System Architecture Documentation

ZK Dark Pool Trading System

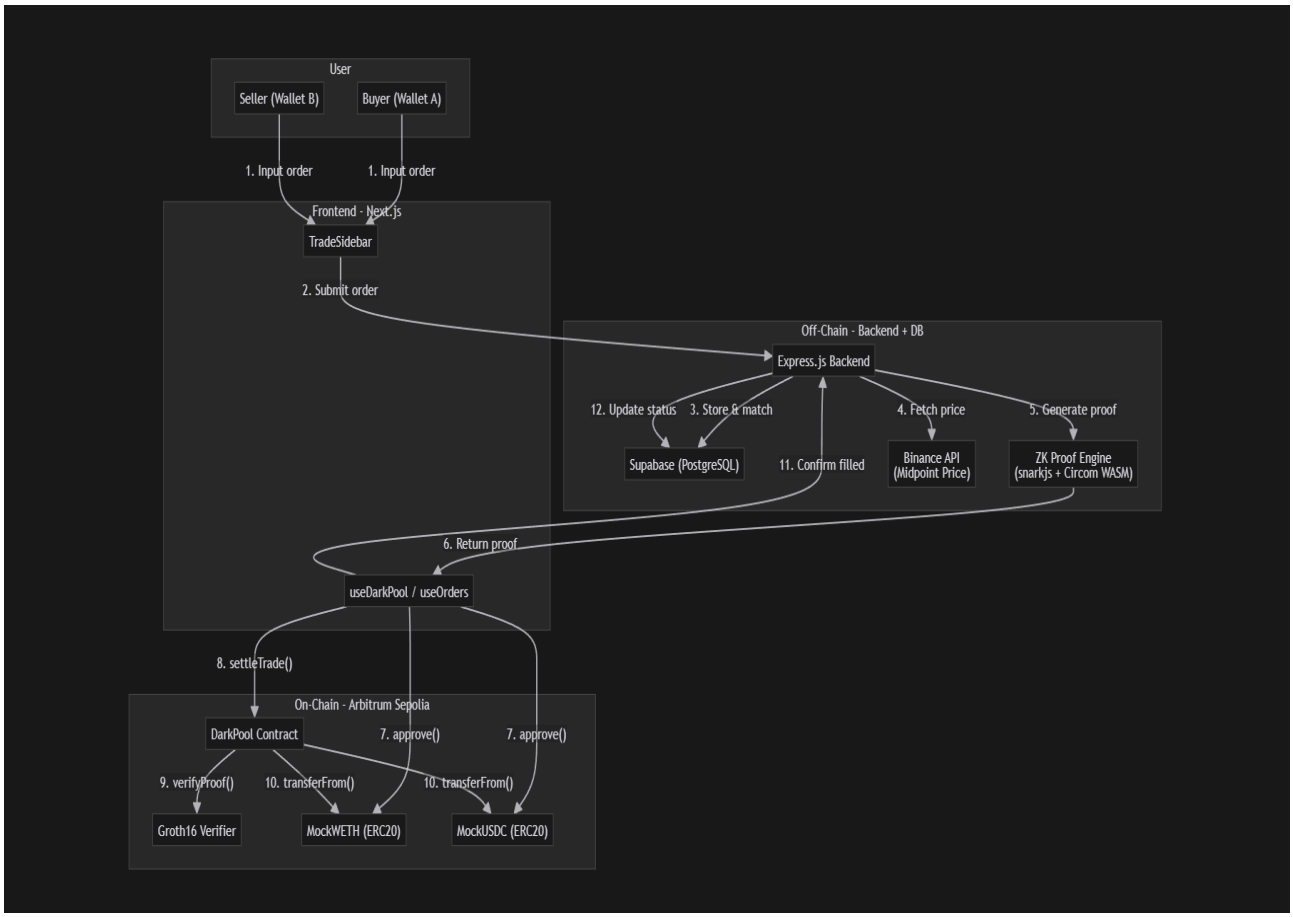
This document describes the system architecture and workflow of the ZK-based Dark Pool trading system. It covers frontend, backend, off-chain services, on-chain smart contracts, and zero-knowledge proof integration.

1. System Overview

The system enables private trading using off-chain order matching and zero-knowledge proofs for on-chain settlement. Orders are submitted via frontend, matched in backend, verified through ZK proofs, and settled on blockchain.

