Proposte di approfondimenti

Francesco Pasquale

May 27, 2026

1 Prima parte: Problemi classici di consenso

1. Il *lower bound* sul numero di *round* nel protocollo di Dolev-Strong [10].
2. Approfondimenti sulle nozioni di *random oracle* [3] e funzione hash crittografica [34].
3. Il modello *Partially Synchronous* [11].
4. Il modello *Partially Authenticated* [28].
5. Il CAP Theorem [5, 14, 4, 15].
6. Altri algoritmi di consenso [26, 27].
7. Byzantine Agreement tramite *blacklisting* dei nodi corrotti [24, 25, 20].

2 Seconda parte: Bitcoin

1. Analisi del meccanismo di consenso in Bitcoin [12, 23, 2, 13].
2. Analisi della sicurezza dello schema di firma digitale ECDSA [21, 17] e l'importanza della scelta del *nonce* [35].
3. Malleabilità delle transazioni e il caso MtGox [7].
4. Soft-fork e l'evoluzione del consenso in Bitcoin [32].
5. Inferire la struttura della rete P2P di Bitcoin [30, 31, 9, 29].
6. Firme di Schnorr [36] e l'upgrade Taproot BIP-341, BIP-342
7. La curva ellittica `secp256k1` e algoritmi quantistici per il logaritmo discreto su curve ellittiche [1].

3 Terza parte: Lightning

1. Una versione dei *payment channels* con caratteristiche leggermente diverse da quelle della *Lightning network* [8].
2. Analisi empirica di diversi aspetti della *Lightning network* [39, 38, 16].
3. Modelli per l'analisi dei *payment path* nella *Lightning network* [33]
4. Tecniche di *routing* per la *Lightning network* [19]

5. Analisi del traffico nella *Lightning network*, gli algoritmi per il *routing* dei pagamenti e possibili attacchi *DoS* [37].

6. *Lightning network* e *privacy* [22].

7. *Cross-chain swaps* [18, 6].

References

[1] Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi, Justin Drake, and Dan Boneh. Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations. *arXiv preprint arXiv:2603.28846*, 2026. `https://arxiv.org/pdf/2603.28846`.

[2] Christian Badertscher, Juan Garay, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. But Why Does It Work? A Rational Protocol Design Treatment of Bitcoin. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 34–65, Cham, 2018. Springer International Publishing. `https://link.springer.com/content/pdf/10.1007/978-3-319-78375-8_2.pdf`.

[3] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993. `https://dl.acm.org/doi/pdf/10.1145/168588.168596`.

[4] Eric Brewer. A certain freedom: thoughts on the CAP theorem. In *Proceedings of the 29th ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, pages 335–335, 2010.

[5] Eric A. Brewer. Towards robust distributed systems (abstract). In *Proceedings of the Nineteenth Annual ACM Symposium on Principles of Distributed Computing*, PODC'00, page 7, New York, NY, USA, 2000. Association for Computing Machinery. `https://doi.org/10.1145/343477.343502`.

[6] Michele Ciampi, Muhammad Ishaq, Rafail Ostrovsky, Ioannis Tzannetos, and Vassilis Zikas. Cross-chain lightning trades: Getting the advantages of a custodial exchange while keeping your assets. *Cryptology ePrint Archive*, 2025. `https://eprint.iacr.org/2025/1746.pdf`.

[7] Christian Decker and Roger Wattenhofer. Bitcoin transaction malleability and Mt-Gox. In *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19*, pages 313–326. Springer, 2014. `https://tik-old.ee.ethz.ch/file/7e4a7f3f2991784786037285f4876f5c/esorics2014_submission_48.pdf`.

[8] Christian Decker and Roger Wattenhofer. A fast and scalable payment network with bitcoin duplex micropayment channels. In *Stabilization, Safety, and Security of Distributed Systems: 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings 17*, pages 3–18. Springer, 2015. `https://tik-old.ee.ethz.ch/file/716b955c130e6c703fac336ea17b1670/duplex-micropaymentchannels.pdf`.

[9] Sergi Delgado-Segura, Surya Bakshi, Cristina Pérez-Solà, James Litton, Andrew Pachulski, Andrew Miller, and Bobby Bhattacharjee. Txprobe: Discovering bitcoin's network topology using orphan transactions. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security - 23rd International Conference, FC 2019,*

Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers, volume 11598 of *Lecture Notes in Computer Science*, pages 550–566, Frigate Bay, 2019. Springer. http://fc19.ifca.ai/preproceedings/58-preproceedings.pdf.

[10] Danny Dolev and H. Raymond Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983. https://www.cs.huji.ac.il/~dolev/pubs/authenticated.pdf.

[11] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. *Journal of the ACM (JACM)*, 35(2):288–323, 1988. https://dl.acm.org/doi/pdf/10.1145/42282.42283.

[12] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-662-46803-6_10.pdf.

[13] Juan A. Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications. *J. ACM*, apr 2024. https://doi.org/10.1145/3653445.

[14] Seth Gilbert and Nancy Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *Acm Sigact News*, 33(2):51–59, 2002. https://www.cse.unsw.edu.au/~cs9243/20t3/papers/gilbert02:.brewers.conjecture.pdf.

[15] Seth Gilbert and Nancy Lynch. Perspectives on the CAP Theorem. *Computer*, 45(2):30–36, 2012. https://dspace.mit.edu/bitstream/handle/1721.1/79112/Brewer2.pdf.

