

Matheus V. X. Ferreira

Research Statement

Vision

I am broadly interested in algorithmic game theory, mechanism design, and how strategic behavior impacts computer systems' security and fairness. While algorithmic game theory studies algorithmic design under incentive constraints, information security explores the protection of a computer system against adversaries. In many real-world settings, adversaries are not intentionally malicious but rather rational and economically driven. By considering a rational adversarial model, we can solve problems that otherwise would be impossible. For example, Bitcoin [Nak19] solves the permissionless Byzantine agreement by monetarily rewarding honest behavior.

In the other direction, the development of the Internet and the World Wide Web brought the need to rethink the traditional adversarial model in mechanism design. Since its inception, mechanism design theory has focused on designing algorithms to allocate scarce resources where a trusted center is responsible for collecting data and implementing the allocation algorithm. Information democratization and system decentralized brought by the Internet started to challenge the concept of a central trusted authority. Questions such as "Who should be accountable when things do not go as expected?" have no clear answer on Internet systems. For that reason, Internet mechanisms often lack transparency and unclear responsibilities with online misinformation, and lack of transparency in online auctions being a few examples. Misinformation is now a reality faced by democratic countries in every election cycle. Many advertising auctions have opaque rules that are often impossible to audit.

Towards the goal of designing secure, fair, and accountable computer systems, my research focuses on:

1. Rethinking the traditional mechanism design framework for an age where Internet systems are increasingly less transparent and decentralized. For that, we must design accountable mechanisms – that is, even when the mechanism designer is an adversary, users must have confidence that the system is fair.
2. Designing decentralized mechanisms that scale, are energy efficient, and are secure against rational adversaries. Blockchains are a powerful tool in this direction, but existing solutions like Bitcoin are energy-inefficient and do not scale. For large-scale adoption, we must develop blockchains that are energy-efficient and provides a good user experience.
3. Understanding the role of policy and regulation in providing better security. Personal computer systems are often vectors for large scale Internet attacks. Users suffer little consequences from purchasing insecure hardware or having bad security practices because they are not held accountable or cannot quantify their privacy loss. Regulation provides economic incentives towards improving the status quo.

Credible Auctions. Vickrey–Clarke–Groves (VCG) auction [Vic61] where the highest bidder wins the item and pays the second-highest bid inspired online auctions such as eBay. Compared with first-price auctions, this simple pricing scheme removes any incentive for strategic bidding, providing a better user experience. However, for many settings, the VCG mechanism introduces a strong assumption that the auctioneer will honestly implement the promised auction. In online auctions such as eBay, it is impossible to guarantee that the platform would not collude with sellers and impersonate fake bidders. As an example, consider an eBay auction where two bidders Alice and Bob bid \$10 and \$5, respectively. If the auction is honest, Alice wins the item and pays only \$5. Still, a malicious auctioneer can easily announce a third bid of \$9.99 after observing Alice's bid to obtain an additional revenue of \$4.99.

Even before the Internet, history has shown that credibility is an essential factor in mechanism adoption. The trusted center has always being a concern in second-price auctions, and increasing lack of transparency in online ad-auctions led major ad exchanges to move away from second-price auctions towards non-strategyproof first-price auctions [Kle02, Slu19].

One of my lines of research addresses the question of designing credible and strategyproof auctions. That is, auctions that neither bidders nor the auctioneer has any incentive to be strategic. Akbarpour, and Li [AL20] showed that the ascending price auction with reserves is the *only* auction that satisfies these conditions. Unfortunately, the ascending price auction requires unbounded rounds of communication between bidders and the auctioneer, which is prohibitively expensive in many applications such as ad-auctions that must run in milliseconds before a search browser loads. Their impossibility result assumes the auctioneer is computationally unbounded, and we overcome this with a mild cryptographic assumption (existence of commitment schemes).

Theorem 1 ([FW20a]) *Assume there exists a cryptographically secure commitment scheme. Then, there is a two-round optimal auction that is both strategyproof and credible.*

Incentives in Energy-Efficient Blockchains.

Blockchains and smart contracts are useful tools to construct transparent mechanisms without a trusted center. As a result, there are many use cases in application domains where market barriers outweigh technical limitations. As an example, Ripple's decentralized ledger allows cross-border payments that circumvent market barriers in international banking.

Unfortunately, to this date, there are no fully decentralized and scalable blockchains. Bitcoin's solution is fully decentralized; however, its Proof-of-Work (PoW) consensus is wasteful and can only process seven transactions per second. In the hope of scaling blockchains, significant effort is put in developing novel energy-efficient consensus algorithms with Proof-of-Stake (PoS) receiving the most attention.

