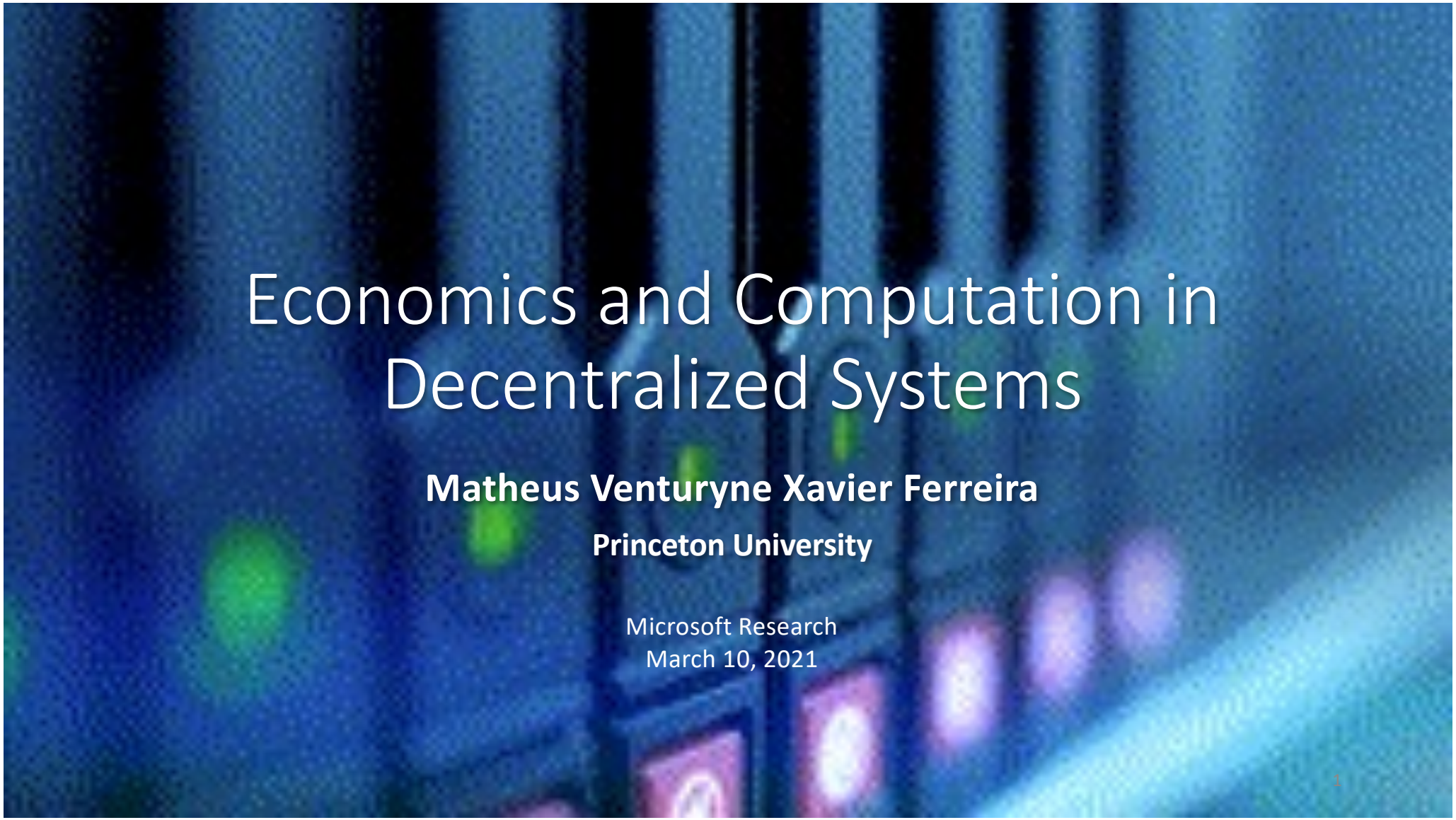


Economics and Computation in Decentralized Systems

Matheus Venturyne Xavier Ferreira

Princeton University

Microsoft Research
March 10, 2021

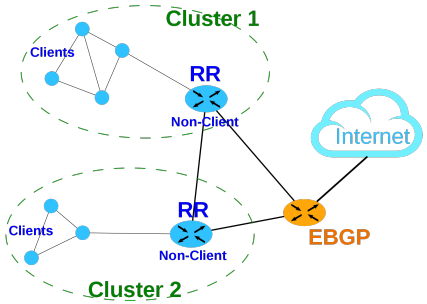
Economics and Computation

- Many computer science applications require economic reasoning

Source: Public Auction Finder

Online Markets

- Auctions: eBay.
- Sharing economy: Uber, Lift, Airbnb.
- Advertisement: Bing, Google, Facebook.



Internet routing

- Network formation: BGP.
- Congestion games.

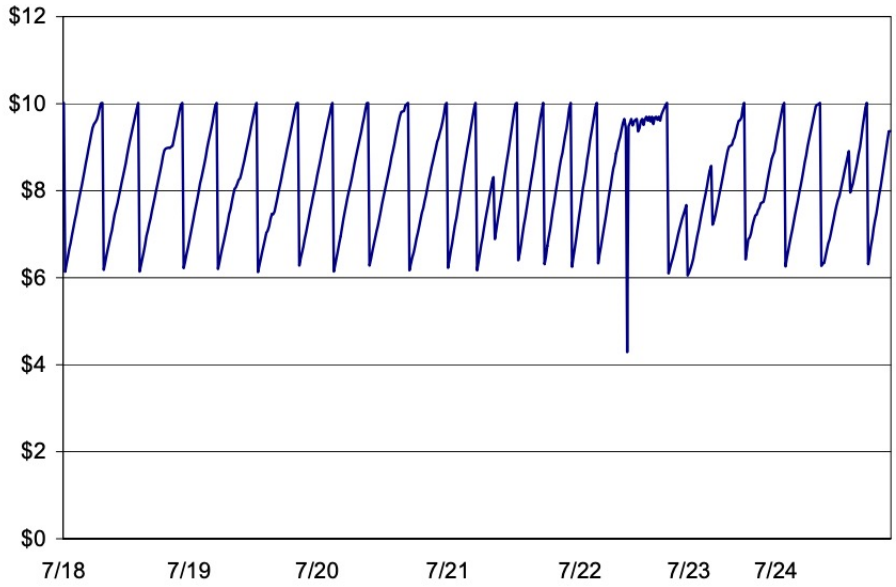
Source: Equity Trust

Blockchains

- Cryptocurrencies: Bitcoin, Ethereum.
- Decentralized applications in finance, healthcare, supply-chain, …

Early days of sponsored search

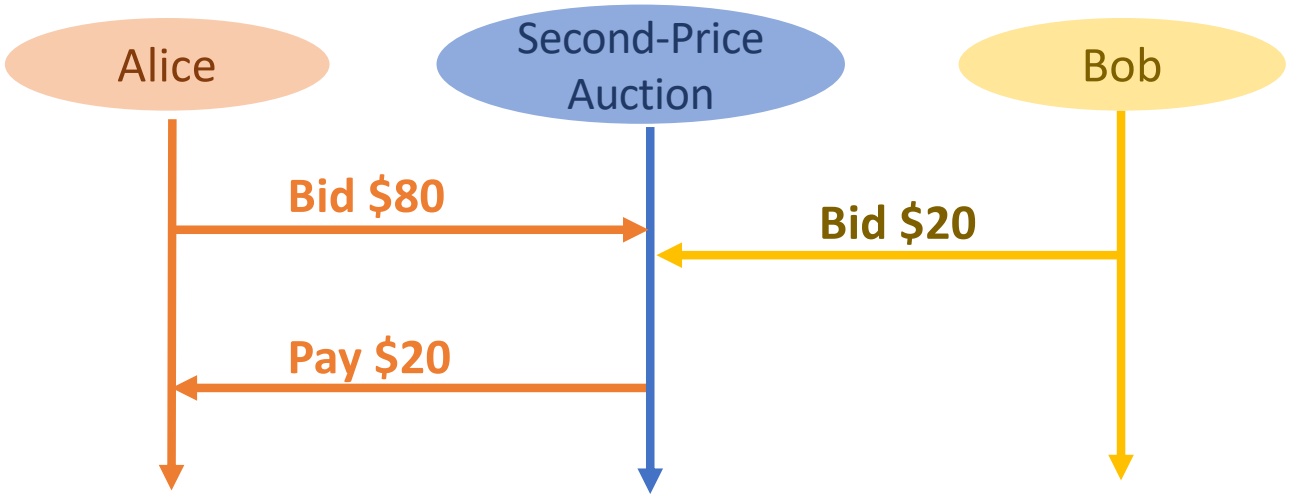
- Strategic bidding caused instability in first-price auctions.