[16] Florian Grötschla, Lioba Heimbach, Severin Richner, and Roger Wattenhofer. On the lifecycle of a lightning network payment channel. *arXiv preprint arXiv:2409.15930*, 2024. https://arxiv.org/pdf/2409.15930.

[17] Dominik Hartmann and Eike Kiltz. Limits in the provable security of ecdsa signatures. In *Theory of Cryptography Conference*, pages 279–309. Springer, 2023. https://eprint.iacr.org/2023/914.pdf.

[18] Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254, 2018. https://dl.acm.org/doi/pdf/10.1145/3212734.3212736.

[19] Hsiang-Jen Hong, Sang-Yoon Chang, and Xiaobo Zhou. Auto-tune: Efficient autonomous routing for payment channel networks. In *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, pages 347–350. IEEE, 2022.

[20] Shang-En Huang, Seth Pettie, and Leqi Zhu. Byzantine agreement in polynomial time with near-optimal resilience. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 502–514, 2022. https://dl.acm.org/doi/pdf/10.1145/3519935.3520015.

[21] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1:36–63, 2001. https://cmapsconverted.ihmc.us/rid=1V1Z7BB5X-ZBQ686-2X4/Elliptic%20Curve%20Digital%20Signature%20Algorithm.pdf.

[22] George Kappos, Haaroon Yousaf, Ania Piotrowska, Sanket Kanjalkar, Sergi Delgado-Segura, Andrew Miller, and Sarah Meiklejohn. An empirical analysis of privacy in the lightning network. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25*, pages 167–186. Springer, 2021. https://arxiv.org/pdf/2003.12470.

[23] Lucianna Kiffer, Rajmohan Rajaraman, and Abhi Shelat. A better method to analyze blockchain consistency. In *Proceedings of the 2018 acm sigsac conference on computer and communications security*, pages 729–744, 2018. https://dl.acm.org/doi/pdf/10.1145/3243734.3243814.

[24] Valerie King and Jared Saia. Byzantine agreement in expected polynomial time. *Journal of the ACM (JACM)*, 63(2):1–21, 2016. https://dl.acm.org/doi/pdf/10.1145/2837019.

[25] Valerie King and Jared Saia. Correction to byzantine agreement in expected polynomial time, jacm 2016. *arXiv preprint arXiv:1812.10169*, 2018. https://arxiv.org/pdf/1812.10169.

[26] Leslie Lamport. The part-time parliament. *ACM Transactions on Computer Systems*, 16(2):133–169, 1998. https://dl.acm.org/doi/pdf/10.1145/279227.279229.

[27] Leslie Lamport. Paxos made simple. *ACM SIGACT News (Distributed Computing Column)*, 32(4):51–58, 2001. https://ldpreload.com/p/paxos-simple.pdf.

[28] Christoph Lenzen, Julian Loss, Kecheng Shi, and Benedikt Wagner. Byzantine consensus in the partially authenticated setting. *Cryptology ePrint Archive*, 2026. https://eprint.iacr.org/2026/470.pdf.

[29] Shaoyu Li, Shanghao Shi, Yang Xiao, Chaoyu Zhang, Y Thomas Hou, and Wenjing Lou. Bijack: Breaking bitcoin network with tcp vulnerabilities. In *European Symposium on Research in Computer Security*, pages 306–326. Springer, 2023. https://shaoyu-li.github.io/files/bijack.pdf.

[30] Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee. Discovering bitcoin's public topology and influential nodes. *et al*, 2015. https://allquantor.at/blockchainbib/pdf/miller2015topology.pdf.

[31] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, July 18-21, 2016*, pages 358–367, Toulouse, 2016. IEEE Computer Society. https://philipp-andelfinger.net/pdfs/neudecker2016timing.pdf.

[32] Jakob Svennevik Notland, Mariusz Nowostawski, and Jingyue Li. Runtime evolution of bitcoin's consensus rules. *IEEE Transactions on Software Engineering*, 2023. https://d197for5662m48.cloudfront.net/documents/publicationstatus/173728/preprint_pdf/4fa41105d30caed777146bd554327b12.pdf.

[33] Rene Pickhardt, Sergei Tikhomirov, Alex Biryukov, and Mariusz Nowostawski. Security and privacy of lightning network payments with uncertain channel balances. *arXiv preprint arXiv:2103.08576*, 2021. https://arxiv.org/pdf/2103.08576.

[34] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*, pages 371–388. Springer, 2004. https://eprint.iacr.org/2004/035.pdf.

[35] Dylan Rowe, Joachim Breitner, and Nadia Heninger. The curious case of the half-half bitcoin ecdsa nonces. In *International Conference on Cryptology in Africa*, pages 273–284. Springer, 2023. https://eprint.iacr.org/2023/841.pdf.

[36] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4:161–174, 1991. https://link.springer.com/content/pdf/10.1007/bf00196725.pdf.

[37] Saar Tochner, Aviv Zohar, and Stefan Schmid. Route hijacking and dos in off-chain networks. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 228–240, 2020. https://eprints.cs.univie.ac.at/6554/1/61-aft20.pdf.

[38] Philipp Zabka, Klaus-T Foerster, Christian Decker, and Stefan Schmid. Short paper: A centrality analysis of the lightning network. In *International Conference on Financial Cryptography and Data Security*, pages 374–385. Springer, 2022. https://arxiv.org/pdf/2201.07746.

[39] Philipp Zabka, Klaus-T Foerster, Stefan Schmid, and Christian Decker. Empirical evaluation of nodes and channels of the lightning network. *Pervasive and Mobile Computing*, 83:101584, 2022. https://schmiste.github.io/pmc22.pdf.