Research Statement

Ke Wu, Computer Science Department, Carnegie Mellon University

My current research mainly lies in the intersection of cryptography and game theory. The recent success of cryptocurrency and blockchains offer innovative financial services. As these applications gain widespread adoption, their security and fairness become increasingly crucial to build safe crypto ecosystems. In contrast to classical distributed systems, where fault tolerance is the main focus and incentives are less of a concern, decentralized blockchain environments require a strong incentive for participants to act honestly. Although various decentralized designs are already deployed in real-world applications, most are based on heuristic security and lack formal guarantees. This demands a solid theoretical foundation for the incentive aspect of blockchain and decentralized applications in general. My work mainly focuses on **combining cryptography and game theory to design incentive compatible and provably secure decentralized protocols**. My research in this area can be summarized in the following directions.

- **Decentralized mechanism design.** I designed decentralized mechanisms by leveraging cryptographic primitives. My work used cryptography to circumvent the previous impossibility results in mechanism design and built incentive compatible mechanisms for blockchain applications [SCW23, WSC23].
- **Cryptography meets game theory.** I built cryptographic protocols with strong game-theoretic guarantees. My research studied game-theoretic fairness in multi-party computations and gave a complete characterization of game-theoretic fairness for coin toss protocols [WAS22, KMSW22].

In addition to my work in cryptography and game theory, I have also made contributions in the areas of coding theory [CHL+19, CJLW19, CJLW22, WW21, GGRW22] and the intersection of cryptography and data privacy [SW21]. Through my research, I aim to contribute to the development of secure and fair decentralized environments. I am honored to be recognized for my contributions, having received the *CMU Cylab Fellowship* and the *J.P. Morgan AI Fellowship* during my Ph.D. studies. Below I will describe my previous research and future plans.

1 Previous Research

1.1 Decentralized Mechanism Design

Real estate on a blockchain is a scarce resource. On average, the two largest blockchains, Bitcoin and Ethereum, process roughly 5 and 15 transactions per second, respectively. However, the demand for the blockchain far surpasses the supply, necessitating a mechanism that selects a subset of transactions to include on-chain. This mechanism is called the transaction fee mechanism (TFM): it selects which pending transactions should be included and at what price. We can view it as an auction, in which the miner acts as an auctioneer and auctions off the positions in the block. Interestingly, decentralized mechanism design departs significantly from classical mechanism design in the following sense: 1.) The miner of a block is a strategic player itself and can deviate from the prescribed mechanism, including dictatorially controlling the contents; 2.) Miners and users can easily collude off-chain and manipulate the mechanism to improve their joint gains; 3.) Blockchain is an open system in which users or miners can create many pseudonyms and submit fake transactions that are indistinguishable from the real ones under these pseudonyms. Consequently, well-understood paradigms in classical mechanism design often fail in a decentralized environment since, in classical auction theory, the auctioneer (the miner) is usually assumed to be honest.

Recent developments, such as Ethereum's "EIP-1559" [BCD+19] that was rolled out in August 2021, have prompted efforts to design an "ideal" TFM. Motivated by these developments, [LSZ22, Rou20, Rou21] proposed a formal framework for the following desired properties of an "ideal" TFM.

1. *User incentive compatibility*: every user should be incentivized to follow the protocol honestly;
2. *Miner incentive compatibility*: the miner should implement the mechanism honestly as prescribed;
3. *Side-contract-proofness*: a coalition of the miner and some users should not gain benefit by deviating.

Unfortunately, Chung and Shi [CS23] gave a fundamental impossibility result: No transaction fee mechanism can guarantee all three properties simultaneously. This motivates me to explore whether we can use cryptography to enlarge the design space and circumvent this impossibility result.

In my recent work [SCW23], we showed that, indeed, by leveraging cryptographic primitives, we could design a mechanism that satisfies all three desired properties. Specifically, we designed a new multi-party computation (MPC)-assisted model, where a group of miners together run an MPC to implement the mechanism. This enforces an honest implementation of the mechanism and thus makes it possible to circumvent the previous impossibility result. While cryptography significantly enhances the design space of transaction fee mechanisms, it does not trivialize the problem: We showed that there are still limitations in the MPC-assisted model: the miner cannot gain any positive revenue out of the mechanism. To get rid of this limitation, we consider a mildly stronger assumption in my follow-up work [WSC23]. Specifically, assuming a lower bound on the number of honest users, we gave a mechanism in the MPC-assisted model that achieves positive and asymptotically optimal miner revenue, where a strategic coalition can only increase their joint utility by at most a negligible amount.

