Permissioned Auctions on Suave with Zero-Knowledge Proofs

Has anyone integrated ZK verifiers into a SUAPP?

An immediate use case for this architecture is privacy-preserving transaction authorization for SUAPP auctions. A user must supply a valid ZKP in order to submit a transaction into a SUAPP. Reference this mention of ZK in the docs here and here.

ZK + Suave = Privacy in Multiple Layers

Zero-knowledge proofs would handle access control before Suave's TEE processes auction logic, providing an additional layer of configurable privacy.

FIRST: Zero-Knowledge Authorization Layer

- Participants prove eligibility without revealing credentials
- Supports complex qualification criteria (token holdings, trading history, KYC status)
- Authorization proofs are verified before bid submission
- Credential privacy is maintained even from the auction operator

SECOND: Suave TEE Computation Layer

- Processes authorized bids in a confidential environment
- Manages encrypted bid storage and winner determination
- Ensures fair auction execution
- Provides verifiable computation proofs

Privacy Properties

What Remains Private

- Participant credentials (token balances, NFT ownership, trading history) [ZK Layer]
- Specific authorization criteria met by each participant [ZK Layer]
- Individual bid values [Suave TEE]
- Bid timing and sequence [Suave TEE]

What's Visible to Suave Network

- Transaction sender addresses when submitting compute requests to Kettles
- Kettle interactions (confidential compute requests)
- Request timestamps

What's Partially Private

- While the compute request sender is visible, their underlying identity credentials (KYC, trading history, etc.) remain private through ZK proofs [ZK Layer]
- The relationship between an address and their qualifications remains private [ZK Layer]
- The mapping between bidder addresses and specific bids remains private [Suave TEE]

What's Publicly Verifiable

- Participant eligibility (without revealing why they're eligible) [ZK Layer]
- Auction fairness [Suave TEE]

- Winner determination correctness [Suave TEE]
- Final auction results computation [Suave TEE]

Enhanced Privacy Option

An independent, off-chain ZK verifier layer could be added between the ZKP generation and the transaction submission to Suave. However, it will be important to design for censorship resistance in the verifier network.

Questions for the Community

- Has anyone already integrated ZK with Suave?
- Are there examples of access credentials (ZK or not) for SUAPPs?
- Are there any auctions already deployed into production SUAPPs? Which could benefit from a ZK-based permissioning layer?
- What role should Kettles play in managing changing authorization requirements (e.g., who should maintain and update the SUAPPs with the authorization criteria)?