My primary research interests are in applied cryptography and the foundations of security for decentralized systems. In the past few years, blockchains have emerged as a new class of decentralized systems and are regularly viewed as disruptive technology with a plethora of new applications. A recent report by the Boston Consulting Group projects that blockchains will hold $16 trillion in assets by 2030.

From the broad perspective of security research, blockchains are of particular interest because they operate in a radically new, highly adversarial environment where protocol flaws and software bugs can be immediately monetized by anonymous actors. This makes them an excellent sandbox both for designing more robust protocols and for discovering new adversarial threats.

My research focuses on designing protocols that are secure in this new adversarial environment. In the process, **my work has questioned established modeling assumptions in well-studied, longstanding security frameworks, and found novel insights about classical security notions**—many of which are **of independent interest even beyond blockchains**. My work highlights how the blockchain environment provides a guiding principle for how we should think about the robustness of our systems more broadly.

Research directions. My research has investigated three directions with a similar theme—they demonstrate how the permissionless and highly adversarial environment seen on blockchains surfaces significant new challenges even for well-studied classical security notions.

• *Initiating the study of fair ordering in consensus protocols.* The *consensus* primitive, which underpins many distributed systems, including blockchains, has been studied for the past four decades. But when applications with monetary value are built using it, *new, highly profitable order-manipulation attacks* [10, 13] emerge by exploiting an under-specification—the consensus primitive does not prescribe how transactions need to be ordered. **I initiated a new research direction on *order-fair* consensus protocols** [7, 8, 9], which decentralize trust in the ordering, and provide strong temporal fairness guarantees on the way transactions are ordered. I also uncovered broader connections of order-fairness to questions in social choice theory. My initial work has spawned an active research direction on transaction ordering with 50+ direct followup works by the community that propose new protocols and definitions. I have also been substantially involved in productionizing my research on transaction ordering—an updated version of [5] is being deployed on Arbitrum (the largest layer-2 blockchain); other protocols [4, 8] are being prototyped.

• *Introducing new theory of financial security for decentralized applications.* Traditional notions of software security typically characterize vulnerabilities as error states. But in decentralized settings, the inherently financial nature of smart contracts has surfaced new profit-motivated exploits that leverage complex interactions in ways that can no longer be characterized as software vulnerabilities. Notably, in many cases, these attacks have surfaced despite security audits. In [2], I developed new theory for the security of smart contracts from a *financial lens*—in terms of how much monetary value can be extracted from smart contracts and their composition. Through this lens, and due to the atomic nature of execution, smart contract security can now be cast as a state space search problem. This unlocks the use of formal verification tools [2] and learning techniques [3] to **generically discover new financial exploits**, rule out specific ones, and provide developers with bounds on the exploitable value of their smart contracts. Using these tools, my work discovered two new attacks that extract value from smart contracts.

• *Uncovering deficiencies within cryptographic models of knowledge.* The security goal for many cryptographic protocols is based on a simple intuition: the honest user—who "knows" the secret key—should succeed, while the attacker—who doesn't know the key—should fail. But it turns out that this common model can be eroded [11, 12] by attackers nefariously using trusted execution environments (TEEs) or secure multi-party-computation (MPC)—the very tools employed for building secure protocols. These tools allow for selectively restricting access to the key in ways that can break protocol guarantees without detection. As one example, despite substantial prior work on coercion-resistant electronic voting, this enables powerful new bribery attacks by *violating implicit assumptions* about key ownership in prior work. In [1], I also show how blockchains make these attacks more threatening by enabling large-scale deployment. In [6], I unify the attacks by identifying a common root cause—**a subtle insufficiency in the way cryptography characterizes *knowledge***. I show how the standard proof-of-knowledge primitive doesn't always demonstrate knowledge of the secret key, and develop new theory on *proofs of complete knowledge* (CK) to fix this issue. CK enables proving *unrestricted access* to the secret key, which is in fact *necessary* to prevent these attacks.

The blockchain setting, due to its permissionless and anonymous nature, enables exciting new applications and opportunities for real-world impact. But at the same time, it introduces a radically new adversarial environment for cryptographic systems. As my work shows, building secure protocols in this setting is challenging, and will require new approaches to security. I predict that **security will need to be thought of in a multi-faceted way**—by combining ideas from decentralized systems, cryptography, and mechanism design. I plan to continue to bring this perspective on the security of our systems in my future research.

References

Please see my CV for a full list of publications

* denotes equal first-author contribution
** denotes alphabetical author ordering

[1] James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, **Mahimna Kelkar**, and Ari Juels. *DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs*. 2023. arXiv: 2311.03530 [cs.CR].

[2] Kushal Babel*, Philip Daian*, **Mahimna Kelkar***, and Ari Juels. "Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts". In: *IEEE S&P*. 2023, pp. 2499–2516. **(i) Smart Contract Research Forum (SCRF) Research Impact Award; (ii) Best 2023 DeFi Paper (awarded by the DeFi@CCS'24 Workshop)**.

[3] Kushal Babel, Mojan Javaheripi, Yan Ji, **Mahimna Kelkar**, Farinaz Koushanfar, and Ari Juels. "Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning". In: *CCS*. 2023, pp. 1212–1226.

[4] Kushal Babel, Nerla Jean-Louis, Yan Ji, Ujval Misra, **Mahimna Kelkar**, Kosala Yapa Mudiyanselage, Andrew Miller, and Ari Juels. *PROF: Protected Order Flow in a Profit-Seeking World*. 2024. arXiv: 2408.02303 [cs.CR].

[5] Akaki Mamageishvili, **Mahimna Kelkar**, Jan Christoph Schlegel, and Edward W. Felten. "Buying Time: Latency Racing vs. Bidding for Transaction Ordering". In: *AFT*. 2023, 23:1–23:22. **Deployed by Arbitrum** (the largest layer-2 "rollup" on Ethereum) **and Espresso Systems**.

[6] **Mahimna Kelkar***, Kushal Babel*, Phillip Daian*, James Austgen, Vitalik Buterin, and Ari Juels. "Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets". In: *CCS*. 2024.

[7] **Mahimna Kelkar**, Soubhik Deb, and Sreeram Kannan. "Order-Fair Consensus in the Permissionless Setting". In: *APKC*. 2022, pp. 3–14. **Best paper award**.

[8] **Mahimna Kelkar**, Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan. "Themis: Fast, Strong Order-Fairness in Byzantine Consensus". In: *ACM CCS*. 2023, pp. 475–489. **Prototyped by Chainlink** (the largest oracle provider on Ethereum).

[9] **Mahimna Kelkar**, Fan Zhang, Steven Goldfeder, and Ari Juels. "Order-Fairness for Byzantine Consensus". In: *CRYPTO*. 2020, pp. 451–480.

---

[10] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability". In: *IEEE S&P*. 2020, pp. 585–602.

[11] Lachlan J Gunn, Ricardo Vieitez Parra, and N Asokan. "Circumventing cryptographic deniability with remote attestation". In: *PETS* 2019.3 (2019), pp. 350–369.

[12] Ivan Puddu, Daniele Lain, Moritz Schneider, Elizaveta Tretiakova, Sinisa Matetic, and Srdjan Capkun. *TEEvil: Identity Lease via Trusted Execution Environments*. 2019. arXiv: 1903.00449 [cs.CR].

[13] Kaihua Qin, Liyi Zhou, and Arthur Gervais. "Quantifying Blockchain Extractable Value: How dark is the forest?" In: *IEEE S&P*. 2022, pp. 198–214.