10/27/26: ORFE seminar, Tim Roughgarden

"The computer in the sky" (i.e., distributed computing and the blockchain)

[SJ: Warning: he has vested interests in the technology, so this is not an ordinary academic talk.]

The original protocol, IP, is not stateful. It's like USPS for your web packets.

What would a "stateful" version of the internet look like, important for financial applications?

A "blockchain protocol" allows for a stateful version of the internet.

The internet becomes a *single* virtual machine, as opposed to a collection of individual physical ones.

See Tim's two papers: "Transaction Fee Mechanism Design" (2023) and "Transaction Fee Mechanism Design for Ethereum Blockchain" (2020). (Tim started working on this topic in 2020, building on his experience with algorithmic game theory and mechanism design theory.)

[SJ: See Tim's Youtube channel for more.]

Transaction = "Alice wants to pay Bob 10 dollars". Trans' are processed in batches ("blocks"). These are only produced so often, and can only be so big. (The "heartbeat" of the blockchain– once every 12 seconds for Ethereum, where a block is 300 transactions. It's often the case that demand-for-transactions exceeds supply; and the *transaction fee mechanism* decides who gets to transact.)

Original mechanism: *first-price auction.* "Alice wants to pay Bob 10 dollars; and is willing to bid 1 dollar to have it processed". ... But who does the 1 dollar go to? Whoever's picking you to transact. Who's that? A randomly selected "validator", a physical machine sampled from the set of all validators.

Sadly, a first-price auction doesn't elicit honest bidding. Consider a second-price auction? Why isn't this trivial? (See Tim's blogpost titled "8 reasons why blockchain mechanism design is hard".)

One reason: this isn't a 5G spectrum auction, where the government is the auctioneer, and is (hopefully) reliable. Here the auctioneer is a random person, is not reliable. [SJ: Ex where the auctioneer meddles with the minimum bid?]

EIP-1559, by Buterin, proposed a fix. *Posted-price mechanism* is just based on a base-fee; "take it or leave it", like Amazon. Only those bids above the base-fee of 10 cents are considered. For EIP-1559, we relax the constraint that a block contains exactly 300 transactions, to requiring that blocks containing . This allows the base-fee to vary by block; if for

The cumulative base-fee doesn't go to the block producer [SJ: auctioneer?]; that could cause *collusion* [SJ: between the block producer and bidders, using off-chain transactions; example?]. Instead, it gets "burned" by the software. [SJ: These are "incentive compatibility" properties?]

[SJ: Tim analyzes only a single block. Noam Nisan paper on "welfare" with persistent bidders", by considering the multi-block ("multi-period") setting?]

[SJ: My Q + follow-up: this leaves open how the ? Reply: the goal is simply to get the right number of "passing" bidders; what happens up to that is up to ? What if the block size is over the apriori maximum of 600, and *everyone* is over the (i.e., the base-fee is set far too low)?]

Tim wrote a report card on EIP-1559 and deduce it's a Pareto improvement over the first-price mechanism. Further, EIP-1559 is on the Pareto frontier of IC properties [SJ: ?] of possible mechanisms. This report card and related results presumably played a role in the adoption of EIP-1559, which is a rare event among EIPs.

Next topic: consensus protocol. (Joint work with a mathematician from LSE and an economist from Chicago.)

Goals of consensus: "consistency" and "liveness".

[SJ: Related to Lamport's algorithm that Shyam was telling me about? Byzantine generals from the 80s, if attacker's "stake" is bounded by $\rho < 1/3$, attacks are impossible with a well-designed protocol, hence there will be no consistency violation.]

Permissionless consensus.

The promise of proof-of-stake (versus proof-of-work). [SJ: ?]

Q: can a blockchain protocol "fight back" against certain kinds of attacks, *programmatically?*

Specific attack: hashrate. An adversary trying to convince two different (physical) machines that you're two different people? [SJ: ?]