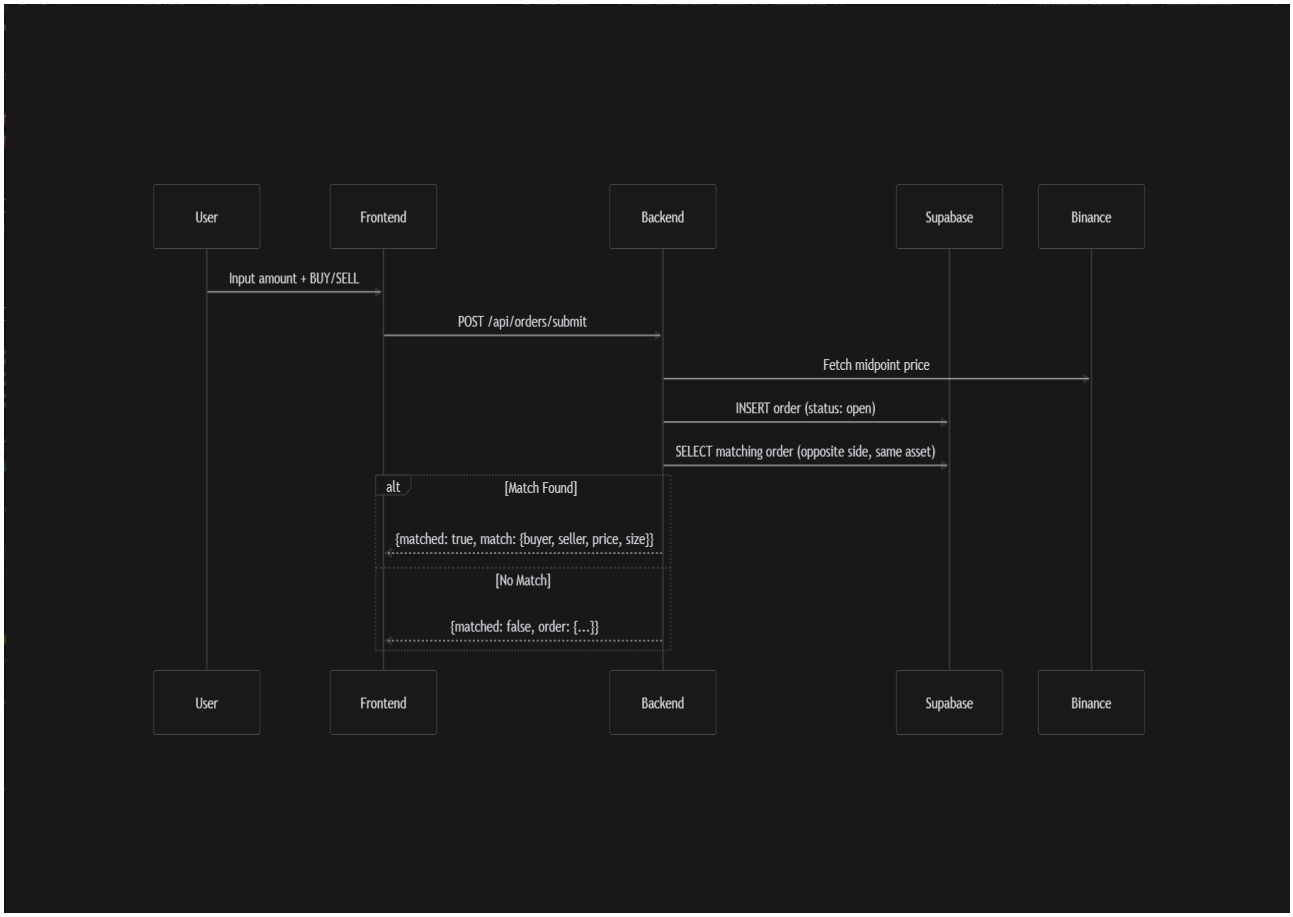
2. High-Level Architecture

This diagram shows the interaction between users, frontend, backend, database, ZK engine, and blockchain.



