References

[1] K. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, "Analysis of an Electronic Voting System," *Proc. IEEE Symposium on Security and Privacy,* pp. 27-42, 2014.

[2] A. D. Rubin, "Security considerations for remote electronic voting," *Communications of the ACM,* vol. 45, no. 12, pp. 39-44, 2002.

[3] B. Schneier, Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, New York: John Wiley & Sons, Inc, 1996.

[4] Caltech/MIT Voting Technology Project, "Voting: What Has Changed, What Hasn't, & What Needs Improvement (2012)," October 2012. [Online]. Available: http://www.vote.caltech.edu/reports/.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 2008. [Online]. Available: https://www.bitcoin.org.

[6] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," in *CCS '14 Proc. ACM SIGSAC Conference on Computer and Communications Security*, New York, 2014.

[7] S. Wolchok, E. Wustrow, D. Isabel and J. A. Halderman, "Attacking the Washington, D.C. Internet Voting System," in *Proc. 16th Conference on Financial Cryptography & Data Security*, Kralendijk, 2012.

[8] K. W. a. R. T. A. Villafiorita, "Development, Formal Verification, and Evaluation of an E-Voting System With VVPAT," *IEEE Transactions on Information Forensics and Security,* vol. 4, no. 4, pp. 651-661, 2009.

[9] "H.R.3295 - Help America Vote Act of 2002," 29 10 2002. [Online]. Available: https://www.congress.gov/bill/107th-congress/house-bill/3295/.

[10] fec.gov , "Direct Recording Electronic (DRE)," [Online]. Available: http://www.fec.gov/pages/dre.htm.

[11] P. Y. A. Ryan, D. Bismark , J. Heather, S. A. Schneider and Z. Xia, "Prêt à voter: a voter-verifiable voting system," *IEEE Transactions on Information Forensics and Security,* vol. 4, no. 4, 2009.

[12] D. Chaum, R. T. Carback and J. Clark, "Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes," *IEEE Transactions on Information Forensics and Security,* vol. 4, no. 4, pp. 611-627, Dec. 2009.

[13] R. L. Rivest, "On the notion of 'software independence'," *Phil. Trans. R. Soc. A,* vol. 366, p. 3759–3767, 2008.

[14] D. Wagner, "Voting Systems Audit Log Study," Report commissioned by the California Secretary of State, Berkeley, 2010.

[15] L. Barlow, "An Introduction to Electronic Voting," November 2003. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.136.2993.

[16] "THE FUTURE OF E-VOTING," *IADIS International Journal on Computer Science and Information Systems* , vol. 12, no. 2, pp. 148-165, 2017.

[17] . J. A. Feldman, J. A. Halderman and E. W. Felten, "Security analysis of the diebold AccuVote-TS voting machine," *EVT'07: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology,* 2007.

[18] P. D. DeVries, "An Analysis of Cryptocurrency, Bitcoin, and the Future," *International Journal of Business Management and Commerce,* vol. 1, no. 2, 2016.

[19] F. Liu, X. Li and G. Gao, "The Design of an e-cash System," *International Conference On Computer Design and Applications,* 2010.

[20] Y. Baseri, J. Mohajeri and B. Takhtaei, "Secure untraceable off-line electronic cash system," *Scientia Iranica,* vol. 20, no. 3, pp. 637-646, 2013.

[21] bitcoin.org, "Transactions Guide - Bitcoin," 2017. [Online]. Available: https://bitcoin.org/en/transactions-guide. [Accessed 1 March 2017].

[22] Certicom Research, "Standards for Efficient Cryptography Group," [Online]. Available: http://www.secg.org/. [Accessed 1 March 2017].

[23] Certicom Corp, "Standards for Efficient Cryptography 2 (SEC 2)," 27 January 2010. [Online]. Available: http://www.secg.org/sec2-v2.pdf.

[24] "Base58Check encoding - Bitcoin Wiki," 27 November 2017. [Online]. Available: https://en.bitcoin.it/wiki/Base58Check_encoding#Background.

[25] "Pubkey Script, ScriptPubKey - Bitcoin Glossary," [Online]. Available: https://bitcoin.org/en/glossary/pubkey-script. [Accessed 1 March 2017].

[26] E. Abu-Shanab, M. Knight and H. Refai, "E-voting systems: A tool for e-democracy," *anagement Research and Practice,* vol. 2, pp. 264-274, 2010.

[27] "RIPEMD-160," 30 June 2014. [Online]. Available: https://en.bitcoin.it/wiki/RIPEMD-160. [Accessed 1 March 2017].

[28] Bitcoin Project, "Transactions — Bitcoin," [Online]. Available: https://developer.bitcoin.org/devguide/transactions#pay-to-public-key-hash-p2pkh. [Accessed 1 March 2017].

[29] "Bitcoin-wallet," [Online]. Available: https://github.com/bitcoin-wallet/bitcoin-wallet. [Accessed 30 June 2017].

[30] "Developer Guides — Bitcoin," [Online]. Available: https://developer.bitcoin.org/devguide/. [Accessed 31 March 2017].

[31] "Debian/Ubuntu OpenSSL Package Random Number Generator Weakness," [Online]. Available: https://knowledge.digicert.com/solution/SO9094.html. [Accessed 1 March 2017].

[32] "Secp256k1," [Online]. Available: https://en.bitcoin.it/wiki/Secp256k1. [Accessed 1 March 2017].

[33] T. Ahmad, J. Hu and S. Han, "An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography," *2009 Third International Conference on Network and System Security,* pp. 474-479, 2009.

[34] D. W. Jones, "A Brief Illustrated History of Voting," The University of Iowa Department of Computer Science, 2003. [Online]. Available: http://homepage.divms.uiowa.edu/~jones/voting/pictures/.

[35] A. Ekblaw, A. Azaria, J. D. Halamka and A. Lippman, "A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data," MIT Media Lab, Beth Israel Deaconess Medical Center, 2016.

[36] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum & Ethcore, 2017.