Crypto Crossroads: Reflections from an IC3 Summer Camp Rookie

I'm Pradyumna Shome, a PhD student at the Georgia Institute of Technology, and I've been working on microarchitectural side-channel security for some time. This summer, I am a research intern at Flashbots working on building side-channel mitigations in trusted execution environments (TEEs) to realize the vision of a Single Unifying Auction for Value Expression (SUAVE). In this context, I attended my first blockchain conference: theInstitute of CryptoCurrencies and Contracts (IC3)'s annual summer camp.

The event featured talks on interdisciplinary research and practice on blockchains: from advancements in zero knowledge proofs, hype around TEEs, Ethereum's centralized block builder market, to legal aspects of blockchains, mechanism design, geopolitics of blockchain adoption, and the digital asset offerings from traditional finance (TradFi) firms. I also participated in the hackathon, where our team won 3rd place (and 0.25 ETH!) for a TEE-based Decentralized Verified IPFS Gateway

.

As a relative outsider to a rapidly growing field, I thought I'd share some insights coming from a different background but straight into the research firehose.

Blockchain research is highly interdisciplinary.

Here were just some of the domains in which the talks I attended fit into.

- Computer Science -> Computer Security -> Distributed systems security
- Computer Science -> Computer Security -> Trusted Execution Environments
- Computer Science -> Cryptography -> Zero-knowledge proofs
- Computer Science -> Cryptography -> Threshold cryptography
- Computer Science -> Cryptography -> Multi-party computation
- Computer Science -> Formal Methods -> Verification
- Computer Science -> Distributed Systems -> Consensus algorithms
- Computer Science -> Distributed Systems -> Byzantine fault-tolerance
- Economics -> Game theory
- Economics -> Microeconomics -> Mechanism design
- Law -> Digital Assets

Unlike side-channel security, which I'd describe as an island of knowledge, blockchains are much more of a "full-stack phenomenon", drawing on expertise in multiple computer science disciplines as well as economics, finance, and law. Design decisions and improvements in one field as applied to a blockchain involve trade-offs that affect others. Here are some examples:

1. Consensus algorithms influencing game theory.

The move to Proof-of-Stake consensus algorithms has led to work in game theory to understand incentives of proposers, builders, and relays, and has spawned the emergence of the Maximal Extractible Value (MEV) phenomenon which I will get to later.

1. Mechanism design influencing distributed systems.

Research on token economics, rewards, incentives, and decentralized governance (DAOs) has influenced how distributed systems have been architected.

1. Program verification influencing smart contract languages and vulnerabilities.

Research in formal verification, theorem proving, and analysis of blockchain programs has led to bespoke languages being created for the blockchain, such as Solidity, Move, and Motoko. Programming languages research has also identified automated methods of detecting bugs and vulnerabilities in deployed smart contracts.

1. Byzantine fault tolerance influencing development of threshold cryptography schemes

. Given the very real possibility of malicious actors attempting to subvert consensus algorithms for personal profit, blockchains have seen emerging use of threshold cryptography schemes to minimize risk of corruption, for example the Threshold Network.

1. Graph algorithms and machine learning being used to analyze blockchain activity

. Chainalysis, a blockchain data analysis company uses a knowledge graph, unsupervised machine learning, and network clustering algorithms to detect fraud, ensure compliance, and improve the clarity of the blockchain transaction ecosystem.

Evolving applications of distributed systems and TEEs

A lot of distributed systems research between 2000 and 2020 has been focused around a centralized public cloud provider model such as highly available, reliable, and performant key value stores. At this conference, I saw quite a different focus: with high valuations of cryptocurrencies like Bitcoin and Ethereum at stake, there is real incentive to perform malicious Byzantine faults, which creates the need to push forward research into algorithms and systems with stronger threat models.

In a similar vein, trusted execution environments like Intel SGX, AMD SEV, and ARM TrustZone were created to enforce digital rights management policies and to support secure remote computation for enterprise customers. Now, TEEs have emerged as a compelling alternative to Zero Knowledge Proofs and Multi-Party Computing, with a far more approachable developer experience.

As adoption of cryptocurrencies and decentralized finance increases, I see many exciting opportunities ahead for public cloud, software, and hardware vendors to collaborate, account for new constraints and threat models, and make these technologies better suited to Web3 use cases.

There is tight integration between academia and industry.

I've spent several years hanging out with PhD students and faculty, at UIUC and Georgia Tech. In all these years, I've yet to see something like IC3, in pretty much every other computer science subdiscipline. Nearly all the professors affiliated with IC3 hold either an advising or visiting research position at a blockchain startup. What's more, there is a strong record of collaboration between the 8 or so universities having IC3 faculty, spanning North America (UC Berkeley, Carnegie Mellon University, University of Illinois Urbana-Champaign, Cornell Tech), Europe (University College London, École Polytechnique Fédérale de Lausanne), Middle East and North Africa (Technion – Israel Institute of Technology).