Meanwhile, I also explored other decentralized mechanisms like automated market maker (AMM) mechanisms. An AMM exchange is an application running on a blockchain that maintains a pool of crypto assets. It automatically trades assets with users according to some pricing function that prices the assets based on the relative demand/supply. AMMs have created a challenge commonly known as the Miner Extractable Value (MEV), which is widely acknowledged as one of the most critical challenges for blockchain today. In particular, the miners who control the contents and ordering of transactions in a block can extract value by front-running and back-running users' transactions, leading to arbitrage opportunities that guarantee them risk-free returns. In other words, MEV is exploited at the expense of users, hurting the stability and security of the underlying consensus protocol. In our recent work submitted to SODA 2024, we designed the first AMM mechanism that provably eliminates MEV opportunities of miners and, in addition, guarantees incentive compatibility for users.

For a long time, the blockchain community has been seeking secure mechanisms that can be deployed in real-world blockchains and guarantee incentive compatibilities as desired. Our work has been pioneering in exploring the formal guarantees that cryptography can offer in decentralized mechanism design. This opens up a promising design space that lies in the intersection of cryptography and game theory. Importantly, our mechanisms in the MPC-assisted model has the potential to be employed in real-world blockchains. For example, the Ethereum researchers have a keen interest in our recent work in order to understand how cryptography can help with transaction fee mechanisms.

1.2 Cryptography Meets Game Theory

A line of past work [HT04, KN08, ADGH06, OPRV09, AL11] explored the intersection of game theory and cryptography about a decade ago. Many of these papers had similar goals of designing protocols where rational players are incentivized to follow the protocol honestly, as we aim for today. However, the utility notions they adopted were based on the assumption that a rational player prefers to compute the function correctly and learn others' secrets while not leaking their own secrets. This is a mismatch for today's decentralized applications. The real-world applications shed light on what are the correct problem formulation and utility notions of practical relevance. Now is the perfect time to revisit this direction and explore what definitions of utility and security fit best for these applications.

My work has been focused on building game-theoretic fair protocols. An important reason why we care about game-theoretic fairness is that it allows us to circumvent broad impossibility results associated with classical cryptographic notions of fairness. Cryptographic notions of fairness are known to be impossible when there is a majority-sized coalition [Cle86] . However, it is particularly important to

achieve meaningful fairness against a majority-sized coalition in a blockchain environment because it is cheap for parties to create many pseudonyms, and the same party may control a majority number of pseudonyms. This kind of attack has actually taken place in the real world [1], where someone created many pseudonyms to juice the value on the Solana blockchain. This motivates me to explore how we can achieve meaningful fairness against majority-sized coalitions.

In my work [WAS22], we showed that we could achieve game-theoretic fairness against a majority-sized coalition for coin toss protocols, a core primitive in which mutually distrustful players together agree on a uniformly random coin. Game theoretic fairness states that no coalition can bias the output towards its favor, thus guaranteeing a coalition-resistant Nash equilibrium. As a result, no profit-seeking coalition of players would be incentivized to deviate from the protocol. We also gave a complete characterization of the landscape of game-theoretically fair coin toss on the size of the coalition it can tolerate. In my following work [KMSW22], we explored the game-theoretic fairness in leader election protocol, another core primitive in which players want to choose a random leader. Specifically, we build a $\log^*$-round leader election protocol that achieves approximate game-theoretic fairness against majority-sized coalitions. Right now, I am working on extending game-theoretic fairness to tasks of arbitrary randomness generation. I have already built a protocol generating randomness for any distribution of interest while achieving game-theoretic fairness against majority-sized coalitions. The manuscript will be submitted to EUROCRYPT 2024.

The expansion of blockchain has brought about an urgent need for a robust theoretical foundation concerning the incentive aspects of blockchains. My work has made a significant contribution to characterizing the mathematical landscape of game-theoretic fairness, and it is a useful tool for analyzing decentralized protocol incentives. Also, the game-theoretically fair designs we have developed can potentially be deployed on real-world blockchains to generate trusted randomness, which is widely used in decentralized applications like lotteries and leader elections of the underlying consensus of blockchains.