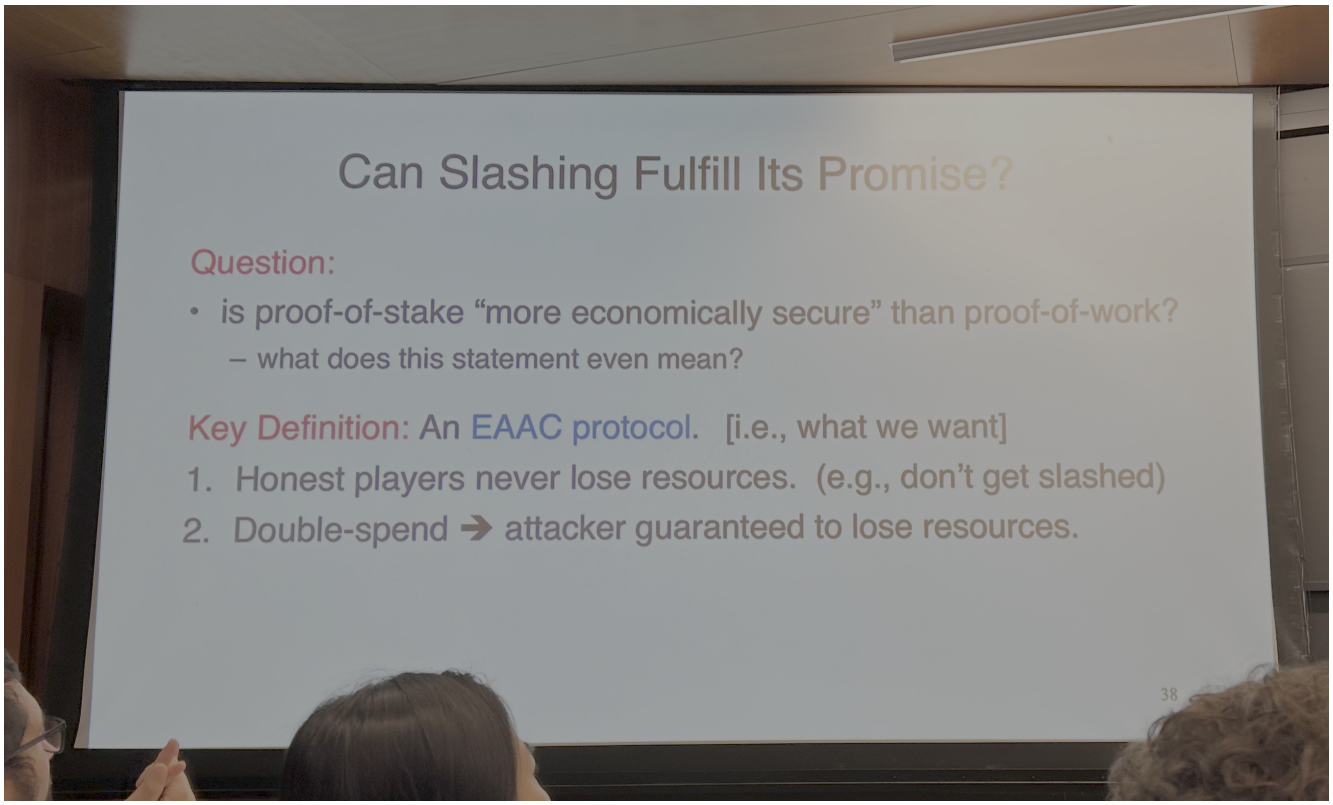


Figure 11: Enter Caption

Positive result, existence of EAAC mechanisms:

Thm: there is an EAAC protocol in the *quasi-permissionless* and *synchronous* setting with an ρ-bounded attacker for $\rho < 2/3$.

Phase transition in ρ, where ρ quantifies the attacker's control over the protocol. [SJ: What does this mean?] For $\rho < 1/3$, this is classical; and for $\rho < 2/3$, you can *punish* by revoking stake, so that the protocol remains "secure". [SJ: "Provable 'slashing' properties".]

Tim then got an email from the Fed Board's payment research team, whose members all read his paper. They were trying to do a risk assessment on the event that financial companies all adopted crypto.

Automated market-making and LVR.

[SJ: Computer is about to die, see Simons slides.]