Instability in Overture auctions [Edelman, Ostrovsky '07]

The Internet popularized second-price auctions

- [Vickrey ‘61] Second-price auctions.
  - Auctioneer collects bids privately.
  - Winner pays the second highest bid.



Vickrey. Awarded the ‘96 Nobel prize in economics.

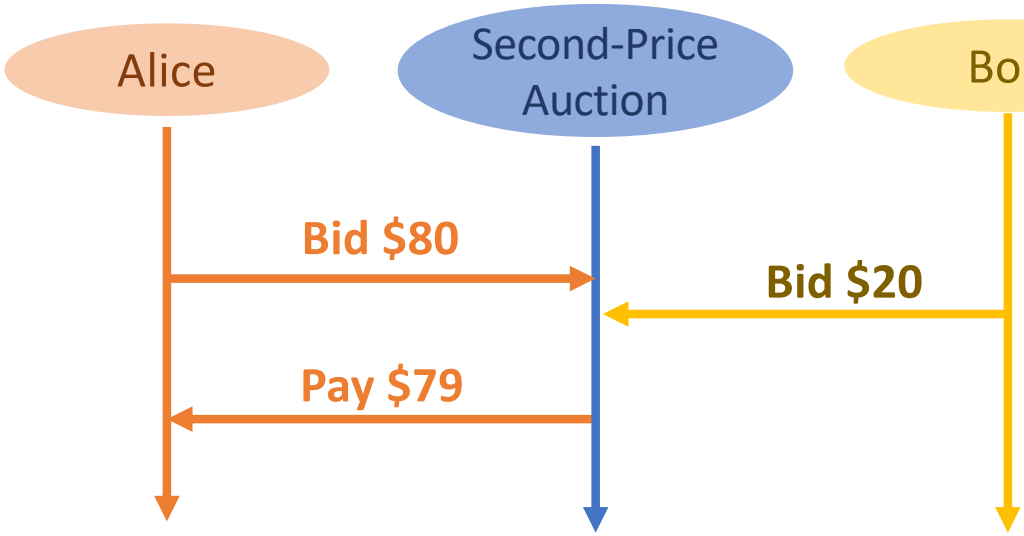
The return of first-price auctions

Google Switches To First-Price Auction

Date: March 6th, 2019

What went wrong???

Algorithm designer as an adversary



The New York Times

F.B.I. Opens Investigation of EBay Bids

Suspicion of Shills Rises as Web Auctions Grow

By JUDITH H. DOBRZYNSKI

ARTnews Est. 1902

Legislators Seek to Stop 'Chandelier Bidding' at Auction

BY *Daniel Grant* ORIGINALLY PUBLISHED 09/04/07

The Register®

Business ▸ Policy

eBay jewellery store fined $400,000 for shill bidding

eBay reports offender to authorities

By Lester Haines 11 Jun 2007 at 11:17 18 SHARE ▼

Desire for transparency is a universal concern

- Blockchains enable decentralization and overcome market barrier.
  - Removal of intermediaries.
  - Diverse application domain: healthcare, supply chain, finance, e-commerce, …

Microsoft Industry Blogs

Bühler will track crops from farm to fork using blockchain technology

Çağlayan Arkan, September, ‘18

SCM SUPPLY CHAIN MOVEMENT

Trends | Thursday | 23 August 2018 | 17:02h

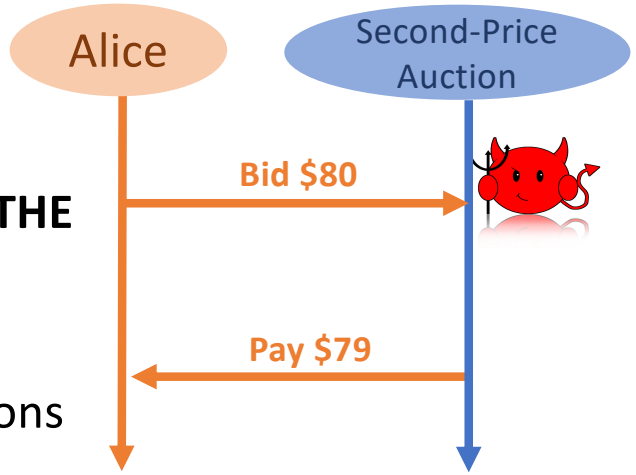
Nestlé trials blockchain to improve food-ingredient supply chain transparency

Research Question

- How can we design algorithms when the **algorithm designer is an economically driven adversary?**
- To instantiate this agenda:
  - Credible auctions.
  - Incentive compatible energy-efficient blockchains.

Credible Auctions

- **Desiderata:**
  - Incentive compatible for bidders.
  - Incentive compatible for the auctioneer (Credible).
  - Revenue optimal
- [Akbarpour and Li '20] The **ascending price auction IS THE UNIQUE** auction that satisfy all this properties.
  - **BUT** the communication complexity is **unbounded**!
- **Main Question.** Can we introduce additional assumptions to circumvent their impossibility?



Credible, Truthful, Two-Round Optimal Auctions via Cryptographic commitments [FW ‘20]

Matt Weinberg

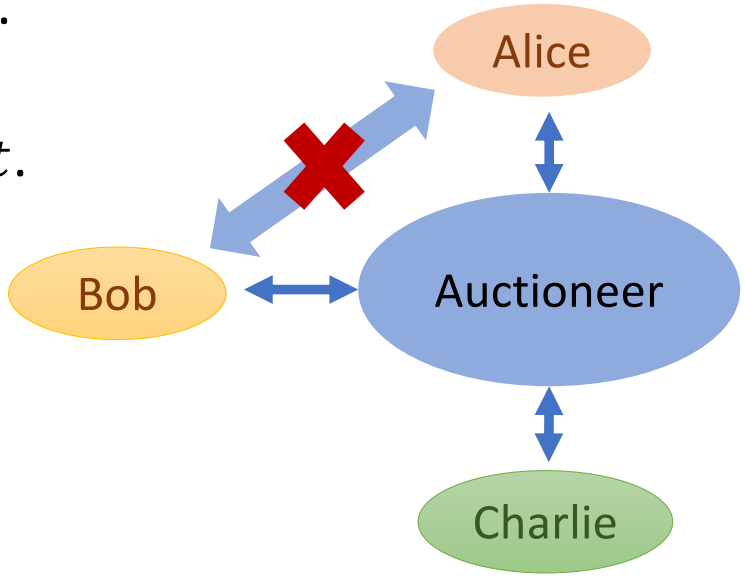
PRINCETON UNIVERSITY

- Under standard cryptographic assumptions, there is an auction that is:
  - Incentive compatible for bidders.
  - Incentive compatible for the auctioneer (Credible).
  - Revenue optimal.
  - **AND** requires only **two rounds** of communication.

