

Foundations of Blockchain
Instructor: Tim Roughgarden
Fall 2020
Course Developed for Columbia-IBM Center for Blockchain and Data
Transparency

Week 1: Bitcoin basics. Transactions, proof-of-work, mining.

Week 2: Attacks on Bitcoin. Double-spend attacks. The difficulty adjustment algorithm. Selfish mining.

Week 3: Formal properties of Bitcoin. Security and liveness.

Week 4: Mining pools. Optimality results for reward-sharing schemes.

Week 5: Issues with Bitcoin. Introduction to Ethereum. Survey of layer-1 scalability solutions.

Week 6: Proof-of-stake blockchains. Verifiable delay functions.

Week 7: Introduction to classical theory of consensus, possibility and impossibility results.

Week 8: Asynchronous consensus. The FLP impossibility result.

Week 9: Streamlet: BFT for the blockchain era.

Week 10: Bitcoin in the context of classical consensus. Dichotomy result between security and adaptive liveness.

Week 11: Payment channels and the Lightning Network: how they work and what they're good for.

Week 12: Transaction fee mechanism design in Ethereum: an economic analysis of EIP-1559. (Part 1)

Week 13: Transaction fee mechanism design in Ethereum: an economic analysis of EIP-1559. (Part 2)