Module 2 further readings

The two types of failures that can happen in a distributed system

Lamport, L. (1987, May 28). Distribution [Bulletin board message]. Retrieved from https://lamport.azurewebsites.net/pubs/distributed-system.txt

Lampson, B., & Rinard, M. (2002). Principles of computer systems: Distributed systems [Lecture notes]. Retrieved from https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-826-principles-of-computer-systems-spring-2002/lecture-notes/

Impossibility of consensus

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems, 20*(4), 398-461. doi: 10.1145/571637.571640

Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the Association for Computing Machinery, 32*(2), 374-382. doi: 10.1145/3149.214121

Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in the presence of faults. *Journal of the Association for Computing Machinery, 27*(2), 228-234. doi: 10.1145/322186.322188

Schreiber, F. R. (1975). *Sybil: the true story of a woman possessed by sixteen separate personalities*. Melbourne, Australia: Penguin Books Australia.

Proof of work and the importance of miners

Back, A. (2002). *Hashcash - a denial of service counter-measure*. Retrieved from http://www.hashcash.org/papers/hashcash.pdf

Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In E. F. Brickell (Ed.), *Lecture Notes in Computer Science: Vol. 740. Advances in cryptology - CRYPTO' 92* (pp. 139-147). doi: 10.1007/3-540-48071-4_10

Resolving forks

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://nakamotoinstitute.org/bitcoin/

51% attacks and network delays

Rosenfeld, M. (2012). *Analysis of hashrate-based double-spending*. Retrieved from https://bitcoil.co.il/Doublespend.pdf

GHOST protocol

Sompolinsky, Y., & Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In T. Okamoto, & R. Böhme (Eds.), *Lecture Notes in Computer Science: Vol. 8975. Financial Cryptography and Data Security. FC 2015 (pp. 507-527)*. doi: 10.1007/978-3-662-47854-7_32

Wood, G. (n.d.). *Ethereum: A secure decentralised generalised transaction ledger, EIP-150 revision*. Retrieved from https://gavwood.com/paper.pdf

*Wherever possible we have provided you with an open access/ free version of the readings in this MOOC. In some cases however, we have not been able to find a free version so we have provided the full title of the reading for you to search on **WorldCat** or **Amazon.**