Model

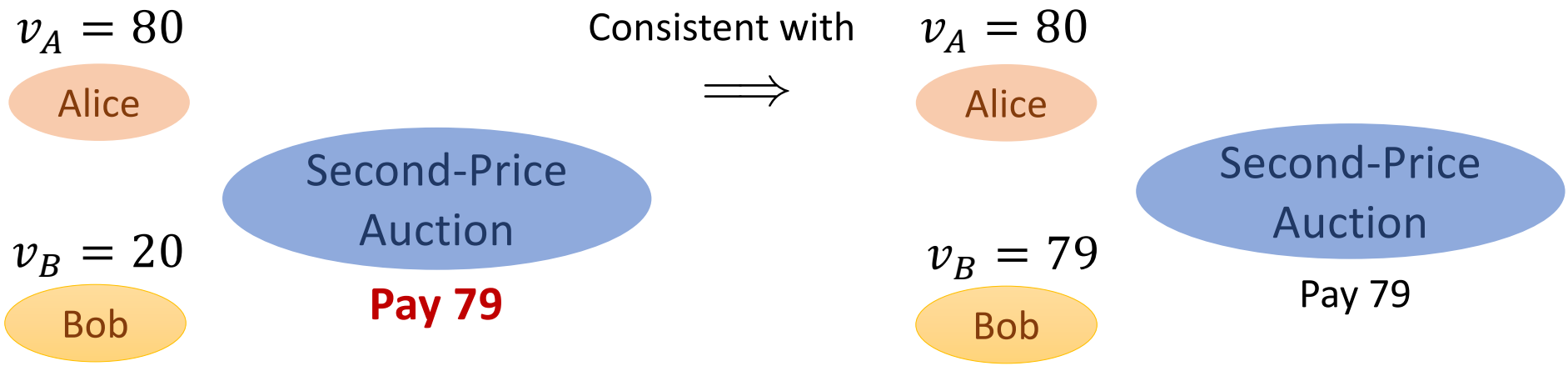
- Single item, n bidders with private values drawn i.i.d. from public distribution D.
  - Can be generalized for non i.i.d. values.
- Quasilinear utility: $value - payment$.

1) **Private communication between auctioneer and bidders.**
   - No communication among bidders.
2) **Voluntary Participation.**
   - Bidders can abort at any point in time.



Safe Deviations [Akbarpour and Li '20]

- The auctioneer publicly **"promises"** to implement an auction format.
- A deviation from the promised auction is safe if for all bidders, the outcome of the auction is **always** consistent with some realization of the auction.



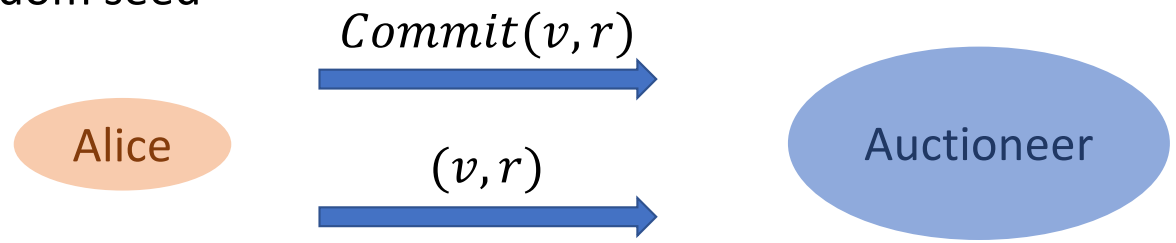
Credible Auction

- No **safe deviation** from the promised auction yields more revenue than implementing the promised auction in earnest.

Deferred Revelation Auction (DRA)

Cryptographic Commitments

r : random seed

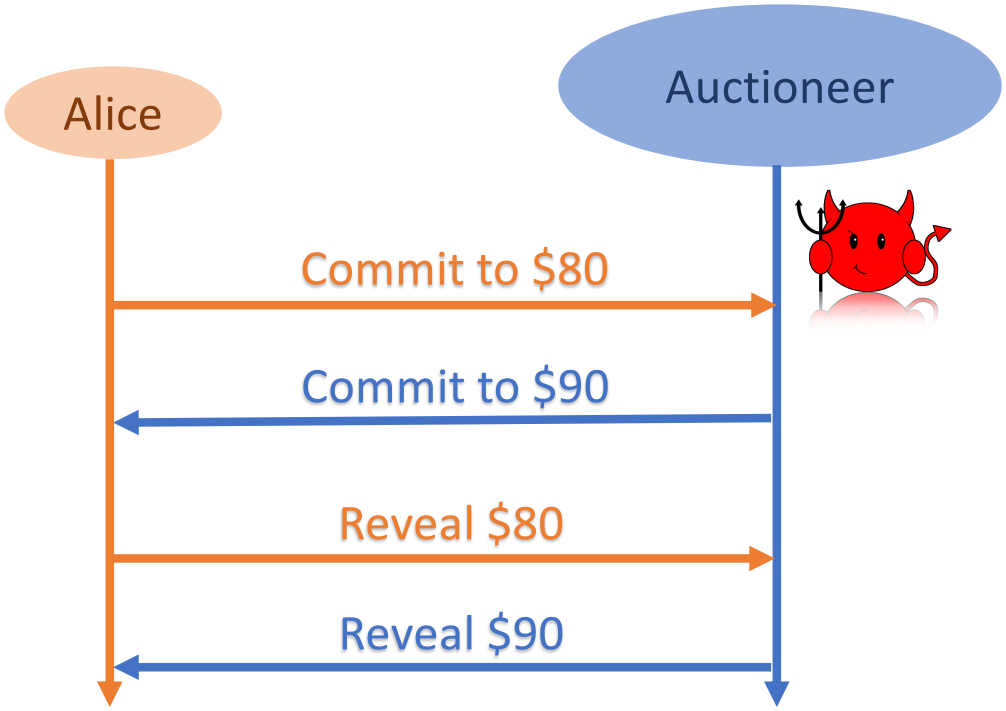


- **Perfectly Hiding**: auctioneer learns nothing about the bid by only observing the commitment.
- **Computationally Binding**: ''hard'' for the sender to find pairs $(v', r') \neq (v, r)$ that open the same commitment: $Commit(v', r') = Commit(v, r)$.

First Attempt

Commit to bids $\Longrightarrow$ Broadcast commitments $\Longrightarrow$ Reveal bids

$\Longrightarrow$ **Second-price auction with optimal reserve $r(D)$** [Myerson, '81]