2 Future Work and Desired Impact

2.1 Decentralized Mechanism Designs

Decentralized mechanisms have the potential to revolutionize the financial services industry by creating more accessible and transparent financial systems. Although many real-world blockchain and smart contract protocols employ incentive-based designs and leverage collateral and penalty mechanisms to discourage misbehavior, most real-world protocols today lack formal guarantees. This presents an exciting and promising area that heavily relies on the interplay of cryptography and game theory. Moving forward, I will continue to explore the possibilities of modern cryptographic techniques in the area of decentralized mechanism designs, with a focus on addressing several open questions in the short term.

Heterogeneous transaction sizes. While my previous work explored the feasibility landscape of transaction fee mechanisms, we focus on a simple model where transactions are of equal size. This leads to immediate open questions of designing transaction fee mechanisms that account for heterogeneous transaction sizes. The key technical challenge here is that the feasible subsets of unequal-size transactions, which correspond to feasible knapsack solutions, can not be solved in polynomial time in general. Adapting knapsack auctions from the classical setting [AH06] to the blockchain setting is a potential solution, but it poses challenges due to the decentralized nature.

Game-theoretic analysis of encrypted mempool. Recently, the blockchain community has been trying to build an "encrypted mempool" technique to address the MEV and censorship problem from the consensus layer. Encrypted mempools use cryptographic primitives to encrypt pending transactions, and the miner must first commit to the transactions to include in a block before decrypting. Intuitively, this prevents MEV since the miner cannot see the content of a transaction. While this approach seems promising, it is essential to conduct a rigorous analysis to understand its formal guarantees.

[1] https://www.coindesk.com/layer2/2022/08/04/master-of-anons-how-a-crypto-developer-faked-a-defi-ecosystem/

In the long term, I am enthusiastic about building decentralized mechanisms that can handle more sophisticated real-world models.

Analyzing long-term behaviors. Previous work [CS23, SCW23] mainly focuses on incentive compatibility at a single time scale. While this is a natural starting point, practical transaction fee mechanisms can entangle the auctions run for different blocks. Such dependencies between blocks may open up new strategies for miners' deviation over a longer time scale. For example, [Rou20] investigated miner collusion at a long time scale of the EIP-1559 mechanism: A miner can choose to strategically publish a small block to increase the miner's revenue for the next block. However, other kinds of long-range coordinated deviations are still poorly studied. Understanding the incentives of long-term behaviors and deviations is a central long-term focus of my proposed work on transaction fee mechanisms.

Mechanisms for other decentralized applications. Apart from transaction fee mechanisms, the expansion of decentralization has given rise to other mechanism design challenges. For example, Ad exchanges facilitate real-time auctions for advertisers to purchase digital advertisement space from publishers like NY Times. Earlier this year, Google was sued for monopolizing the Ad exchange market. It is an exciting open space to explore whether cryptographic tools can be integrated into the design of these mechanisms to address issues like monopolization and ensure fair outcomes. The proposed research will investigate the desired incentive compatibility properties for different settings and construct mechanisms that uphold these properties.

2.2 Cryptography Meets Game Theory

Due to the success of blockchain and cryptocurrency, bridging game theory and cryptography is no longer a theoretical-only concern. The blockchain community has a growing appetite for provable secure protocols, yet they do not know the right way to analyze the protocols or the right tool to use in practice. Many factors contribute to the difficulty of modeling or reasoning about incentives in decentralized protocols since this is a brand-new field that lies at the intersection of cryptography, game theory, and economics. There is an urgent need for a solid scientific foundation of the incentive aspect for blockchain and decentralized applications. In the future, I plan to continue building provable secure protocols with strong incentive compatibility guarantees.

Financially fair protocols. Right now, many real-world decentralized designs adopt collateral and penalty mechanisms to incentivize participants to behave honestly: people are required to put in collateral, and they will get punished if they misbehave. In the most naive way, we need a player's collateral to be as large as the maximum total loss of others had the player deviated. Although intuitively correct, many of these designs do not have provable security. This approach is also undesirable since it may require a large amount of collateral, which will discourage participation from small players. Interestingly, my previous work [KMSW22, WAS22] guarantees fairness without any use of collateral. Therefore, I would like to more systematically explore financially fair protocols with minimal collateral for a broader scope of applications. Specifically, I will study the trade-offs between the amount of collateral needed and incentive compatibility for various multi-party computation tasks.