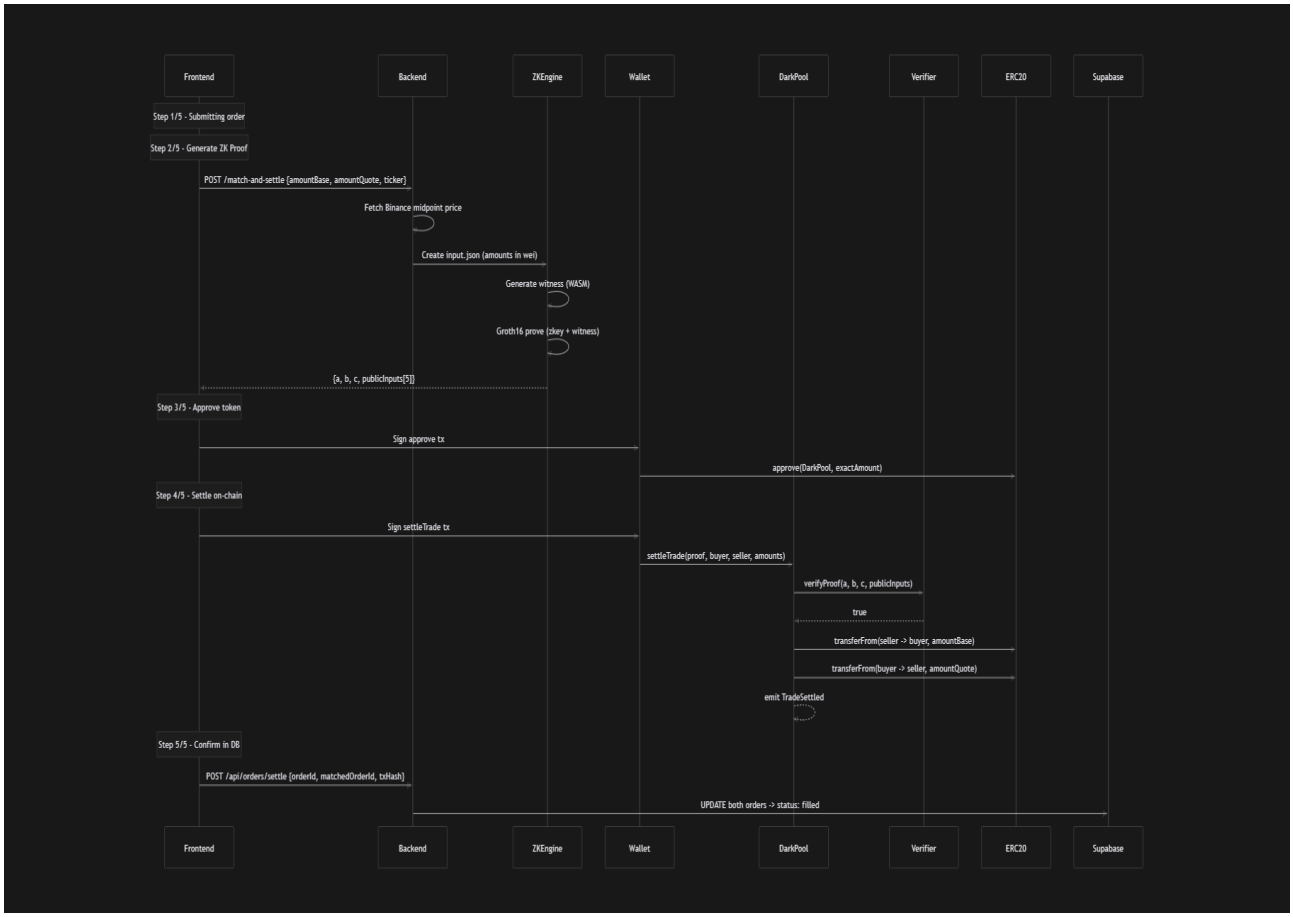
3. Order Matching Flow

This sequence illustrates how orders are submitted, stored, and matched in the backend.



