RexBit

Litepaper

(Testnet)

Nov
2024

A Decentralized Crypto Exchange That Enhances User Experience & Performance

We use new technology so that the user has the best user experience, security and self-custody

Content

Intro.....2

Content.....3

Overview.....4

Vision.....4

Problem Statement.....4

Our solution 1.....5

Our solution 2.....6

How It Works?.....7

Technology 1.....8

Super State Channels.....8

Technology 2.....9

Blind Computing.....9

Wallet MPC TSS + AA...10

Roadmap.....11

FAQs.....12

Note.....13

End Page.....14

Vision for Rexbit

In 5 years, RexBit becomes the largest exchange by volume in perps, spot, of crypto and RWAs (CFDs on-chain).

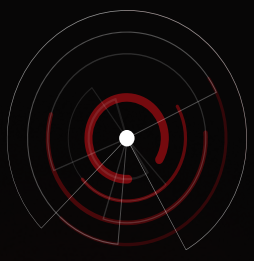
Problem Statement

Decentralized exchanges (DEXs) have changed crypto trading, but they still face significant challenges:

- **User Experience** 🤔**.** Complex interfaces deter non-technical users. Limits broader adoption of decentralized trading platforms (>4 click per action, ≈>1 minute per action & ≈> $1USD per action.)
- **Latency Issues** ⏳**.** Transaction delays hinder real-time trading. Frustrates users seeking instant results.
- **Miner Extractable Value** (*MEV*) ⚔️**.** Miners can reorder or exclude transactions to extract additional profits, enabling unfair practices like front-running.
- **Interoperability Issues** 🌐**.** Liquidity is scattered across blockchains, limiting market depth. Traders on different chains can't easily connect, reducing efficiency.

We stopped there to keep it simple, but there are many more

Our Solution



A decentralized exchange that improves user experience & performance. RexBit Exchange is here to reshape the decentralized trading experience with cutting-edge technology and a user-centered approach.

- **Zero Gas Fees** 🎁. No gas fees for shares within the DEX, making transactions more affordable and accessible. 100% Gas Free.
- **Zero Latency** 🪨. Sub-millisecond transaction finality for real-time trading without typical blockchain delays. <1ms Finality.
- **Zero Friction** 🎯. 1-click trading experience, mirroring the ease of centralized exchanges.
- **Efficiency** 📈. Trade without MEV, slippage. ~0% Slippage.
- **Blind Computing Orderbook** 🕶️. Private transaction details until execution, ensuring maximum confidentiality and security. Decentralized blind computation.
- **Interoperability** 🌐. EVM agnostic.Trade with users from all blockchains without even realizing it. All your blockain tokens as 1 only.
- **Hybrid Access** 💫. Choose between Web3 and Web2 login methods, offering versatility in access. Multiple Login Options. MPC TSS + AA Technology (*Athena*).
- **Bridges** 📻. Send tokens between blockchains instantly and P2P. Secure & no waiting.

Our Solution

Feature	RexBit Exchange (DEX)	Traditional DEXs	CEXs
Gas Fees	100% Gas Free	Variable gas fees	Non-existent concept
Transaction Speed	<1ms Finality	Slower due to blockchain confirmations	Fast, centralized processing
Privacy	Private until after execution with CLOB	Public transaction details (MEV)	Centralized data
Interoperability	👉EVM agnostic. 👉Trade with users from all blockchains without even realizing it. 👉All your blockain tokens as 1 only.	👉Limited to specific chains 👉Limited to blockchain users 👉Fragmented Liquidity	Typically limited to supported assets
User Experience	👉Zero Gas ($0 USD) 👉 Zero Friction (1 click per action) 👉Zero Latency (<1ms)	Often bad & complex interfaces and user experience (>clicks, > waiting time & spend on gas fees)	User-friendly but centralized
Slippage	Low Slippage (No MEV)	Variable slippage (MEV Problems). Depend AMM or slow CLOBs	Low Slippage. Centralized data.
Security	Privacy. Self-custody. Dependent on SC security	Self-custody. Dependent on SC security	Possible failures like FTX
Accessibility	Web3 and Web2 Login Options, Telegram	Primarily Web3	Web2-centric, broader user base

How It Works

RexBit Exchange operates through a simple process ensuring efficiency, cost-effectiveness, and security:

1- Deposit Funds 🔗

Lock your assets into a secure smart contract (*Vault*) on your chosen blockchain. This keeps your funds safe and ready for trading without unnecessary risks.

