privacy while enabling efficient trading
- Supporting cross-platform usage, including browsers

DarkSwap is designed specifically to address these challenges, providing a secure, private, and user-friendly platform for trading Bitcoin, runes, and alkanes without centralized intermediaries.

3 Solution Overview

DarkSwap is a comprehensive decentralized exchange platform built on a pure peer-to-peer architecture. It enables direct trading between users without relying on centralized servers or authorities for matching or executing trades.

3.1 Core Principles

DarkSwap is built on the following core principles:

- **Decentralization**: No central authority controls the platform or user funds
- **Security**: Strong encryption, authentication, and authorization mechanisms
- **Privacy**: Minimal data collection and end-to-end encrypted communications
- **User Control**: Users maintain control of their private keys and funds
- **Usability**: Intuitive interfaces that abstract technical complexity
- **Cross-Platform**: Support for both desktop and web environments

3.2 Key Components

DarkSwap consists of several key components:

- **DarkSwap SDK**: Core functionality and APIs
- **DarkSwap CLI**: Command-line interface for interacting with the platform
- **DarkSwap Daemon**: Background service for handling ongoing operations
- **DarkSwap P2P**: Peer-to-peer networking infrastructure
- **Web Interface**: Browser-based user interface

3.3 Trading Flow

The typical trading flow in DarkSwap follows these steps:

1. User creates or imports a wallet
2. User connects to the P2P network
3. User browses the distributed order book
4. User places a buy or sell order
5. Order is broadcast to the network
6. When a matching order is found, users are connected directly
7. Trade is executed peer-to-peer with atomic swap guarantees
8. Transaction is broadcast to the Bitcoin network
9. Order book is updated to reflect the completed trade

This flow ensures that users maintain control of their funds throughout the trading process, with no centralized intermediary holding custody at any point.

4 Technical Architecture

DarkSwap employs a modular architecture with clear separation of concerns, allowing for independent development, testing, and deployment of components.

4.1 System Architecture

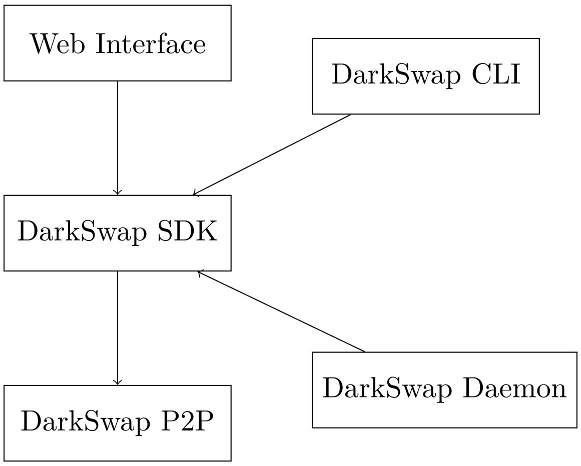

Figure 1: DarkSwap System Architecture

4.2 Component Details

4.2.1 DarkSwap SDK

The SDK provides the core functionality and APIs, including:

- Wallet management
- Order book handling
- Trade execution
- Type definitions

It is implemented in Rust for performance, security, and cross-platform compatibility, with WebAssembly bindings for browser environments.

4.2.2 DarkSwap P2P

The P2P networking layer is a critical component, providing:

- WebRTC transport for browser compatibility
- Circuit relay for NAT traversal
- Connection pooling for efficient connection management
- Relay discovery and ranking
- Authentication and authorization
- End-to-end encryption
- Metrics and monitoring

This component enables reliable peer-to-peer communication across diverse network conditions, including browsers and devices behind NATs.

