Scalable Off-Chain Auctions

Achieving $\mathcal{O}(k)$ On-Chain Complexity with Programmable Payment Channels and zkSNARKs

Mohsen Minaei[1] Ranjit Kumaresan[1] Andrew Beams[1] Pedro Moreno-Sanchez[1,2]
Yibin Yang[3] Srinivasan Raghuraman[1,4] Panagiotis Chatzigiannis[1] Mahdi Zamani[1]
Duc V. Le[1]

[1]Visa Research

[2]IMDEA

[3]Georgia Institute of Technology

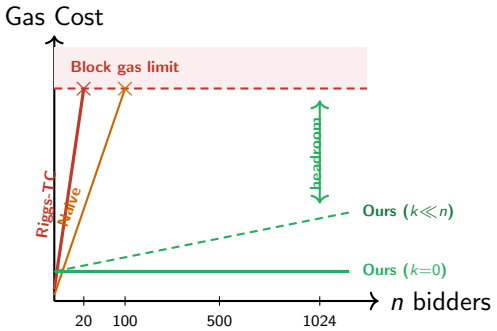
[4]MIT

NDSS 2026

Outline

The Problem: Blockchain Auctions Don't Scale

- **On-chain** ops are expensive (gas fees); **off-chain** ops are essentially free
- Goal: move as much work off-chain as possible
- Existing auctions: $\mathcal{O}(n)$ *on-chain* $\Rightarrow$ cost grows with every bidder
- State-of-the-art (Riggs-TC) hits gas limit at **20 bidders**



Our Result

$\mathcal{O}(1)$ on-chain when honest
$\mathcal{O}(k)$ on-chain when k misbehave
Scales to **1,024+ bidders**

Our Contribution

Key Innovation

First sealed-bid auction protocol supporting **1,000+ bidders**:

- $\mathcal{O}(k)$ on-chain when k bidders misbehave; $\mathcal{O}(1)$ when all honest
- Full bid privacy via zkSNARKs — only winner's bid revealed
- Financial fairness enforced by collateral and covenants

Three Building Blocks:

1. **Programmable Payment Channels (PPC)** — hub-and-spoke, off-chain execution
2. **zkSNARKs** — prove winner without revealing other bids
3. **Covenant Contracts** — penalize misbehavior on-chain

Programmable Payment Channels (PPC)

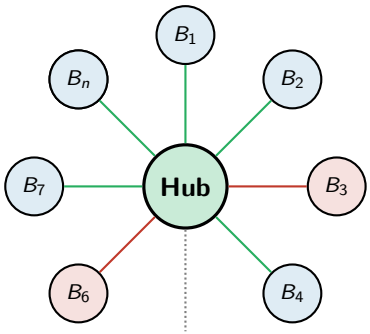
Key Idea: Off-chain conditional IOUs settled on-chain only on dispute

Why PPC (not state channels)?

- State channels: dispute deploys **entire contract**
- PPC: dispute deploys only the **disputed promise**

$\Rightarrow$ Each bid = individual promise; only misbehaving bidder's goes on-chain

On-chain cost $\mathcal{O}(k)$ where k = misbehaving, not $\mathcal{O}(n)$ total



zkSNARKs for Winner Revelation

Challenge: How to prove the winner without revealing all bids?