2- Connect 🧿

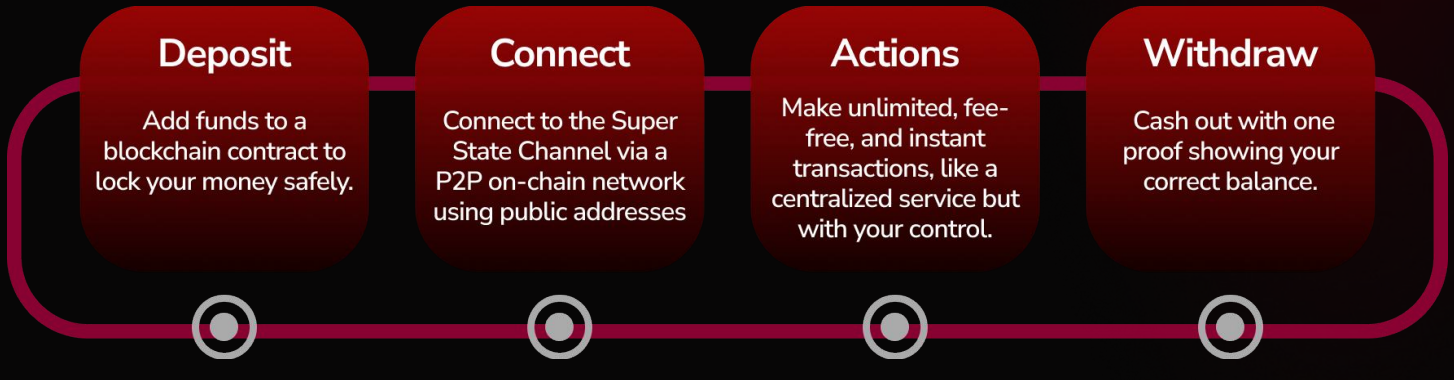
Connect to the **Super State Channel (*SSC*)** via a peer-to-peer (P2P) on-chain network using your public addresses. This connection provides a secure and seamless trading experience.

3- Trade Instantly ⚡

Execute unlimited transactions without gas fees or delays. Advanced state channels enable instant trading, allowing you to seize market opportunities in real-time.

4- Withdraw Funds 💸

Unlock and withdraw your funds from the smart contract. Transfer assets to any blockchain or convert them to fiat and send directly to your bank account.



Technology

Super State Channels (SSC)

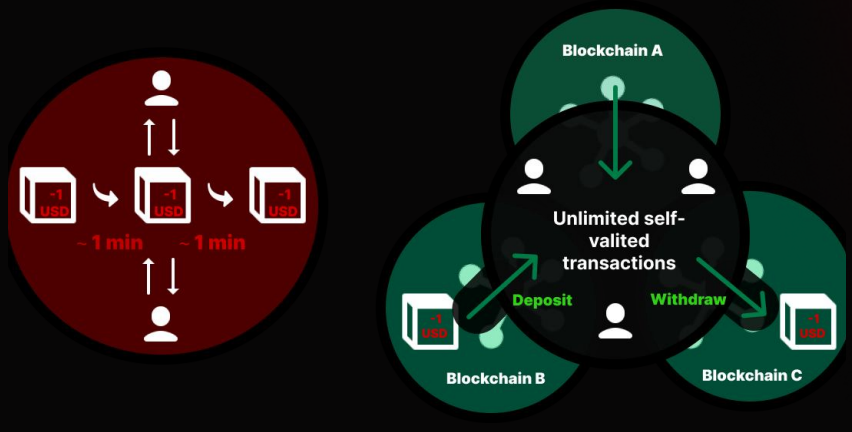
Super State Channels improve blockchain speed and privacy. They use P2P communication and on-chain contracts to enable fast, secure transactions without overloading the blockchain, keeping all data private with zero-knowledge proofs.

Example

Imagine you have several friends. Some go to **Mars**, others to **Jupiter**, and the rest stay on Earth. Each group wants to play different games on their respective planets (*e.g., on Earth, some friends want to play Monopoly and others Jenga*). They initially kept a list of everyone's moves to prevent cheating, but for "recurrent transactions," they found a better way:

- Before playing, they lock their money in a smart contract (*set funds aside*).
- They play without gas fees, delays, or friction, just like Web2 but with full control.
- Sending money between planets is instant and secure, with no need for bridges.
- If there's a dispute, the blockchain acts as the referee.
- Players can withdraw or move their money whenever they want.

Blockchain A **Super State Channels**



RexBit

Technology

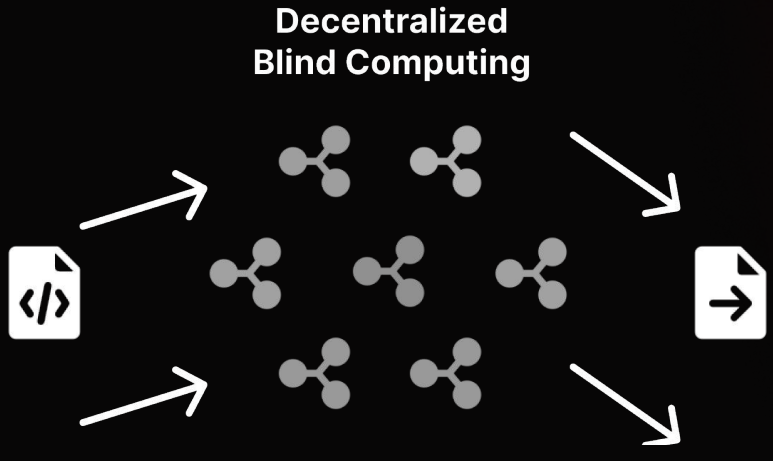
Blind Computing

CLOB Blind Computation enhances privacy, security, and efficiency in decentralized trading by using cryptographic techniques to perform order matching without exposing sensitive data. Computation is done without revealing individual inputs, ensuring privacy and security while enabling decentralized order execution.