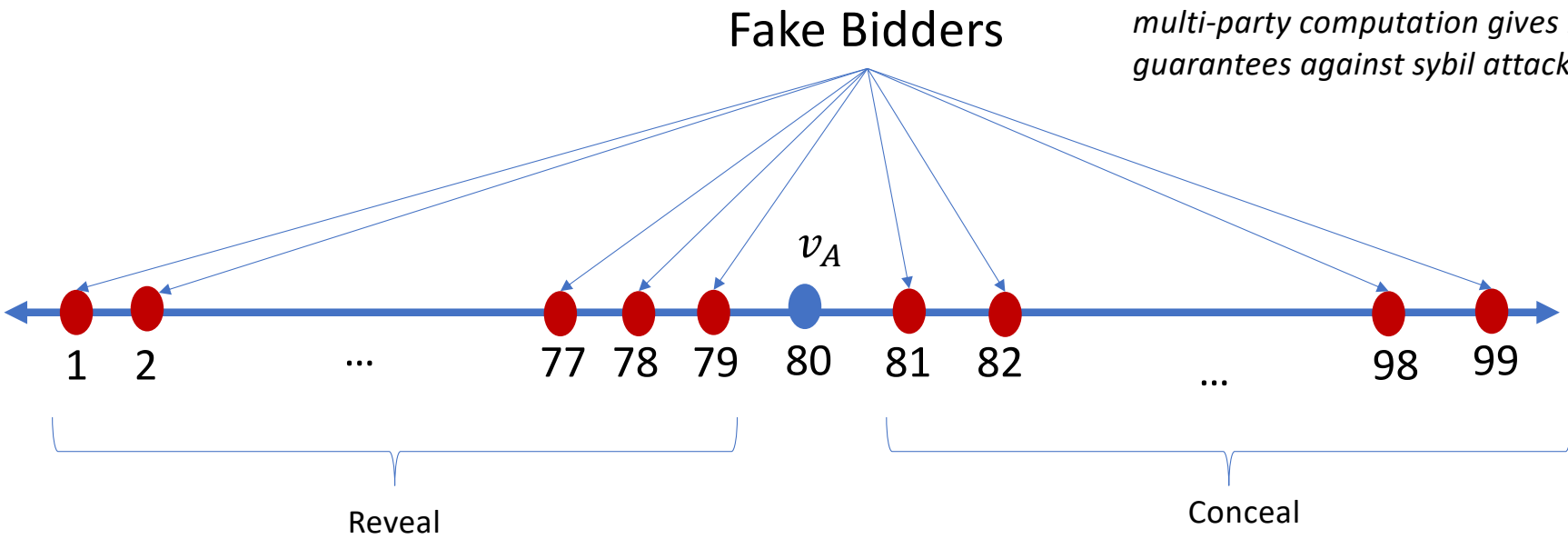


Myerson. Awarded the '07 Nobel prize in economics

Sybil Attack

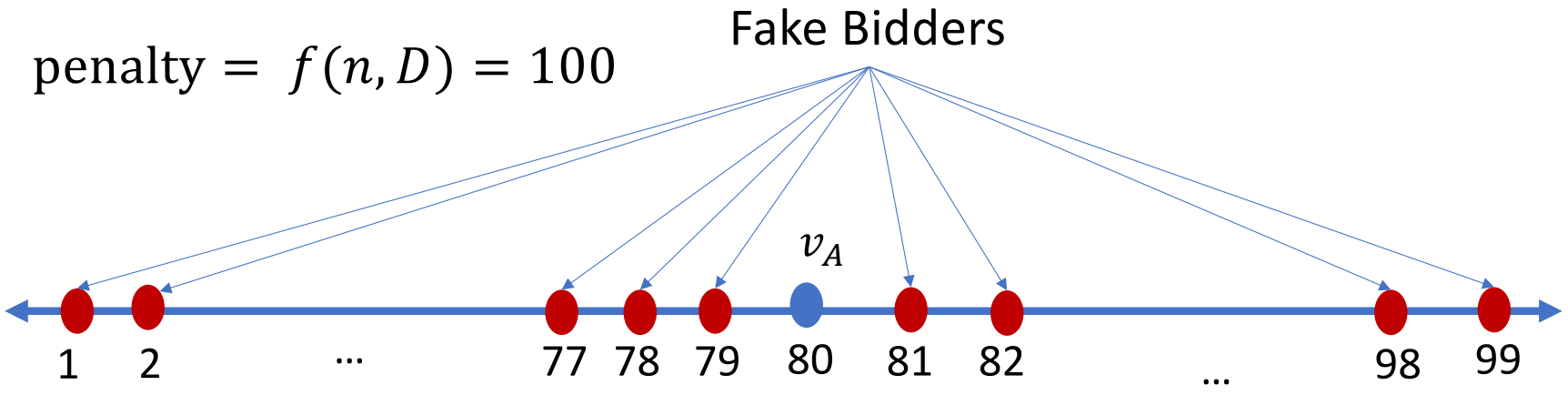
- There is no cost to submit fake bids.
- **AND** there is no cost for aborting fake bidders.

***Remark**: off-the-shelf secure multi-party computation gives no guarantees against sybil attacks.*



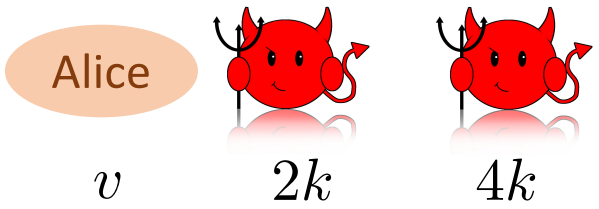
One new idea

- Same as before **BUT** *a*ny bidder that aborts pays penalty $f(n, D)$ to the ***WINNER!***



A sufficiently large penalty might not exist

- Single bidder from distribution: $\Pr[v > p] = \frac{1}{p}$
  - For all $p \geq 1$, the revenue is $p \cdot \Pr[v > p] = 1$.

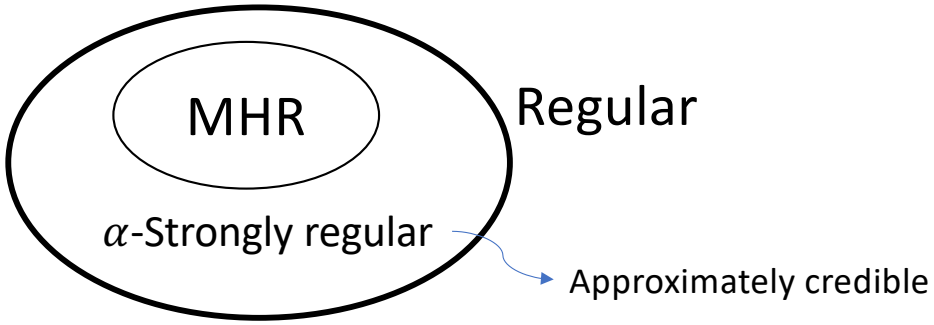


- Submit two fake bids $2k, 4k$ where $k = f(3, D)$.
- When $v < 2k$: reveal all bids.
- When $v \in [2k, 4k)$: conceal $4k$.
- When $v > 4k$: reveal all bids.

$$E[Revenue] = \underbrace{0 \cdot \Pr[v < 2k]}_{0} + \underbrace{(2k - k) \cdot \Pr[2k \leq v < 4k]}_{> 0} + \underbrace{4k \cdot \Pr[v \geq 4k]}_{= 1}$$

Main results

- **MHR Distributions:**
  - DRA **IS** Credible when penalties $f(n, D) \geq r(D)$. (optimal reserve price)
- **Regular Distributions:**
  - DRA **IS NOT** always credible.
    - There is a distribution where the optimal auction has revenue 1.
    - **YET**, for any penalty $f(n, D)$, the auctioneer can extract ∞ revenue.