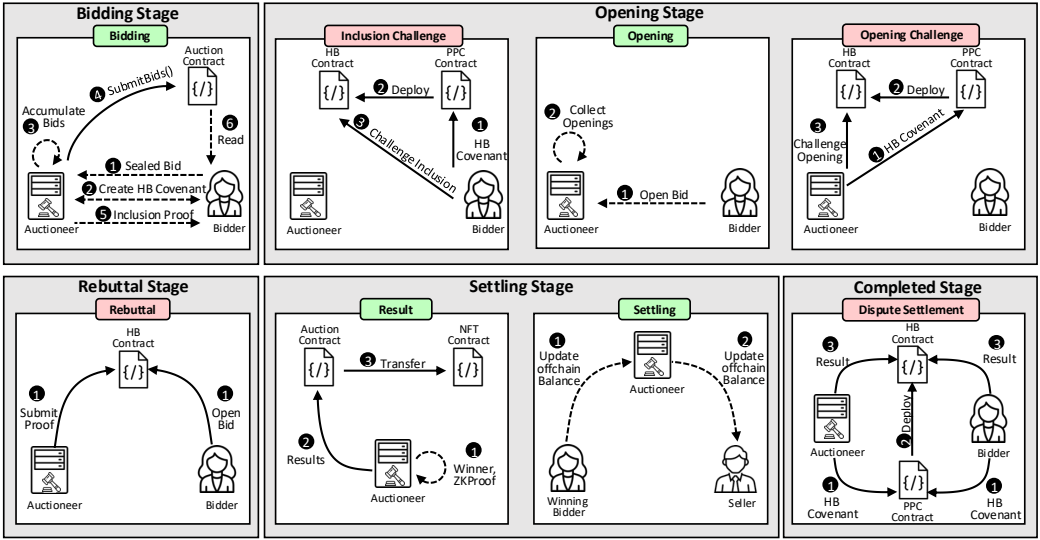
zkSNARK Proof

Hub proves in zero-knowledge:

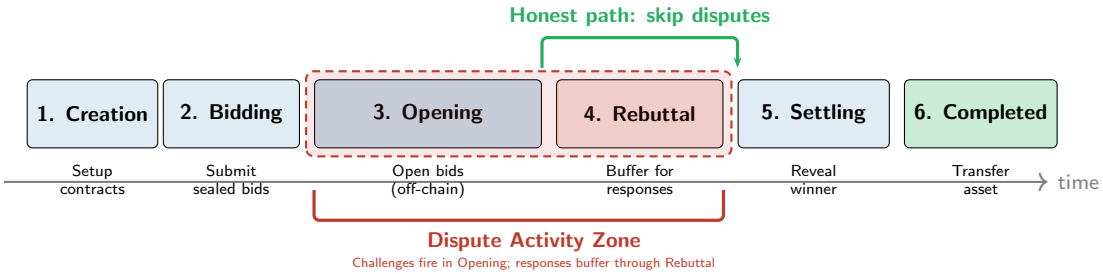
- Winner's bid is in the committed Merkle root
- Winner's bid $\geq$ all other committed bids
- **Without revealing any other bid values**

Result: only the winner's bid is revealed; all losing bids remain private

Protocol Overview



Protocol Stages



Honest: All off-chain $\Rightarrow$ $\mathcal{O}(1)$ on-chain

k **misbehaving:** Disputes span Opening + Rebuttal $\Rightarrow$ $\mathcal{O}(k)$ on-chain

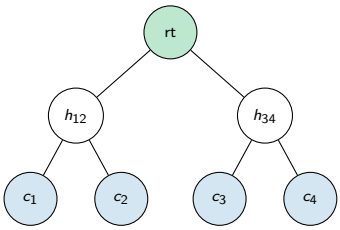
Stage 1–2: Creation and Bidding

Creation: Hub deploys auction contract, locks collateral $\geq n \cdot b_{\max}$

Bidding:

1. Bidder i commits sealed bid $c_i = H(b_i \| r_i)$
2. Hub aggregates all c_i into Merkle tree
3. Hub posts root rt on-chain

Only rt *goes on-chain — individual bids stay off-chain*



Merkle Tree of sealed bids

Stage 3–4: Opening and Rebuttal

Opening (off-chain):

- Bidders reveal (b_i, r_i) to Hub via PPC
- Hub verifies $c_i \stackrel{?}{=} H(b_i \| r_i)$

If misbehavior detected:

- Hub excludes bid $\Rightarrow$ bidder calls `challengeInclusion`
- Bidder refuses to open $\Rightarrow$ hub calls `challengeOpening`
- Challenges can fire **during Opening**

Rebuttal = buffer for responses:

- Parties can respond immediately in Opening **or** wait until Rebuttal
- Guarantees enough time for all on-chain responses

Key Insight

Only k misbehaving bidders trigger on-chain activity $\Rightarrow \mathcal{O}(k)$

Stage 5–6: Settling and Completion

Winner Revelation: Hub generates zkSNARK proof π for:

$$\exists\,(b^*, \text{path}) : \text{Verify}(\text{rt}, b^*, \text{path}) = 1 \ \wedge \ \forall\, b_i \in \text{OpenedBids} : b^* \geq b_i$$

On-chain:

1. Contract verifies proof π
2. Winner's PPC payment finalized
3. Other bidders' channels refunded

Privacy

Only winner's bid revealed; all other bids remain private

Security and Threat Model

Properties:

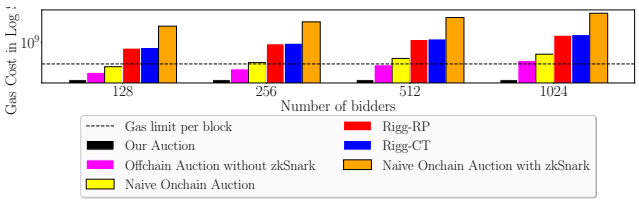
- **Correctness**: highest bidder wins
- **Privacy**: non-winning bids stay hidden
- **Bid Binding**: commitments are irrevocable
- **Financial Fairness**: misbehavior $\Rightarrow$ collateral slashed
- **Liveness**: bounded termination

All properties formally proven via **UC framework** and **game-theoretic analysis**

Adversary: Rational Hub and up to $n-1$ colluding bidders

Scenario	On-Chain	Off-Chain
All honest	$\mathcal{O}(1)$	$\mathcal{O}(n)$
k misbehaving	$\mathcal{O}(k)$	$\mathcal{O}(n)$
Malicious hub	$\mathcal{O}(n)$	$\mathcal{O}(n)$

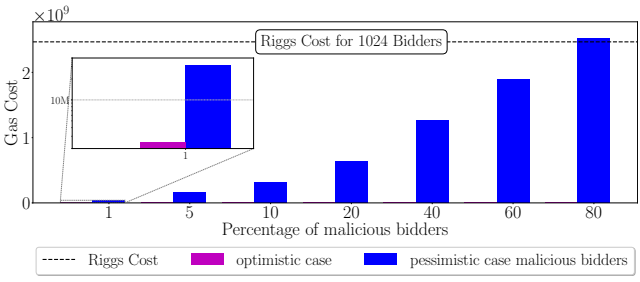
Results: Scalability



- **50× improvement** over Riggs-TC
- Scales to **1,024+ bidders**
- Constant on-chain cost when honest

Riggs-TC bottleneck:
Timelock puzzles require $\mathcal{O}(n)$ on-chain
$\Rightarrow$ gas limit at $\sim$20 bidders

Results: Gas Cost with Malicious Bidders



Honest case:

- Total: ∼2.4M gas (constant in n)

With k malicious bidders:

- $+\sim$100K gas per dispute
- Scales with k, not n

Implementation: Solidity + Groth16 (snarkjs)

Practical Concerns

Trusted setup?

- MPC ceremonies (Zcash, Tornado Cash); can migrate to PLONK/STARKs

Hub censorship?

- Covenant contracts enforce inclusion; hub loses collateral if caught

Is 1,000 bidders enough?

- Enables markets previously impossible on-chain; extensible via hierarchical hubs

Comparison with Related Work

Protocol	**On-chain**	**Privacy**	**Max n**	**Off-chain**
Naive on-chain	$\mathcal{O}(n)$	None	$\sim$100	No
State channels	$\mathcal{O}(n)$	Partial	$\sim$50	Yes
Rollups	$\mathcal{O}(n)$	None	$\sim$500	Partial
Riggs-TC	$\mathcal{O}(n)$	Yes	20	No
Ours	$\mathcal{O}(k)$	Yes	**1024+**	**Yes**

Only protocol achieving $\mathcal{O}(k)$ on-chain complexity with full bid privacy

Summary and Future Work

Contributions

1. First scalable off-chain sealed-bid auction: **1,024+ bidders**
2. $\mathcal{O}(k)$ on-chain cost (k = misbehaving); $\mathcal{O}(1)$ when honest
3. Full bid privacy via zkSNARKs; financial fairness via covenants
4. **50**$\times$ improvement over state-of-the-art

Takeaway

Advanced cryptographic techniques are not always the answer — sometimes the right **architectural decomposition** (isolating each bid as an independent promise) unlocks scalability that pure cryptographic approaches cannot achieve alone.

Future: Multi-item auctions, cross-chain support, PLONK/STARKs migration

Thank you! — Questions?

Backup: Protocol Notation

Symbol	Description
n	Number of bidders
k	Number of misbehaving bidders
b_i	Bid value of bidder i
$c_i = H(b_i \| r_i)$	Sealed bid (commitment)
rt	Merkle root of all sealed bids
π	zkSNARK proof for winner
C_{auction}	Main auction smart contract
C_{covenant}	Covenant enforcement contract