4.2.3 DarkSwap CLI

The command-line interface provides:

- User commands for trading and wallet management
- Configuration management
- Status reporting
- Automation capabilities

4.2.4 DarkSwap Daemon

The background service handles:

- Long-running processes
- Event handling
- System integration
- Network maintenance

4.2.5 Web Interface

The browser-based interface provides:

- React components for user interaction
- WebRTC integration for P2P communication
- Responsive design for various devices
- WebAssembly integration with the SDK

4.3 Technology Stack

DarkSwap leverages a modern technology stack:

- **Programming Languages**:
  - Rust for core components, SDK, daemon, and CLI
  - TypeScript for web interface and browser integration
  - WebAssembly (WASM) for running Rust code in browsers
- **Core Libraries**:
  - libp2p for peer-to-peer networking
  - tokio for asynchronous runtime
  - ring for cryptographic operations
  - bdk (Bitcoin Dev Kit) for Bitcoin wallet functionality
  - React for web UI
  - WebRTC for browser-based P2P communication

5 Key Features and Components

5.1 P2P Networking

DarkSwap's P2P networking layer is built on several innovative technologies:

5.1.1 WebRTC Transport

WebRTC enables direct browser-to-browser communication, allowing DarkSwap to work in web environments without centralized servers. Key features include:

- Direct peer connections using WebRTC data channels
- Signaling server for initial connection establishment
- ICE candidate exchange for NAT traversal
- Efficient binary data transfer

5.1.2 Circuit Relay

To overcome NAT traversal challenges, DarkSwap implements circuit relay:

- Relay nodes facilitate connections between peers behind NATs
- Relay discovery mechanism finds and ranks available relays
- Connection establishment through optimal relay paths
- Fallback mechanisms for challenging network conditions

5.1.3 Connection Pooling

For efficient connection management, DarkSwap implements connection pooling:

- Reuse of existing connections to reduce overhead
- Connection lifecycle management
- Automatic pruning of expired connections
- Performance optimization for high-traffic scenarios

5.2 Security Features

5.2.1 Authentication and Authorization

DarkSwap implements a comprehensive authentication system:

- Multiple authentication methods (shared key, challenge-response, public key)
- Authorization levels for different operations
- Trusted and banned peer management
- Token-based authentication with automatic expiration

5.2.2 End-to-End Encryption

All communications are protected with strong encryption:

- Multiple encryption algorithms (AES-GCM-256, ChaCha20-Poly1305)
- X25519 key exchange for secure key agreement
- Forward secrecy with ephemeral keys
- Key rotation and automatic key expiration

5.3 Wallet Integration

DarkSwap supports multiple wallet implementations:

- Simple wallet for basic functionality
- BDK wallet for advanced Bitcoin operations
- Support for Bitcoin, runes, and alkanes
- Secure key management
- Transaction creation and signing

5.4 Order Book Management

The distributed order book system provides:

- Order creation and validation
- Order storage and retrieval
- Order matching algorithms
- Order distribution across the network

5.5 Trade Execution

The trade execution system ensures:

- Secure peer-to-peer trade protocol
- Transaction validation
- Atomic swap guarantees
- Error handling for failed trades

5.6 Monitoring and Metrics

For system health and performance tracking:

- Comprehensive metrics collection
- Prometheus integration
- Grafana dashboards
- Alerting system

6 Security Model

DarkSwap employs a defense-in-depth security approach with multiple layers of protection.

6.1 Threat Model

The security model addresses several threat vectors:

- **Network Attacks**: Man-in-the-middle, eavesdropping, replay attacks
- **Identity Spoofing**: Impersonation of peers or relays
- **Denial of Service**: Resource exhaustion attacks
- **Trade Manipulation**: Attempts to manipulate order matching or execution
- **Wallet Compromise**: Unauthorized access to wallet keys

6.2 Security Layers

6.2.1 Network Security

- End-to-end encryption of all communications
- Authenticated connections between peers
- Secure relay selection and connection
- Protection against replay and man-in-the-middle attacks

6.2.2 Authentication Security

- Multiple authentication methods for flexibility and strength
- Challenge-response protocols for secure verification
- Token-based authentication with automatic expiration
- Authorization levels for access control