The annual summer camp in the US and winter retreat in Switzerland have certainly helped create a strong network and community among not just the faculty, but also students, and industry partners. A number of startups including Ava Labs, bloXroute, Flashbots, Gyroscope, Oasis Labs, Pisa Research, and Thunder Token, and more have arisen from community members. This has created a vibrant ecosystem in which members can learn from hands-on experience, connect with experts, and contribute in numerous ways. Many of these startups developed from prototypes or academic research projects, which is fantastic. Blockchain companies benefit from advancements in academia needed to create the edge they need, PhD students get to complement their academic research with real-world impact on a live product, while faculty get to straddle two parallel worlds living in a symbiotic relationship. It would be amazing if other research fields had an equivalent community and were less siloed off.

Decentralization creates many challenges that remain to be addressed.

Performance

Centralization is highly suited for efficiency and performance. Single sources of truth greatly expedite decision-making and make for simpler regulation. It's why global financial systems (banks), computer systems (Web2 services), and governance systems (governments and courts) have operated in this manner for ages.

Decentralization leads to the necessity of having numerous copies of the transaction history database (also known as the blockchain ledger), not just to ensure data availability but also for integrity. This increases overall data movement since Layer 1 blockchains must store and process every single transaction – case in point, Mastercard processes 5,000 transactions a second, whereas Proof of Stake Ethereum 2.0 processes only 14.2 (although with sharding the theoretical maximum is slated to be between 20,000 and 100,000). I expect rollups and Layer 2 chains to make great strides towards bridging this gap. What's more, since decentralized participants must operate the protocol for transactions to be processed, they need to be incentivized, just as a traditional bank earns interest on loans and on portfolio management fees. This brings us to MEV, Flashbots's raison d'être

, so to speak,

Maximum extractable value (MEV)

In the traditional finance world, companies in high-frequency trading benefit from having real-time and ahead-of-time visibility into transactions to exploit short-term increases and decreases in prices. By paying brokerages to send order flow their way, market makers are able to issue transactions based on information about volumes of trades for each asset, in exchange for fast execution. In Proof-of-Stake Ethereum, the the set of pending transactions (the mempool) is generally publicly visible. This allows savvy transaction processors (validators / block builders) to launch complex tactics such as:

- Sandwiching

(issuing a buy and a sell order sequenced around a transaction in the mempool, to take advantage of the slip in price after the transaction)

- Frontrunning

(issuing a transaction sequenced ahead of an existing transaction)

- Arbitrage

(taking advantage of price differences of an asset on different exchanges)

- and more, including time bandit attacks and liquidation of undercollateralized loans

Profits and rewards made from all of these optimal block generation strategies is known as Maximum Extractable Value (MEV). So far, over ~1.2 million USD worth of MEV has been extracted from Ethereum. MEV results in strong centralizing forces, as it incentivizes collusion amongst members to extract the most profit in an increasingly compounding fashion. Despite the many efforts made to combat MEV such as MEV-Share, MEV-Blocker, MEV-Boost, and Flashbots' private transaction pool that protects against such attacks, the block builder market is still dominated by 3 entities that produce over 90% blocks.

I find it interesting to hear about strategies to limit this undesirable value extraction, because it reveals the complexities of appropriately incentivizing each participant to ensure good behavior, in the absence of a traditional judicial system. I see it as running a court via a system of rewards (transaction fees and rewards for optimal sequencing) and penalties (slashing staked Ethereum for violating one of the norms of operating a validator). Whether the optimal solution is (enshrined) Proposer-Block Builder Separation (PBS), Execution Tickets, or something else, it's quite worth experimenting with and simulating a number of strategies, as well as considering second-order effects, which can be hard to predict until a system is deployed.

Usability, Safety, and Education

Unlike many other startups that use market surveys, develop user personas, and attempt to establish product-market fit, blockchain products seem to be developed from a much more experimental and R&D style, with a healthy serving of ideological hacktivism baked in.

One aspect that I found less discussed and emphasized at the conference was safety. Decentralization is not something that shows up in the UX for payments – it's a swap of the back-end layer, which is often abstracted away from the end-user. Thus, the risks with blockchain become an impediment to adoption, from the volatility of the major cryptocurrencies, to scams (including but not limited to FTX), money laundering (such as with Tornado Cash), challenges maintaining private keys, lack of anonymity in transactions, and the difficulty of recovering money accidentally, maliciously, or coercively sent from one's bank account.

Moreover, there is a deluge of barriers that new adopters need to overcome, from getting fluent with all the acronyms, new currencies, apps, and protocols. I think there is a lot of scope for user studies, ethnographic studies, user acceptance testing, and focus groups to explore the landscape of challenges people are facing and will likely face as the decentralized finance landscape grows ever more complex.

Final Thoughts

I had an excellent experience connecting with students, faculty, and industry partners through this 1 week event. Quite clearly, there has been a smorgasbord of progress in the field ever since Satoshi Nakamoto's paper on Bitcoin came out. Many distinct and somewhat siloed areas of computer science research spanning security, distributed systems, cryptography, and program analysis seem to have found promising new applications in the implementation of blockchain technology. For folks looking for an area with potential, I think this industry offers plenty of scope and funding to solve interesting research, implementation, product, and deployment problems with significant practical impact. I would like to thank IC3 for such a well-organized, valuable, and fun event that certainly left a mark.