Principles of Cryptocurrency Design
(Programma provvisorio)

Francesco Pasquale

Marzo 2026

Problemi classici di consenso. Sistemi distribuiti fault-tolerant: modelli sincroni e asincroni. Protocolli per modelli sincroni, teoremi di impossibilità. Preliminari di crittografia e reti: Funzioni hash crittografiche; schemi di firma digitale; curve ellittiche e crittografia; reti P2P e Internet.
[4, 5]

Consenso "permissionless" e Bitcoin. Consistenza finale e il protocollo di consenso di Nakamoto: Decentralizzazione, mining, proof-of-work, regolazione della difficoltà. La struttura dei blocchi, alberi di Merkle, UTXOs. Il linguaggio di scripting di Bitcoin. Malleabilità delle transazioni. Sicurezza e privacy di Bitcoin. I Fork e gli Altcoin.
[3, 1]

I protocolli di secondo livello. Rendere Bitcoin scalabile e la rete Lightning. Canali di pagamento e contratti Hash Time-Locked. Routing sulla rete Lightning. Onion routing. Sicurezza e privacy della rete Lightning.
[2]

References

[1] Andreas M Antonopoulos. *Mastering Bitcoin: Programming the open blockchain*. "O'Reilly Media, Inc.", 2017.

[2] Andreas M. Antonopoulos, Olaoluwa Osuntokun, and René Pickhardt. *Mastering the Lightning Network*. "O'Reilly Media, Inc.", 2021.

[3] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[4] Elaine Shi. Foundations of distributed consensus and blockchains. 2020.

[5] Roger Wattenhofer. *Blockchain science: Distributed ledger technology*. Inverted Forest Publishing, 2019.