Blockchain: Introduction and Challenges

Blockchains as digital commons: Human civilization flourishes in the presence of commons, resources maintained in public interest for everyone to access. The digital realm presents a new opportunity for the emergence of a digital commons shared by all humanity. However, existing digital commons are maintained by large privately-held companies such as Facebook, Twitter, Uber, Airbnb, Ebay and Amazon. These platforms centralize information and control into very few entities leading to significant frictions. Blockchains offer an alternative paradigm for creating a digital commons maintained in a distributed manner without any central intermediary. This can power a host of transformative decentralized applications such as social networking, ride sharing, digital rights management, data markets, and global identity management. However, blockchains are not yet efficient and scalable enough for these applications (see Table below). This talk will summarize recent attempts to design decentralized, secure and scalable blockchains using ideas from information, coding and networking theory.

	Security	**Energy usage**	**Latency**	**Throughput**
Bitcoin	Adversary < 50% power	~Netherlands	~Hours	10 Transactions /Sec
Desirable	Adversary < 50% power	No wastage	Network latency (~Seconds)	Network Bandwidth (~250,000 Tx / Sec)

Overview of Blockchains: We will present an overview of how blockchains work. We will take the example of Bitcoin as a canonical example in order to illustrate the workings of a blockchain. We will explain the mining process and the longest chain protocol underpinning Bitcoin, and illustrate the properties achieved by Bitcoin [1]: immutability and censorship-resistance, which translate to safety and liveness in a traditional distributed system [2]. We also illustrate how a general distributed computer can be constructed on top of a blockchain.

Scaling Blockchains: We illustrate how to convert the Bitcoin system into a proof-of-stake system that does not require energy wastage [4,5]. We use our protocol PoSAT [6,7] as a clean example for illustrating this transformation. We point out connections [3] to the deep stochastic theory of branching random walks to prove and improve [6,7] the security of previously unproven protocols such as the Chia proof-of-space protocol [8]. We then point out how to improve the latency of longest-chain protocols ujsing the idea of Prism. We have used information-theoretic ideas such as list-decoding and typicality to design a new blockchain protocol: Prism [9,10], which is the first proof-of-work protocol with optimal-latency confirmation and security against strongly adaptive adversaries. Finally, we briefly mention how ideas from coding theory [11] with dynamic game theory (Blackwell approachability) can be combined to design a full-stack blockchain system which is the first to achieve full scaling as well as security against a fully adaptive adversary [12] achieving optimal performance.

Front-Running: We mention briefly about the front-running problem: miners order transactions according to transaction fee rather than arrival time, and hence it is possible to front-run transactions by paying higher transaction fee. We talk about recent attempts to improve resistance to front-running by taking a consensus order from many different nodes [13] and [14].

Applications: Finally, we conclude with pointing out two potential applications: (1) running a global carbon exchange on a public blockchain to power the green economy and (2) enabling more democratized monetization of digital content to power the digital creator economy.

References:

1. Nakamoto, Satohsi., "Bitcoin: A peer-to-peer electronic cash system" whitepaper 2009.
2. Garay, Juan, Aggelos Kiayias, and Nikos Leonardos. "The bitcoin backbone protocol: Analysis and applications." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2015.
3. A. Dembo, **S. Kannan**, E. N. Tas, D. Tse, P. Viswanath, X. Wang, O. Zeitouni, "Everything is a Race and Nakamoto Always Wins," to appear in ACM Conference on Computer and Communications Security (CCS) 2020. (Acceptance rate = 15%)
4. Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol." In *Annual International Cryptology Conference*, pp. 357-388. Springer, Cham, 2017.
5. Badertscher, Christian, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. "Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 913-930. 2018.

6. V. Bagaria, A. Dembo, **S. Kannan**, S. Oh, D. Tse, P. Viswanath, X. Wang and O. Zeitouni, “Proof-of-Stake Longest Chain Protocols: Security vs Predictability” preprint on arxiv
7. **S. Deb**, **S. Kannan**, D. Tse, “PoSAT: Proof-of-Work Availability and Unpredictability, without the Work” in Financial Cryptography and Data Security (FC) 2021
8. Cohen, Bram, and Krzysztof Pietrzak. "The chia network blockchain." Whitepaper 2019.
9. V. Bagaria, **S. Kannan**, D. Tse, G. Fanti, and P. Viswanath, “Prism: Deconstructing the Blockchain to Approach Physical Limits," in ACM Conference on Computer and Communication Security (CCS), 2019.
10. Yang, Lei, Vivek Bagaria, Gerui Wang, Mohammad Alizadeh, David Tse, Giulia Fanti, and Pramod Viswanath. "Prism: Scaling bitcoin by 10,000x." arXiv preprint arXiv:1909.11261 (2019).
11. M.Yu, S. Sahraei, S. Li, S. Avestimehr, **S. Kannan**, and P. Viswanath, “Coded Merkle Tree: Solving Data Availability Attacks in Blockchains,” in Proc. Financial Cryptography (FC) Feb. 2020 (Acceptance: 35/162 = 22%).
12. R. Rana, S. Kannan, D. Tse and P. Viswanath, “Free2Shard: Adaptive-adversary-resistant sharding via Dynamic Self Allocation,” preprint in arxiv.
13. M.Kelkar, S. Deb and S. Kannan, Order-Fair Consensus in the Permissionless Setting. Preprint.
14. M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels Order-fairness for byzantine consensus Crypto 2020.