6.2.3 Wallet Security

- Local key storage with no server uploads
- Optional encryption of wallet files
- Minimal exposure of private keys
- Transaction verification before signing

6.2.4 Trade Security

- Atomic swap protocols for trade execution
- Transaction validation before acceptance
- Protection against double-spending attempts
- Timeout mechanisms for incomplete trades

6.3 Security Principles

DarkSwap follows key security principles:

- **Defense in Depth**: Multiple security layers
- **Principle of Least Privilege**: Minimal access rights
- **Forward Secrecy**: Protection of past communications
- **Zero Trust**: Verification of all peers and operations
- **Fail Secure**: Default to secure state on failure

7 Use Cases

DarkSwap addresses several key use cases for different user types.

7.1 Bitcoin Trading

- Secure peer-to-peer Bitcoin trading without intermediaries
- Private transactions without KYC requirements
- Self-custody throughout the trading process
- Protection from exchange hacks and freezes

7.2 Runes and Alkanes Trading

- Specialized support for these Bitcoin-based assets
- Efficient discovery of trading partners
- Secure execution of trades
- Integration with Bitcoin wallets supporting these assets

7.3 Privacy-Focused Trading

- End-to-end encrypted communications
- No central server monitoring transactions
- Minimal data collection and storage
- Protection from surveillance and tracking

7.4 Cross-Platform Trading

- Consistent experience across desktop and web
- Browser-based trading without downloads
- Desktop application for enhanced performance
- Interoperability between platforms

7.5 Developer Integration

- SDK for building custom applications
- API access for integration with other services
- Extensible architecture for custom features
- Documentation and examples for developers

8 Roadmap

DarkSwap development follows a phased approach:

8.1 Phase 1: Foundation (Completed)

- Core P2P networking infrastructure
- Basic wallet integration
- Simple order book functionality
- Command-line interface

8.2 Phase 2: Enhancement (Completed)

- Advanced P2P capabilities
- Improved wallet functionality
- Enhanced order book and trade execution
- Initial web interface

8.3 Phase 3: Production Readiness (Current)

- Security hardening (authentication, encryption)
- Performance optimization
- Comprehensive testing
- Monitoring and metrics
- User experience improvements

8.4 Phase 4: Public Launch (Planned)

- Public beta release
- Community building
- Documentation and tutorials
- Bug fixes and stability improvements

8.5 Phase 5: Ecosystem Growth (Future)

- API enhancements for developers
- Additional asset support
- Advanced trading features
- Mobile applications
- Integration with other Bitcoin projects

9 Conclusion

DarkSwap represents a significant advancement in decentralized exchange technology for Bitcoin, runes, and alkanes. By combining innovative peer-to-peer networking, strong security features, and user-friendly interfaces, DarkSwap addresses the limitations of both centralized exchanges and existing DEX solutions.

The platform's modular architecture, advanced P2P capabilities, and comprehensive security model provide a solid foundation for secure, private, and efficient trading without centralized intermediaries. As DarkSwap progresses through its roadmap, it aims to become the leading decentralized exchange for Bitcoin and Bitcoin-based assets, empowering users with true financial sovereignty.

By prioritizing security, privacy, and user control, DarkSwap aligns with the core principles of Bitcoin itself, offering a trading platform that preserves these values while providing the functionality and user experience expected in modern financial applications.

10 References

1. Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto, 2008.
2. WebRTC 1.0: Real-Time Communication Between Browsers. W3C, 2021.
3. libp2p: A Modular Network Stack. Protocol Labs, 2022.
4. Circuit Relay Protocol. libp2p Specifications, 2023.
5. Bitcoin Development Kit (BDK) Documentation, 2024.
6. Atomic Swap Protocol for Cryptocurrencies, 2020.
7. Runes: A Bitcoin-Native Asset Protocol, 2023.
8. Alkanes: Extended Asset Protocol for Bitcoin, 2024.