Game-theoretic notions of fairness in general MPC tasks. As a starting point, my previous work characterized inputless tasks like the coin toss, leader election, and randomness generation protocols. Extending game-theoretic fairness to general MPC, where players may hold private information as input, is still an open problem. As mentioned, existing attempts to combine game theory and cryptography [HT04, KN08, ADGH06, OPRV09, AL11] used utility notions that may not align with current practical applications. To address this, I plan to examine real-world applications, identify suitable game-theoretic notions of security and fairness, and design protocols that meet these demands.

In addition to the planned research, I believe more opportunities await me in my next career stage. I am passionate about learning new areas and collaborating with researchers from various backgrounds. In particular, I am eager to conduct multi-disciplinary research that combines cryptography and AI. I believe that the convergence of ideas from these distinct fields can be a catalyst for groundbreaking discoveries and novel solutions to real-world challenges.

References

[ADGH06] Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In *PODC*, pages 53–62, 2006.

[AH06] Gagan Aggarwal and Jason D. Hartline. Knapsack auctions. In *SODA*, page 1083–1092. SIAM, 2006.

[AL11] Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair rational secret sharing. *Journal of Cryptology*, 24(1):157–202, 2011.

[BCD+19] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, and Ian Norden. Ethereum improvement proposal 1559: Fee market change for eth 1.0 chain, 2019. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.

[CHL+19] Kuan Cheng, Bernhard Haeupler, Xin Li, Amirbehshad Shahrasbi, and Ke Wu. Synchronization strings: highly efficient deterministic constructions over small alphabets. In *SODA*, pages 2185–2204. SIAM, 2019.

[CJLW19] Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. Block edit errors with transpositions: Deterministic document exchange protocols and almost optimal binary codes. In *ICALP*, pages 37:1–37:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019.

[CJLW22] Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. Deterministic document exchange protocols and almost optimal binary codes for edit errors. *Journal of the ACM*, 69(6):1–39, 2022.

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *STOC*, 1986.

[CS23] Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. In *SODA*, pages 3856–3899. SIAM, 2023.

[GGRW22] Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. Beyond single-deletion correcting codes: substitutions and transpositions. *IEEE Transactions on Information Theory*, 69(1):169–186, 2022.

[HT04] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *STOC*, pages 623–632, 2004.

[KMSW22] Ilan Komargodski, Shin'ichiro Matsuo, Elaine Shi, and Ke Wu. log*-round game-theoretically-fair leader election. In *CRYPTO*, pages 409–438. Springer, 2022.

[KN08] Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *TCC*, pages 320–339. Springer, 2008.

[LSZ22] Ron Lavi, Or Sattath, and Aviv Zohar. Redesigning bitcoin's fee market. *ACM Transactions on Economics and Computation*, 10(1):1–31, 2022.

[OPRV09] Shien Jin Ong, David C Parkes, Alon Rosen, and Salil Vadhan. Fairness with an honest minority and a rational majority. In *TCC*, pages 36–53. Springer, 2009.

[Rou20] Tim Roughgarden. Transaction fee mechanism design for the ethereum blockchain: An economic analysis of eip-1559. *arXiv preprint arXiv:2012.00854*, 2020.

[Rou21] Tim Roughgarden. Transaction fee mechanism design. *ACM SIGecom Exchanges*, 19(1):52–55, 2021.

[SCW23] Elaine Shi, Hao Chung, and Ke Wu. What can cryptography do for decentralized mechanism design. In *ITCS*, pages 97:1–97:22, 2023.

[SW21] Elaine Shi and Ke Wu. Non-interactive anonymous router. In *EUROCRYPT*, pages 489–520. Springer, 2021.

[WAS22] Ke Wu, Gilad Asharov, and Elaine Shi. A complete characterization of game-theoretically fair, multi-party coin toss. In *CRYPTO*, pages 120–149. Springer, 2022.

[WSC23] Ke Wu, Elaine Shi, and Hao Chung. Maximizing miner revenue in transaction fee mechanism design. Cryptology ePrint Archive, Paper 2023/283, 2023.

[WW21] Ke Wu and Aaron B Wagner. A practical coding scheme for the bsc with feedback. In *ISIT*, pages 136–141. IEEE, 2021.