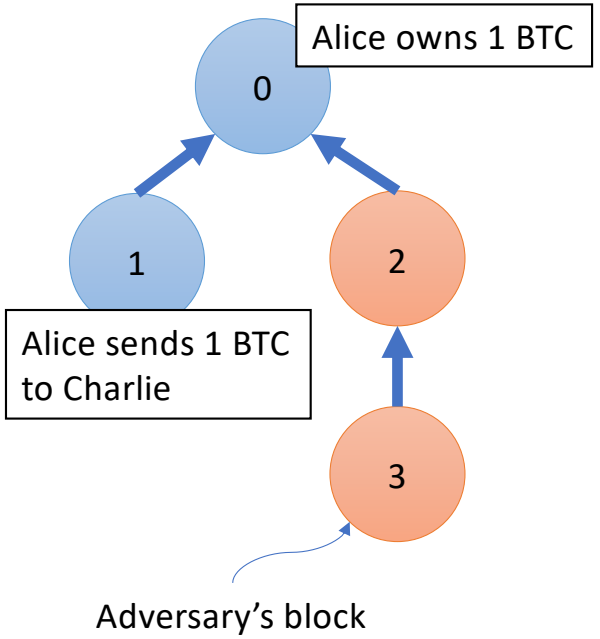


Outline

1. Communication-efficient credible auctions.
2. **Incentive compatible energy-efficient blockchains.**
3. Conclusion.

Blockchains are algorithms

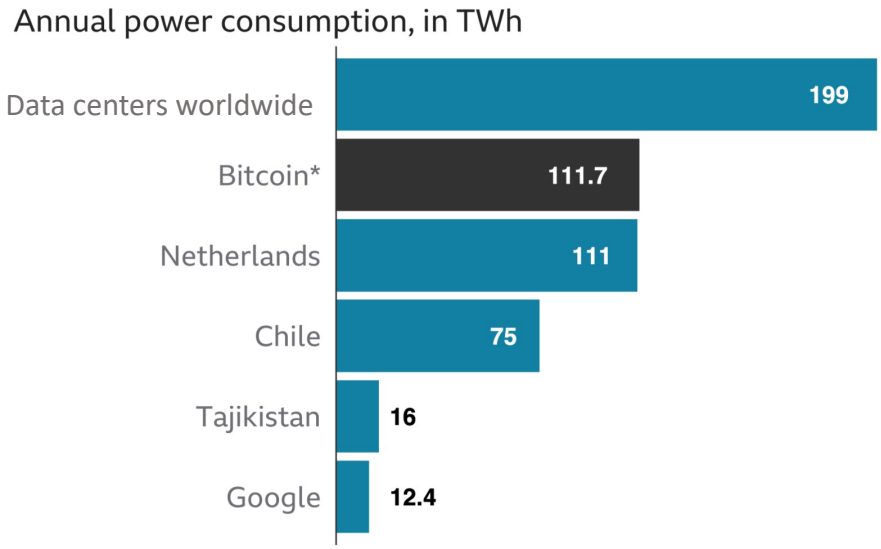
- **Users**
  - Submit transactions.
- **Miners (implement the blockchain protocol)**
  - Create blocks.
  - Each block stores at most m transactions.
- **Tournament**: Each time step t, one miner is chosen **randomly** to create block t.
  - Receives new coins as reward.
- **Honest strategy**: create block t pointing to the **longest chain** and **broadcast** at time t.
- **Miner's utility**: their fraction of blocks in the longest path.



$$\liminf_{T \to \infty} \frac{\#\ Blocks\ of\ strategic\ miner\ in\ the\ longest\ path\ at\ time\ T}{Height\ of\ the\ longest\ path\ at\ time\ T}$$

Environmental cost of Bitcoin

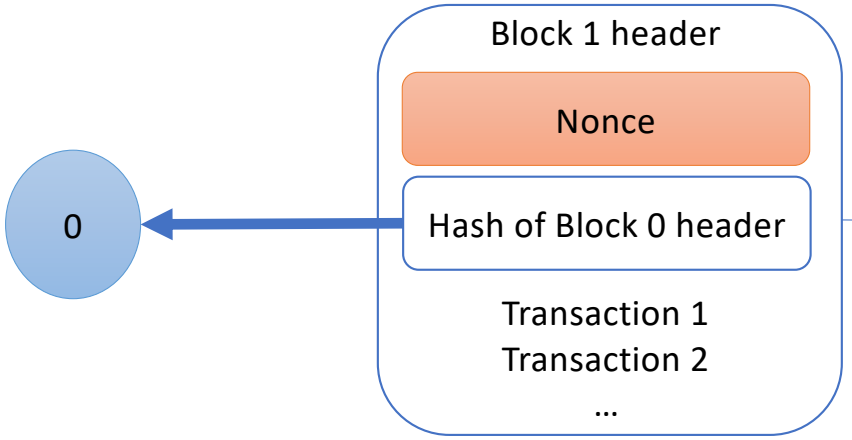
- Bitcoin's consensus algorithm is based on proof-of-work.
  - Energy intensive yet can only process 7 transactions per second.



Source: BBC News. January 2021.

Beyond Proof-of-Work

- Proof-of-work (PoW) requires miners to **compete** to solve a crypto puzzles:



Random oracle model.
For all $x \in \{0,1\}^n$,
$Hash(x) \sim Unif(0, 1, \ldots, 2^{256} - 1)$

$Hash(\ Block\ 1\ ) < 2^{190}$

- Proof-of-stake (PoS) is an energy friendly alternative.
  - **Tournament**: sample a uniformly random coin.

Nash equilibrium

- **Honest mining** is a **Nash equilibrium** if all miners prefer to play honest mining given all other miners are playing honest mining.
- **Desiderata:** under which conditions is honest mining a Nash equilibrium?
- [Brown-Cohen, Narayanan, Psomas, Weinberg '18] gave a **formal barrier**. For any longest-chain protocols, **IF**
  - Mining is computationally efficient.
  - All source of pseudo-randomness comes from the blockchain itself.

  THEN, Honest mining is **NEVER** a Nash equilibrium.
- **Main Question:** Can we introduce additional assumptions to circumvent their impossibility result?

Proof-of-Stake mining games with perfect randomness [FW ‘21]

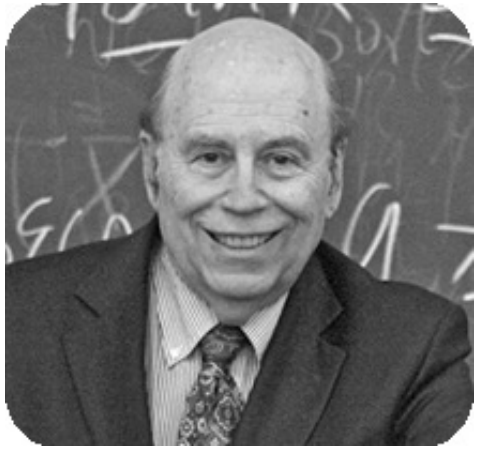
Matt Weinberg

PRINCETON UNIVERSITY

- There is a PoS protocol with access to **random beacon** where honest mining **IS** a **Nash equilibrium** when no miner owns more than 30.8% of the currency.
  - **BUT** Honest mining **IS NOT** a **Nash equilibrium** if some miner owns more than 32.7% of the currency.

Trusted randomness in theory

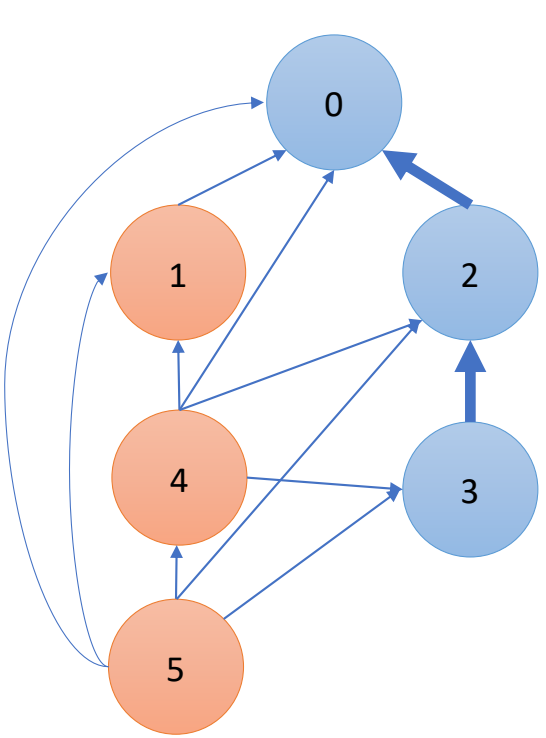
- **Random beacons** almost equivalent to **common random string (CRS)** from cryptography.
  - Except chunks of random bits are revelated in discrete time steps.
  - Transaction Protection by Beacons [Michal O. Rabin '83].
- Trusted randomness allow us to do the impossible:
  - Non-interactive zero-knowledge proofs.
  - Universally composable commitments.
  - **Incentive compatible energy-efficient blockchains.**



Rabin. Awarded the '76 Turing award.