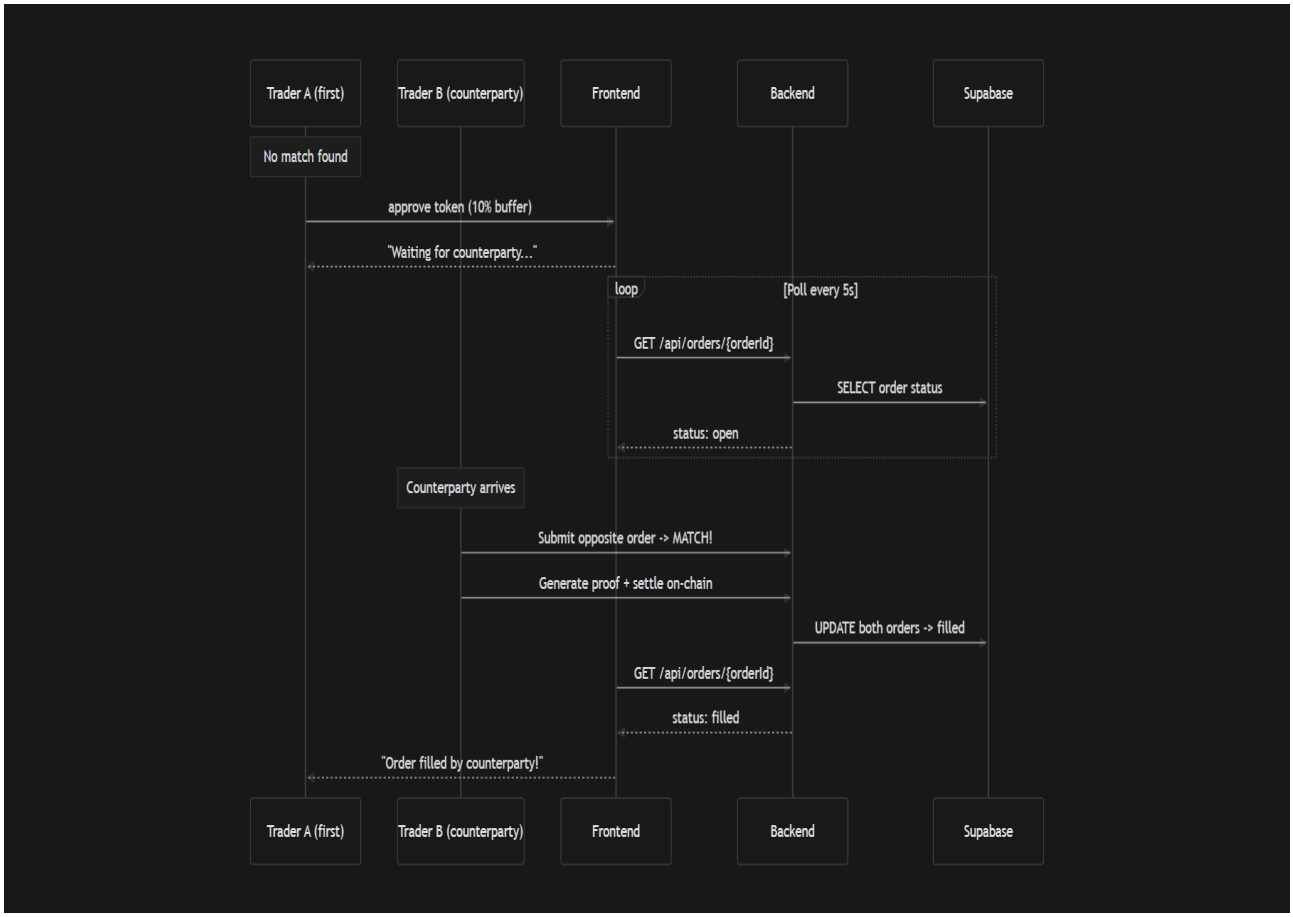
4. ZK Proof and Settlement Flow

This diagram explains proof generation, approval, and on-chain settlement process.



