Module 1 further readings

History of blockchain

Agrawal, G. (2018, March 5). A cypherpunk's manifesto – A definition of privacy. *Coinmonks*. Retrieved from https://medium.com/coinmonks/a-cypherpunks-manifesto-a-definition-of-privacy-66c36f99e940

Basson, P. [PetriB]. (2018, January 26). The untold history of Bitcoin: Enter the cypherpunks. *The Startup*. Retrieved from https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1

Back, A. (1997, March 28). Hash cash postage implementation. [Electronic mailing list message]. Retrieved from http://www.hashcash.org/papers/announce.txt

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

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), *Advances in cryptology: Proceedings of Crypto 82* (pp. 199-203). doi: 10.1007/978-1-4757-0602-4_18

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

Finley, K. (2016, June 16). A $50 million hack just showed that the DAO was all too human. *Wired*. Retrieved from https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

Finney, H. (2004). RPW – Reusable proofs of work. [Electronic mailing list message]. Retrieved from https://cryptome.org/rpow.htm

Hughes, E. (1993). A cypherpunk's manifesto. Retrieved from https://www.activism.net/cypherpunk/manifesto.html

Leech, D. P. & Chinworth, M. (2001). *The economic impacts of NIST's Data Encryption Standard (DES) program* (National Institute of Standards and Technology Program Office Strategic Planning and Economic Analysis Group Planning Report 01-2). Retrieved from https://www.nist.gov/sites/default/files/documents/2017/05/09/report01-2.pdf

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

Narayanan, A. (2013). What happened to the crypto dream?, Part 1. *IEEE Security & Privacy 11*(2), 75-76. doi: 10.1109/MSP.2013.45

Szabo, N. (2008, December 27). Bit gold [Blog post]. Retrieved from https://unenumerated.blogspot.com/2005/12/bit-gold.html

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

Double spending

Hrones, M. (2018, June 3). Zencash target of 51% attack; loses more than $500k in double spend transactions. Retrieved from **http://bitcoinist.com/zencash-target-51-attack-loses-500k-double-spend-transactions/**

Osborne, C. (2018, May 25). Bitcoin Gold suffers double spend attacks, $17.5 million lost. Retrieved from **https://www.zdnet.com/article/bitcoin-gold-hit-with-double-spend-attacks-18-million-lost/**

*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.**