Blockchain: Crypto meets Econ (meets Dist.Comp. meets PL)

Saba Eskandarian (UNC), Yupeng Zhang (TAMU),
Fan Zhang (Duke)
Andrew Miller (UIUC), Elaine Shi (CMU)

Panelists: Muthu Venkitasubramaniam (Georgetown),
Ian Miers (UMD), Kartik Nayak (Duke)

Blockchain: Crypto meets Econ (+ Dist.Comp, + PL)

A trillion-dollar industry has emerged, from the lab to the real world.
This industry has become a proving ground and innovation driver for cryptographic technology, and a focal point for interdisciplinary questions.

Nations are considering how to incorporate blockchain technology into CBDCs.

We remain motivated by the promise to improve financial inclusion, user empowerment, improving transparency in supply chains, governance, and more

We've identified three challenge areas for researchers to tackle?

1. Understanding and mitigating the negative externalities of blockchains
2. Technical challenges in advancing ZKP and MPC for dist. systems at scale
3. Incorporating incentives in distributed systems

Mitigating the negative externalities of blockchains

- Combating the environmental consequences of Proof-of-Work by secure transitioning to Proofs-of-Stake and alternatives. Fair bootstrapping is an obstacle.

- Measurement testbeds to quantify and better understand misuse

- Design and validate user education methods to prevent scams

- Identifying the real obstacles towards realizing the promising positive applications of blockchains?

Providing financial services to the underbanked globally
Spectrum Auctions

- University curriculum. Students are interested, it’s a great conduit for security learning, yet we have a responsibility to discourage overselling it as a panacea

Technical challenges to advance ZKP and MPC at scale

1. Cross-chain payments and swaps via zero-knowledge proofs (ZKP) and secure-multiparty computations (MPC) reveal limitations of our definitions/models

2. Centralization and lack of privacy in Layer 2 solutions are an industry painpoint

3. Space/memory efficiency is the new bottleneck for ZKP and MPC

4. Threshold Signatures have been the first widely adopted MPC application… where are the rest of the applications?

5. Micropayments and fair exchange via zero-knowledge contingent payments

Incorporating incentives in distributed systems

- Identify new attacks and potential defenses. Bribery attacks in particular show a need to consider *external* not just internal source of incentives.

- Mechanism design for transaction fees. Beyond flat fees and block-space auctions, can we assign costs Flat fees are common, others attempting to

- "Miner Extractable Value", or generalized front-running, reveal that assumptions in mechanism design (i.e., an honest auctioneer) should be revisited

- Incentive attacks in applications beyond finance