What is CLOB Blind Computation? CLOB Blind Computation uses MPC protocols to securely execute transactions without revealing order sizes, prices, or identities. It preprocesses data into secure shares, allowing encrypted computations while keeping data confidential.

Benefits

- **Privacy:** Keeps trading strategies and order details hidden.
- **Security:** Protects sensitive data throughout all trading stages.
- **Efficiency:** Facilitates fast transactions without compromising privacy.



Technology

Wallet MPC TSS + AA

We combine MPC-TSS + AA to solve key challenges in decentralized finance. MPC-TSS distributes key fragments among multiple parties, eliminating single points of failure. AA removes the need for traditional private keys, enabling smart contract-based account management that improves user experience and simplifies transactions.

MPC and TSS

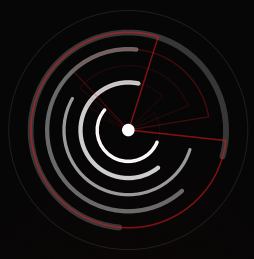
- **MPC splits private keys** into **fragments** distributed across different parties, enhancing security.
- **TSS** uses fragmented keys to **authorize transactions** without ever fully reconstructing the key, maintaining security and flexibility.

Account Abstraction

- **Gasless Transactions:** Users pay gas fees with tokens like USDC or have them sponsored by RexBit.
- **Transaction Batching:** Multiple actions are bundled to save costs.
- **Automated Payments and Recovery:** Recurring transactions and social recovery eliminate seed phrase requirements.
- **Programmable Security:** Features like spending limits and multi-signatures increase wallet control.

Note: *Gas fees only apply during deposits or withdrawals on RexBit. With Super State Channels, **all internal transactions are gas-free**, and we subsidize these fees (deposit/withdraw) when using a RexBit wallet (Mainnet). All concepts presented in context within the Super State Channels* 🧐

Roadmap



🌟 Our Path to Revolutionizing On-Chain Trading We have outlined a clear path to revolutionize the financial ecosystem, structured into four distinct phases inspired by Greek mythology. Each phase represents strategic growth and innovation as we lead the future of decentralized finance.

Phase 1: Prometheus 🔥 Igniting Innovation

- **Launch & Testnet:** Release the public testnet to demonstrate RexBit's key features.
- **Community Engagement:** Build early adopter community for feedback.
- **Partnerships & Security:** Form partnerships and conduct security audits.

Phase 2: Athena 🛡️ Strategic Growth

- **Mainnet Launch:** Deploy mainnet with enhanced trading features for a seamless experience.
- **Advanced Tools:** Introduce leverage, stop-loss, and multi-chain asset transfers to empower traders. Blind Computing, hybrid access...

Phase 3: Hyperion 🌅 Scaling Globally

- **Global Reach:** Expand with multilingual support and localized partnerships.
- **New Features:** Integrate AI analytics, trading bots, and liquidity incentives to boost engagement.

Phase 4: Kronos ⏳ Institutional Integration

- **Institutional Solutions:** Develop solutions for institutional investors, focusing on risk management and compliance.
- **Next-Gen Technologies:** Explore new trading technologies and financial products.

FAQs

What is the RexBit Exchange Testnet? 🛠️

The Testnet is RexBit's playground where you can experiment and get a feel for our platform without real financial risks. Test all features before the official launch.

How can I participate in the Testnet? 🚀

Visit our website, create an account, connect your Web2/Web3 credentials (*like Google or MetaMask*), and deposit test tokens to start trading.

How can I submit a RexBit Improvement Proposal (*RIP*)?

To submit an RIP, request access from the RexBit team.

What features are available on the Testnet? 🔍

The Testnet allows users to trade perpetual futures with 1-click actions, <1ms finality, $0 gas fees, and privacy for all orders until execution.

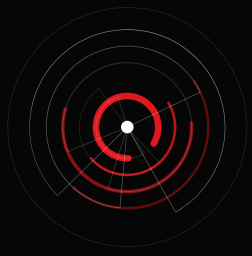
How secure is the Testnet? 🔒

The Testnet is a sandbox for testing—safe and isolated, using test tokens with no real-world value.

How long will the Testnet be active? ⏳

The Testnet will be active for some months until we ensure everything runs smoothly.

Note



Please note that while we strive to provide accurate and up-to-date information, certain aspects of our platform and services may be subject to change due to unforeseen circumstances or external factors. Our team is committed to adapting and improving in response to these changes, always prioritizing the best interests of our users and community. We encourage you to stay informed and engaged with our project to ensure that you're always aware of the latest developments and updates.

RexBit