The main technical challenge in longest-chain blockchains is how to select a miner to mine the next block. The mining mechanism is fair if a miner that owns x fraction of a scarce resource (e.g., computation in PoW and currency in PoS), have probability x of mining the next block. Crypto-puzzles in Bitcoin provides a perfect randomness source because they are unbiased and unpredictable – the winner of the next block is unknown until a miner solves the crypto-puzzle, and a miner with x fraction of all computational power has x probability of solving the crypto-puzzle

and thus mining the next block.

Even if mining is fair, Eyal and Sirer [ES14] showed that when $x > 1/3$, a miner can own more than x fraction of the blocks in the longest-chain by executing withholding attacks. In a withholding attack, a malicious miner hides the longest chain to force honest miners to waste resources. Since miners obtain revenue only from blocks that end up in the longest chain, this strategy creates incentives for miners to form collisions. Moreover, many blockchains allow blocks to vote on system parameters – i.e., Ethereum allows each block to vote on future block sizes. Thus withholding attacks allow miners to increase their voting power in relevant operational decisions. Fortunately, for PoW blockchains, as long as no miner owns more than $1/3$ of the mining power, honest mining is a Nash Equilibrium [SSZ16, KKKT16] – i.e., no strategy allows a miner to own more than his fair share of the blocks in the longest chain.

As an alternative, PoS employs a non-trivial distributed protocol to create randomness. If the randomness source is biased or predictable, the blockchain is vulnerable to new strategies that would not be possible in PoW [BCNPW19] and honest mining is never optimal. Unfortunately, known techniques to create a perfect randomness source without crypto-puzzles are inefficient. As a result, existing PoS blockchains have a predictable randomness sources [KRDO17, GHM⁺17].

Due to the significant effort put into improving PoS blockchains, the fundamental question is to understand if an idealized PoS blockchain (one that has access to unbiased and unpredictable randomness source) can replicate the incentive guarantees of PoW [SSZ16, KKKT16]. In [FW20b], we show that PoS and PoW are fundamentally different.

Theorem 2 ([FW20b]) *Consider a PoS blockchain with access to an unbiased and unpredictable randomness source. Then, honest mining is a Nash Equilibrium if no miner owns more than 30.7% of the currency. On the other hand, honest mining is not a Nash Equilibrium if a miner owns more than 32.5% of the currency.*

This result shows that even an ideal PoS blockchain allows strategies that are strictly more profitable than any strategy in PoW. The main observation is that without proof of work, there is no cost for mining at multiple forks (a phenomenon known as nothing-at-stake). Fortunately, our result also shows that nothing-at-stake has mild implications on security if the PoS blockchain has access to unbiased and unpredictable randomness because the threshold where honest mining is optimal is close to 33.3% (the same as for PoW blockchains).

Information security and tech policy. Recent years have seen the proliferation of large profile attacks in Internet-of-Things (IoT) devices [Jer17]. Manufacturers and users could improve their security, but there are few incentives to do so. Implementing better security features such as regular updates increases engineering costs. Adopting better security practices such as strong, unique passwords and two-factor authentication is costly for users.

External regulation can be an alternative to introduce incentives for improving security. In [CFF⁺19], we consider two classes of regulations:

- Regulating manufacturers: requiring manufactures to implement minimum security standards.
- Regulating buyers: encourage users to adopt better security practices via rewards or penalties in the event of their IoT device participate in an attack.

A regulator wishes to minimize the externalities caused by security vulnerabilities (i.e., the probability of DDoS attacks from vulnerable devices), subject to a minimum impact on the seller's revenue. It is

not surprising optimal regulations must regulate both sellers and buyers. If users make poor security choices, no investment in security standards will completely mitigate an attack's risks. Similarly, if devices are vulnerable, then risks are independent of the user's behavior.

The challenge of optimizing and adopting complex regulations motivates the search for simple regulations – those that regulate only manufacturers or only buyers – and the question “Can simple regulations be approximately optimal?”. In [CFF⁺19], we answer this question positively.

Theorem 3 ([CFF⁺19]) *There is a regulation that regulates only buyers or regulates only manufacturers that is approximately optimal (where the optimal regulation potentially regulates both buyers and manufacturers).*

Ongoing and Future Directions

Understanding the Design Space of Credible Auctions. My previous research has shown that it is possible to construct communication efficient single-item credible auctions by introducing cryptographic assumptions and assumptions in bidders' distributions. To construct credible auctions in more general settings, we need to understand how our assumptions expand the design space of credible auctions: are there other auctions that are single-item credible, strategyproof, and optimal under weaker assumptions?

