

References

- [1] <http://bitcoin.org>.
- [2] https://en.bitcoin.it/wiki/Category:Mixing_Services.
- [3] <http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization>.
- [4] <https://bitcointalk.org/index.php?topic=279249.0>.
- [5] <http://msrvideo.vo.msecnd.net/rmcvideos/192058/dl/192058.pdf>.
- [6] <https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki#Specification>.
- [7] https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#Backwards_Compatibility.
- [8] https://en.bitcoin.it/wiki/Mining_hardware_comparison.
- [9] <https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki>.
- [10] <http://luke.dashjr.org/programs/bitcoin/files/charts/branches.html>.
- [11] <https://bitcointalk.org/index.php?topic=196259.0>.
- [12] <https://en.bitcoin.it/wiki/Contracts>.
- [13] <https://en.bitcoin.it/wiki/Script>.
- [14] <http://litecoin.org>.
- [15] Martín Abadi, Michael Burrows, and Ted Wobber. Moderately hard, memory-bound functions. In *NDSS*, 2003.
- [16] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Ad-hoc-group signatures from hijacked keypairs. In *in DIMACS Workshop on Theft in E-Commerce*, 2005.
- [17] Man Ho Au, Sherman S. M. Chow, Willy Susilo, and Patrick P. Tsang. Short linkable ring signatures revisited. In *EuroPKI*, pages 101–115, 2006.
- [18] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *J. Cryptographic Engineering*, 2(2):77–89, 2012.
- [19] David Chaum and Eugène van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.
- [20] Fabien Coelho. Exponential memory-bound functions for proof of work protocols. *IACR Cryptology ePrint Archive*, 2005:356, 2005.
- [21] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO*, pages 174–187, 1994.
- [22] Cynthia Dwork, Andrew Goldberg, and Moni Naor. On memory-bound functions for fighting spam. In *CRYPTO*, pages 426–444, 2003.
- [23] Eiichiro Fujisaki. Sub-linear size traceable ring signatures without random oracles. In *CT-RSA*, pages 393–415, 2011.