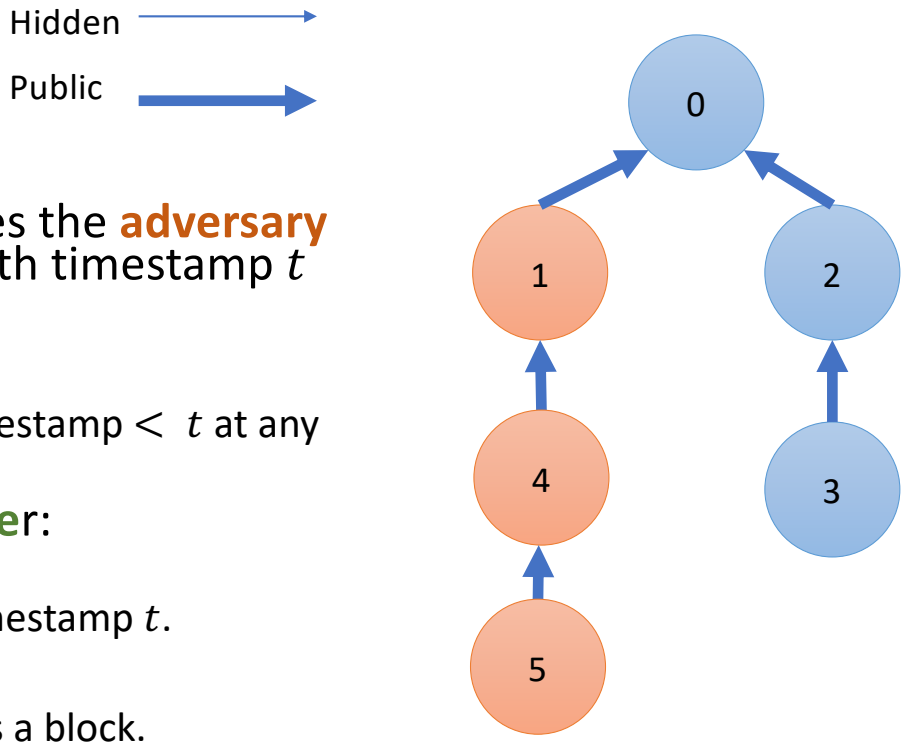
Model: PoS with random beacon

- W.l.o.g. to consider two player game:
  - **Adversary** owns α fraction of currency.
  - **Everyone else** follows the honest strategy.
- Each time step t, the **random beacon** gives the **adversary** the privilege to create a **"single"** block with timestamp t with probability α.
- What the **adversary** can do:
  - Publish block t pointing to any block with timestamp $<$ t at any time $\geq t$.
- What **is allowed** for the **algorithm designer**:
  - Punish detectable dishonest behavior.
  - Example: publish two or more blocks with timestamp t.
- We do not assume latency is bounded:
  - Hence, we cannot punish someone that hides a block.

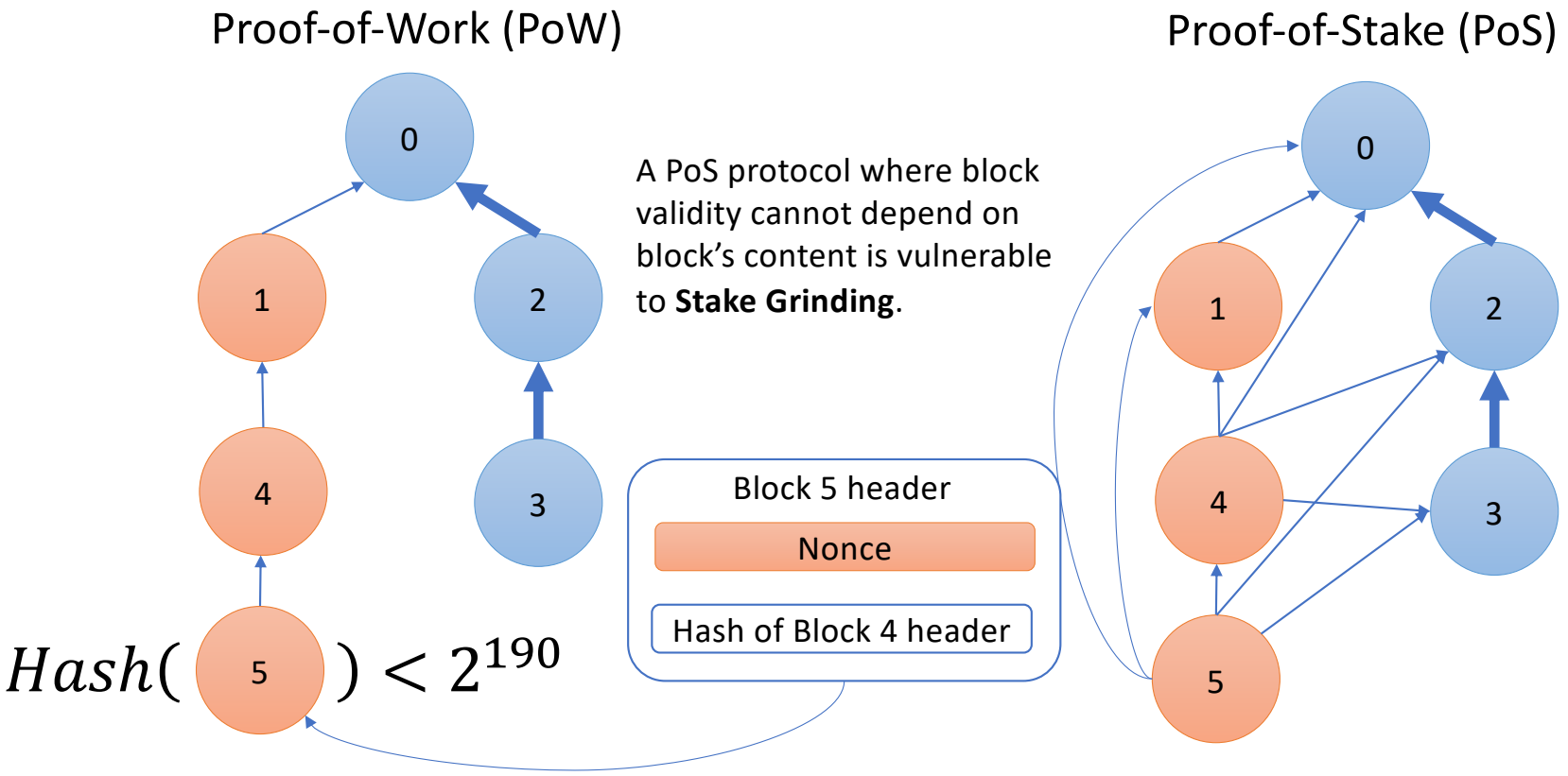


Model: PoS with random beacon

- W.l.o.g. to consider two player game:
  - **Adversary** owns α fraction of currency.
  - **Everyone else** follows the honest strategy.
- Each time step t, the **random beacon** gives the **adversary** the privilege to create a **"single"** block with timestamp t with probability α.
- What the **adversary** can do:
  - Publish block t pointing to any block with timestamp $< t$ at any time $\geq t$.
- What **is allowed** for the **algorithm designer**:
  - Punish detectable dishonest behavior.
  - Example: publish two or more blocks with timestamp t.
- We do not assume latency is bounded:
  - Hence, we cannot punish someone that hides a block.