Another research direction is to expand the theory of credible mechanisms beyond single-item auctions. In recent years, online combinatorial auctions (such as the FCC spectrum auctions [MM04]) are becoming increasingly popular.

Auctions with multiple items with arbitrary combinatorial constraints bring unique challenges because the auctioneer can use previously disclosed information regarding one item to form beliefs about other items. Thus, it is unknown if there is a credible general implementation of combinatorial auctions. It would be interesting to characterize the class of combinatorial auctions that have credible implementation without cryptographic assumptions. Then investigate how the techniques developed for single-item auctions can expand the design space of multi-item credible auctions.

Blockchain Transaction Fee Mechanisms.

Designing robust applications on the blockchain is challenging because block space is limited. Whenever there is a high demand for blockchain access, we must allocate block space to a subset of users. We cannot hope that all users have access to the blockchain, but we can maximize social welfare by awarding blockchain access to those willing to pay the highest transaction fees. Guarantees that transaction fee mechanisms are easy to participate in, are robust to manipulation, and have predictable outcomes are the first steps towards having robust systems in the blockchain.

Traditionally, blockchains have credibility as a first-order constraint when designing their transaction fee mechanism. For that reason, all blockchains use first-price auctions instead of second-price auctions since miners cannot be trusted to implement the auction honestly. That is, miners can easily extract higher revenue from second-price auctions by submitting fake transactions. However, user experience is also becoming a first-order concern in the blockchain community. The complexity of optimizing bids and clearing price volatility in first-price auctions have pushed the agenda of redesigning the transaction fee market [Rou20, Yao].

Blockchains also have the first-order constraint that transaction fee auctions require a single round

of communication between users and the blockchain. *My previous research on credible, strategyproof auctions [FW20a] is a first step towards addressing this question.* Still, our solution would require all bidders to communicate twice with the blockchain, which is prohibitively expensive.

As future research directions, we can leverage blockchain decentralization. Traditionally, the main challenge of designing credible auctions comes from the fact the auctioneer can mischaracterize all interactions with bidders. But in blockchains, the consensus algorithm selects a random miner to be the auctioneer in each round. Thus, we can exploit decentralization to construct dynamic mechanisms that are robust to manipulation.

References

- [AL20] Mohammad Akbarpour and Shengwu Li. Credible auctions: A trilemma. *Econometrica*, 88(2):425–467, 2020.
- [BCNPW19] Jonah Brown-Cohen, Arvind Narayanan, Alexandros Psomas, and S Matthew Weinberg. Formal barriers to longest-chain proof-of-stake protocols. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pages 459–473, 2019.
- [CFF⁺19] Tithi Chattopadhyay, Nick Feamster, Matheus V. X. Ferreira, Danny Yuxing Huang, and S. Matthew Weinberg. Selling a single item with negative externalities. In *The World Wide Web Conference, WWW '19*, page 196–206, New York, NY, USA, 2019. Association for Computing Machinery.
- [ES14] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*, pages 436–454. Springer, 2014.
- [FW20a] Matheus V. X. Ferreira and S. Matthew Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In *Proceedings of the 21st ACM Conference on Economics and Computation*, EC '20, page 683–712, New York, NY, USA, 2020. Association for Computing Machinery.
- [FW20b] Matheus V. X. Ferreira and S Matthew Weinberg. Proof-of-stake mining games with perfect randomness. 2020.
- [GHM⁺17] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68, 2017.
- [Jer17] James A Jerkins. Motivating a market or regulatory solution to iot insecurity with the mirai botnet code. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)*, pages 1–5. IEEE, 2017.
- [KKKT16] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, pages 365–382, 2016.

- [Kle02] Paul Klemperer. What really matters in auction design. *Journal of economic perspectives*, 16(1):169–189, 2002.
- [KRDO17] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.
- [MM04] Paul Milgrom and Paul Robert Milgrom. *Putting auction theory to work*. Cambridge University Press, 2004.
- [Nak19] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.
- [Rou20] Tim Roughgarden. Transaction fee mechanism design for the ethereum blockchain: An economic analysis of eip-1559, 2020.
- [Slu19] Sarah Sluis. Google switches to first-price auction, Mar 2019.
- [SSZ16] Ayelet Sapirshtein, Yonatan Sompolsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.
- [Vic61] William Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of finance*, 16(1):8–37, 1961.
- [Yao] Andrew Chi-Chih Yao. An incentive analysis of some bitcoin fee designs. In *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference)*.