Module 4 further readings

The Balance Attack

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In N. Christin & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8437*. (pp. 436-454). Retrieved from https://link.springer.com/chapter/10.1007/978-3-662-45472-5_28

Natoli, C., & Gramoli, V. (2017, June 26-29). *The balance attack or why forkable blockchains are ill-suited for consortium*. 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi:10.1109/DSN.2017.44

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. Retrieved December 10, 2018, from https://arxiv.org/abs/1402.2009

Double Spending in Ethereum

Ekparinya, P., Gramoli, V., & Jourjon, G. (2018). Double-spending risk quantification in private, consortium and public Ethereum blockchains. Retrieved from https://arxiv.org/abs/1805.05004

Module 4 conclusion

Finney, H. (2011, February 13). Best practice for fast transaction acceptance - how high is the risk? [Forum post]. Retrieved from https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In *Proceedings of the 24th USENIX Security Symposium, Washington, D.C. August 12-14, 2015*. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. Retrieved December 10, 2018, from https://arxiv.org/abs/1402.2009

vector76. (2011, August 17). Fake Bitcoins? [Forum post]. Retrieved from https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391

*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.**