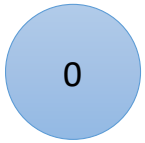


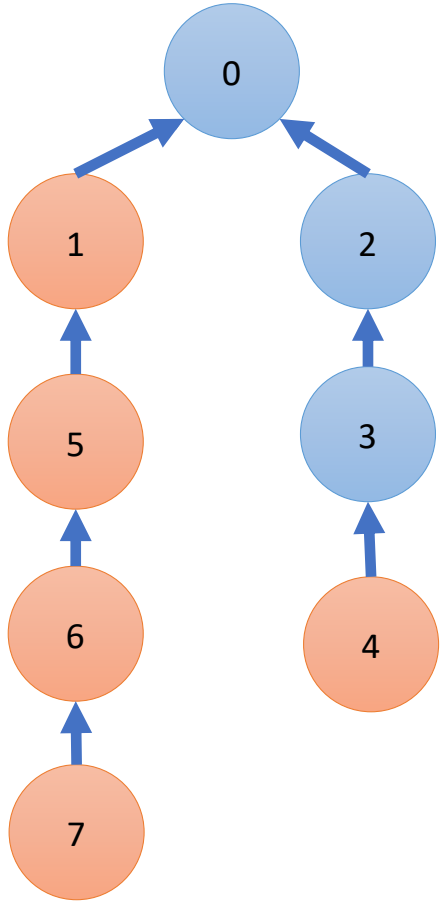
PoW games are a special case of PoS games



Markov decision process

- At time $t = 0$, the game is at **initial state**:

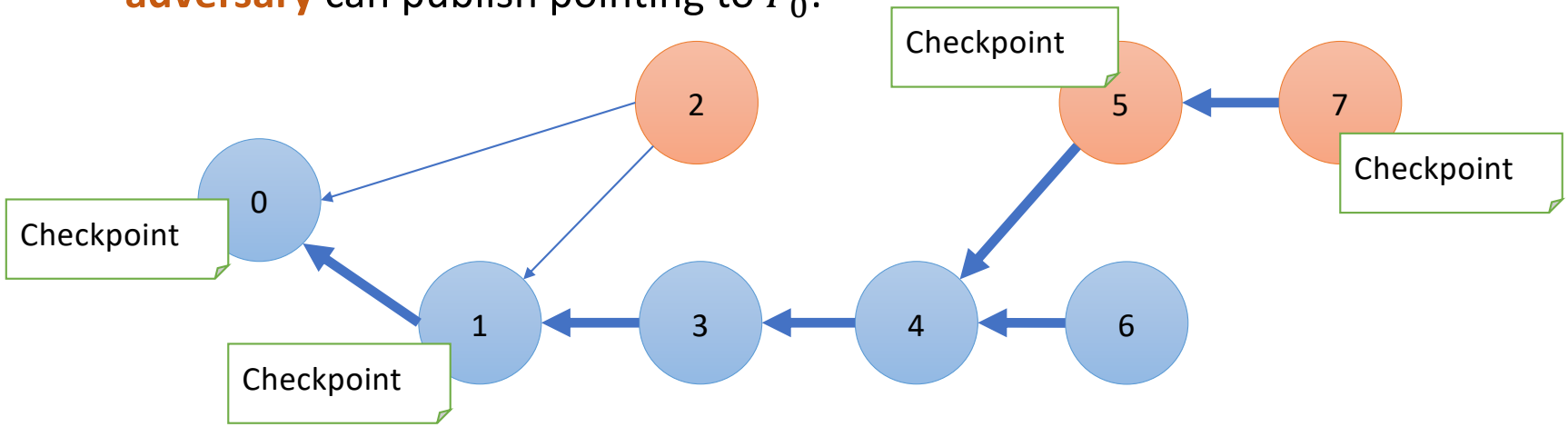




- Let $\tau \geq 1$, be the first-time step the Markov process returns to the initial state.
- **Example**: Suppose block 4 is never forked, then the adversary treats block 4 as block 0.
- **Highly complex** action space and state space.
  - Will a strategic miner ever forget part of the state?
- **There is a hidden structure in this Markov process.**

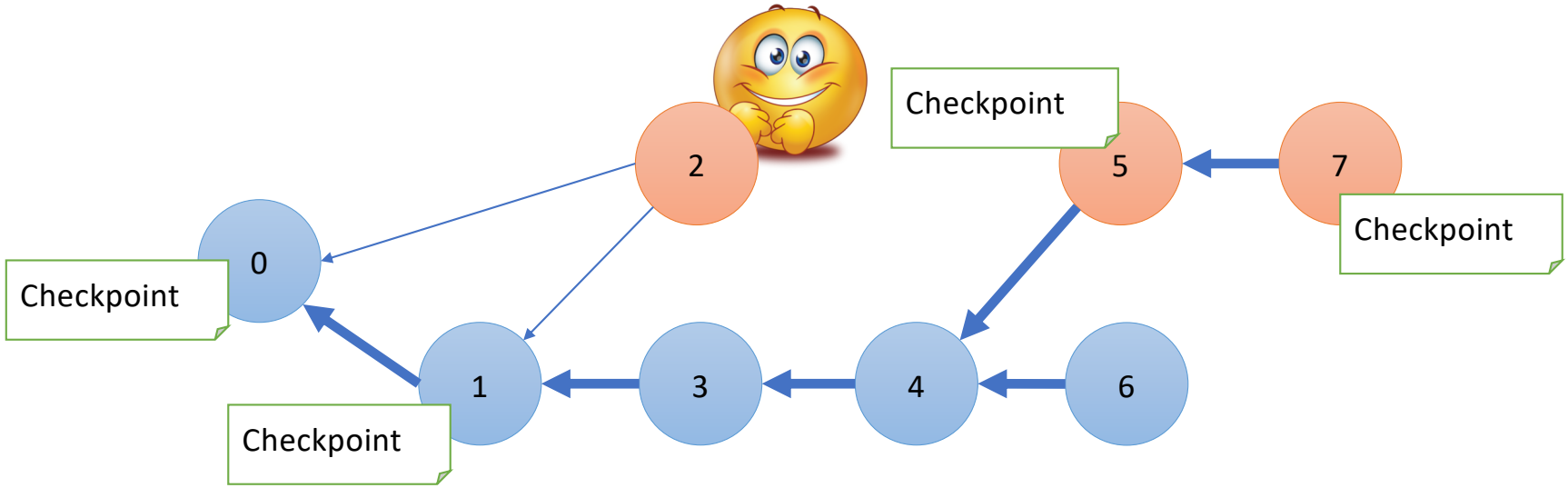
Checkpoints

- Sequence of blocks $P_0, P_1, P_2, \ldots$ in the **longest path**.
  - Block 0 is P_0.
  - P_1 is the first block $v > P_0$ (in the **longest path**) such # **adversary's** blocks in the path from P_0 to v is at least # blocks with timestamp at most v the **adversary** can publish pointing to P_0.



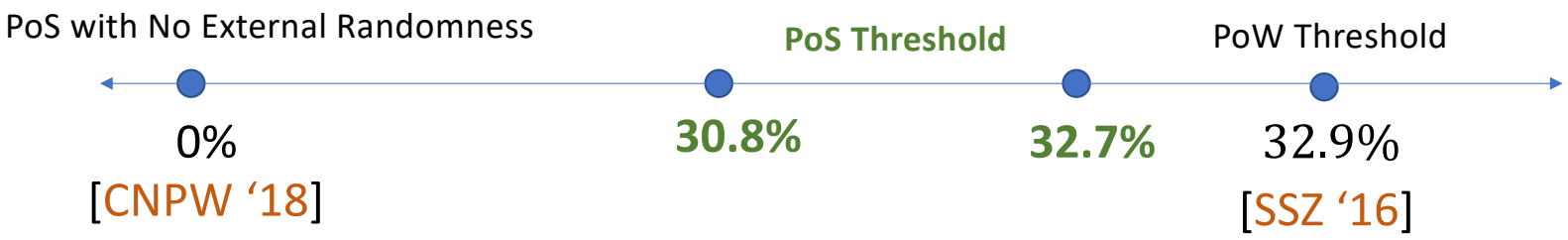
Strong Recurrence

- [**Theorem**] There is an optimal strategy that returns to the **initial state** whenever a new **checkpoint** is defined and $\mathrm{E}[\tau] < \infty$.
  - Random variable $\tau \geq 1$ denotes the time step checkpoint P_1 is defined.



Main results

- Honest mining **IS** a **Nash equilibrium** if all miners own at most 30.8% of currency.
- Honest mining **IS NOT** a **Nash equilibrium** if some miner owns more than 32.7% of the currency.



Outline

1. Communication efficient credible auctions.
2. Incentive compatible energy-efficient blockchains.
3. **Conclusions.**

Conclusions

- In many practical instances, the algorithm designer is an economically driven adversary.
  - Efficiency (i.e., communication, computation, storage) is a recurrent barrier to transparent algorithm design.
- In this talk:
  - Communication efficient credible auctions.
  - Incentive compatible energy-efficient blockchains.
- **Connections between credible algorithm design and blockchains.**
- Future work.