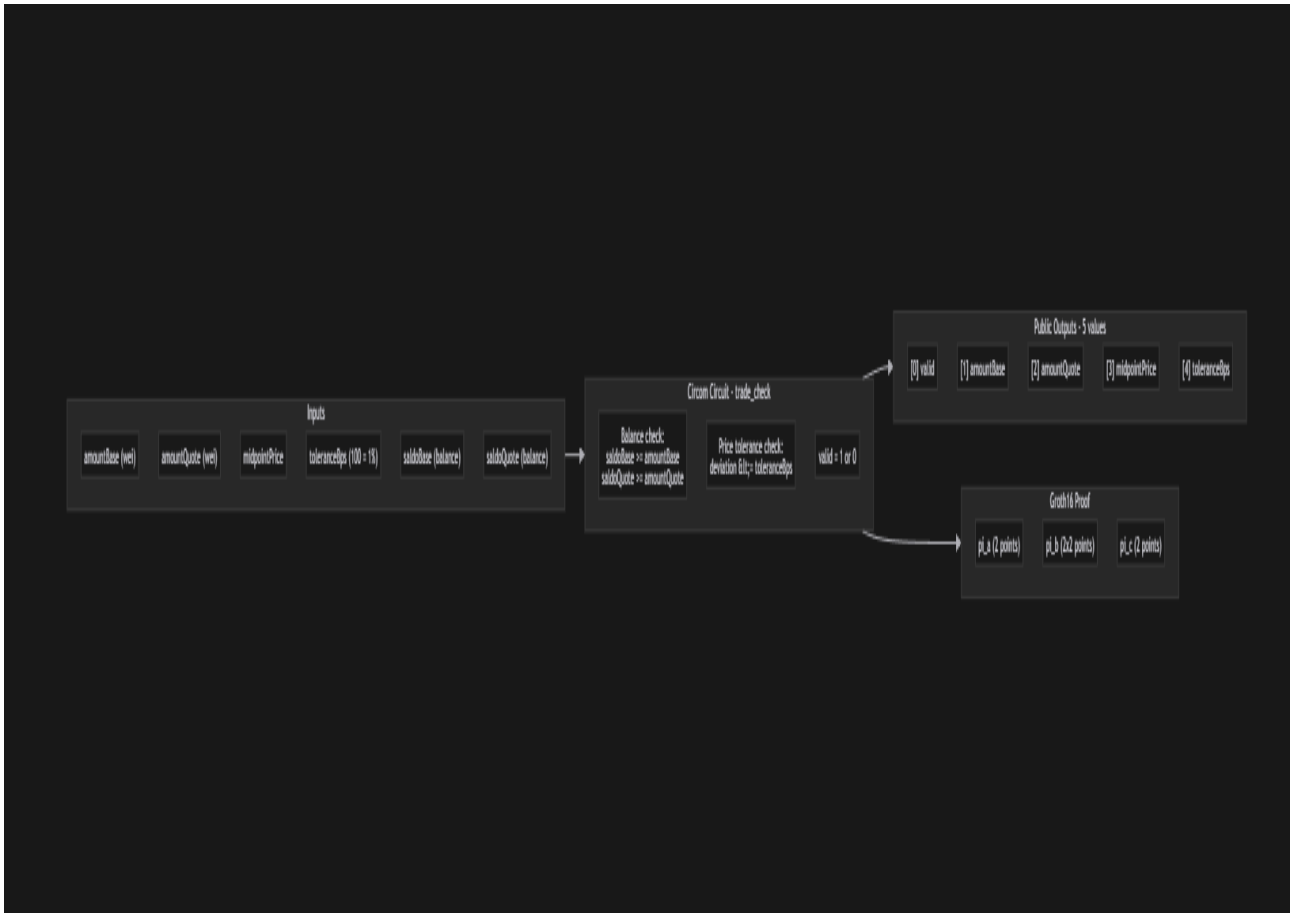
5. Order Lifecycle

This flow describes how orders remain open, get matched, and finalized.



6. ZK Circuit Design

This diagram shows the internal structure of the zero-knowledge circuit.



7. Component Architecture

Frontend:
- Built with Next.js
- Handles order input, approval, and transaction signing

Backend:
- Built with Express.js
- Handles order storage, matching, price fetching, and proof generation

Database:
- Supabase (PostgreSQL)
- Stores order status and matching records

ZK Engine:
- SnarkJS + Circom WASM
- Generates Groth16 proofs

Blockchain:
- Arbitrum Sepolia
- Smart contracts handle verification and settlement

External Services:
- Binance API for midpoint price

8. Security Considerations

- Zero-knowledge proofs ensure trade validity without revealing sensitive data.
- Smart contracts verify proofs before settlement.
- Token approvals are limited to required amounts.
- Backend does not custody user funds.
- Off-chain matching reduces MEV exposure.

9. Conclusion

This architecture provides a secure and privacy-preserving trading system using off-chain matching and on-chain zero-knowledge verification. It balances performance, privacy, and decentralization.