•Use secure MPC to complete the auction without revealing bids to the auctioneer

Secure and Verifiable Reverse Auction Architecture Using Smart Contracts and zk-SNARKS

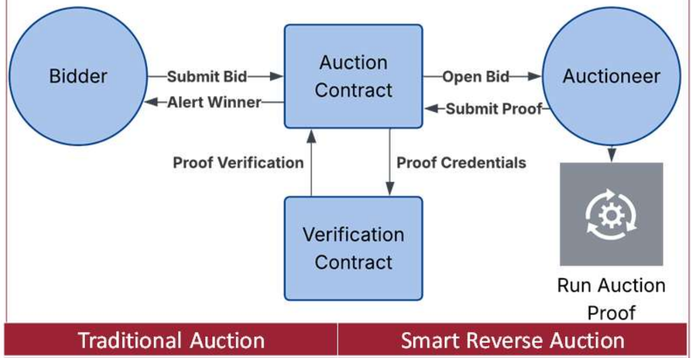
Wade Little

Mentors: Hassan Mahmoud & Dr. Ahmad Alsharif

THE UNIVERSITY OF ALABAMA®

INTRODUCTION

- **What is a Reverse Auction?**
  - In a reverse auction, multiple sellers (or service providers) compete to offer the **lowest bid** for a buyer's request.
- **Objective**
  - This project proposes a **secure, decentralized reverse auction architecture** using commitment schemes, zk-SNARKs, and smart contracts
- **Use Cases**
  - Grid Load Balancing, P2P energy markets, EV Charging Incentives

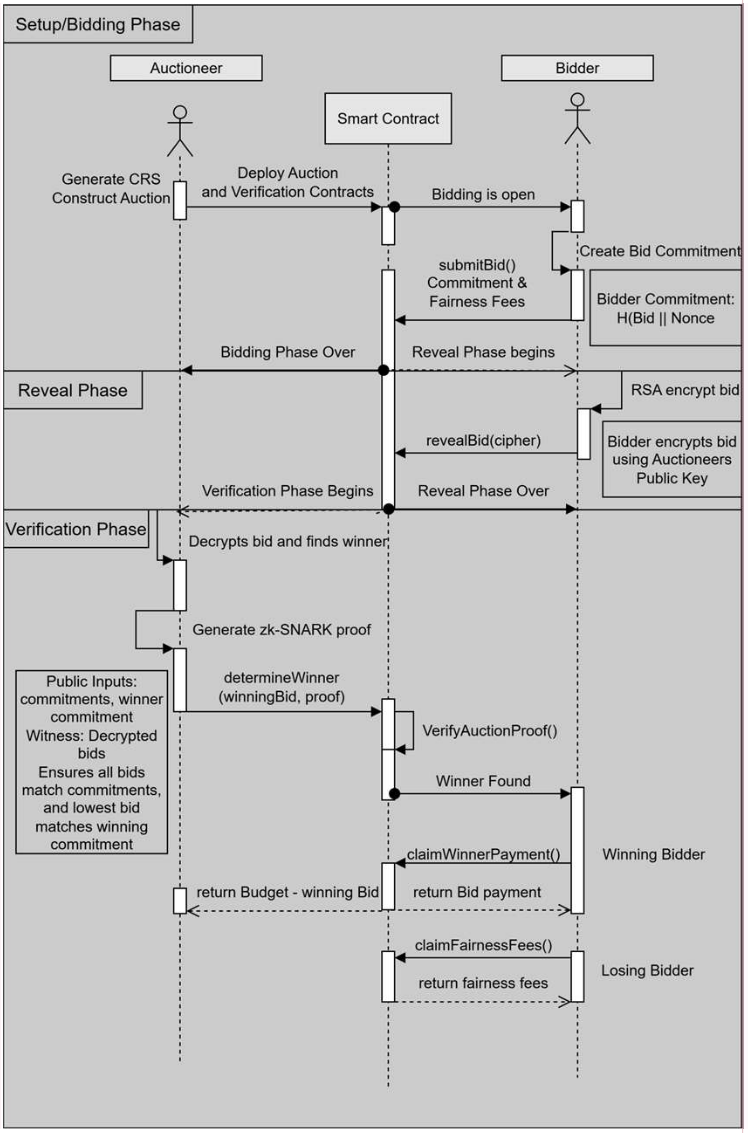


Traditional Auction	Smart Reverse Auction
Requires trusted auctioneer	Trustless via smart contract
Bids are visible	Bids remain private
No proof of correctness	Verifiable via zk-SNARK

TOOLS

- **Commitment schemes:**
  - Conceal bids until the reveal phase
  - Prevent bidders from changing their bids after commitment
- **zk-SNARK**s
  - Prove bid validity and identify the lowest bidder without revealing secret bids
  - Always verify if the prover is honest *(perfect completeness)*
  - Fast and lightweight to verify on-chain *(succinctness)*
- **Smart Contracts**
  - Immutable once deployed – cannot be altered
  - Enforce auction rules without requiring trust
  - Fully transparent – anyone can inspect and verify logic

AUCTION PROCESS



RESULTS

Smart Contract Gas Analysis

Table 1: Cost Breakdown by Role

Role	Price
Auctioneer	$46.60
Bidder	$1.46

Experiment conducted on July 9, 2025 using Remix IDE on a test blockchain. At the time, 1 ETH = $2,500 USD and the median gas price was 3 Gwei.

Function	Transaction Cost	Price
Auction Deployment	2962806	**$22.22**
Verifier Deployment	2375911	**$17.82**
Submit Bid	108320	**$0.81**
Reveal Bid	30862	**$0.23**
Determine Winner	837950	**$6.28**
Claim Payment	55874	**$0.42**
Destroy Contract	36820	**$0.28**

Table 2: Measured gas usage for each key smart contract function (5 bidders)

zk-SNARK Time Analysis

zk-Snark Phase	Time
Setup	4.93 seconds
Proof	2.78 seconds
Verification	0.01 seconds

Table 3: Measured zk-SNARK times (5 bidders)

Malicious Behavior Prevented

- Auction fails verification if the auctioneer excludes any valid bids
- Buyer can reclaim funds if the winner fails to accept payment

CONCLUSION

- Blockchain enables transparent, verifiable transactions without relying on a trusted third party, making it a strong foundation for secure, decentralized auction systems.
- **Future Work**
  - Use secure multi-party computation (MPC) to complete the auction without revealing bids to the auctioneer
  - Extend the system for data exchange using MA-ABE for fair, verifiable access

College of Engineering
Computer Science

College of Engineering
Civil, Construction and Environmental Engineering

ACKNOWLEDGMENTS

This material is based on a study supported by the National Science Foundation under Grant No. 2244371. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, and the U.S. Government assumes no liability for the contents or use thereof.