How to allocate resources in Blockchains?

- [Nakamoto ‘08] In Bitcoin, transactions compete in a first-price auction.
  - Miner that creates the block receives all the auction revenue.

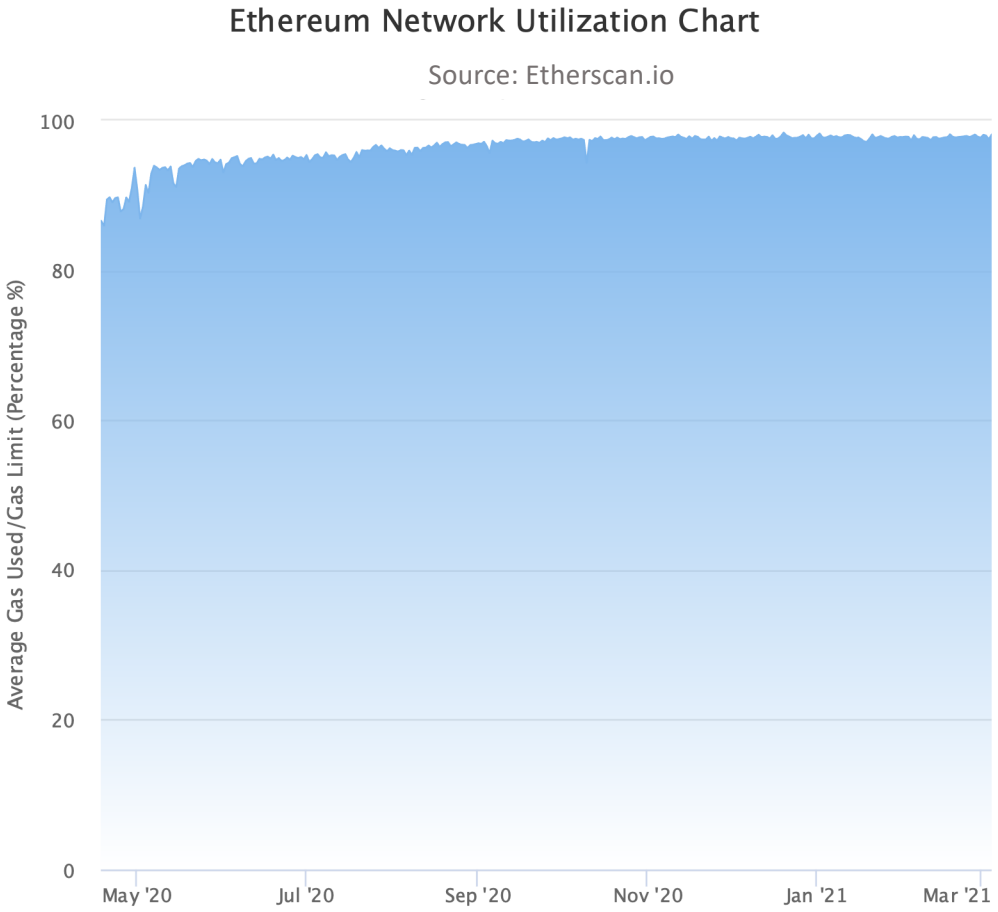
Nasdaq

Ethereum Miners Earned Record $830M in January

CONTRIBUTOR
William Foxley — CoinDesk

PUBLISHED
FEB 2, 2021 11:15AM EST

- ❑ More than $300M of revenue came from transaction fee auctions.



Alternative transaction auctions

- First-price provide bad user experience [Edelman, Ostrovsky '07].
  - If you bid too low, your transaction will take days for confirmation.
  - If you bid too high, you pay more than was necessary.
- Why not use a second-price auction [Vickrey '61]?
  - Miners cannot commit to implement any auction format.
  - **Credibility is essential!!!**
- Why not use the **deferred revelation auction** [FW '20]?
  - Has communication complexity **# bidders** (not the **# items**).

Dynamic Posted-Pricing as Blockchain Transaction Fee Mechanism [FMPS '21]

Daniel Moroz

HARVARD UNIVERSITY

David C. Parkes

HARVARD UNIVERSITY

Mitchel Stern

Berkeley UNIVERSITY OF CALIFORNIA

- **Efficiency** and **credibility** are the first order concern.
- Distributions and demand are **dynamic**.
- **Main results:** conditions for convergence to a unique equilibrium and approximately welfare optimal at equilibrium.
- **Future directions:** robustness to collusion?


Future work

How to design user-centered auctions?

- Develop (approximately) credible auctions in other settings.
  - Combinatorial auctions.
  - Resource allocation in blockchains that is robust to collusion.
- Increasing the concern that online advertising causes negative externalities:
  - Microtargeting and its effects to polarization, addiction, manipulation.
  - Other metrics beyond revenue?

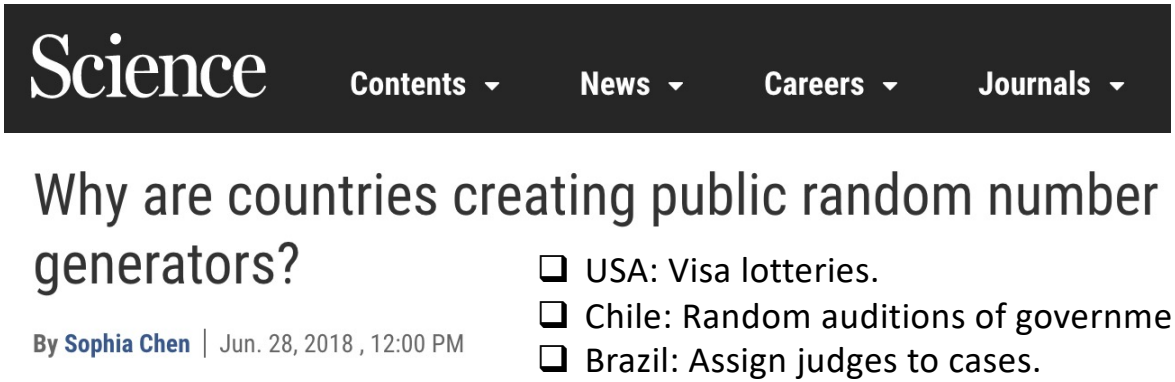

THE WALL STREET JOURNAL.

Regulators Eye the Auctions That Decide Which Web Ads You See

To facilitate real-time bidding, which involves tens of billions of dollars, user data is made available to up to 2,000 companies

How to create energy-efficient blockchains?

- How existing random beacon proposals can take advantage of our reduction of energy-efficient blockchains to the task of designing random beacons.
  - Verifiable delay functions.
  - NIST quantum random-number generators.



- ❑ USA: Visa lotteries.
- ❑ Chile: Random auditions of government officials.
- ❑ Brazil: Assign judges to cases.

How blockchain components affects incentives?

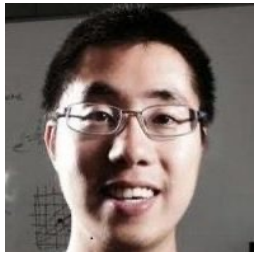
- Expand mining games to consider revenue from new transaction fee auctions.
- Proposals for scalability often offload computation outside blockchains.
  - How to design incentive compatible protocols without using the blockchain?

Source: ACFCS

Economics and Computer Security


Tithi Chattopadhyay


Nick Feamster


Danny Huang


Matt Weinberg

CITP
CENTER FOR INFORMATION TECHNOLOGY POLICY
AT PRINCETON UNIVERSITY

- [CFFHW '19] How can we secure IoT devices when neither users nor sellers are not the most impacted when devices are compromised?

SECURITY

DDoS attacks intensify — Driven in part by COVID-19 and 5G

February 11, 2021

Babur Khan

Thank you

- ``… people have realized that security failure is caused at least as often by bad incentives as by bad design.'' [Anderson and Moore, 07]

Algorithm designer