distributed role-based access control for dynamic coalition environments. In *Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on*, pages 411–420. IEEE, 2002.

[13] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.

[14] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM (JACM)*, 38(3):690–728, 1991.

[15] Nozomi Hayase. The Blockchain and the Rise of Networked Trust. `http://www.coindesk.com/blockchain-rise-networked-trust/`, 2014.

[16] Vincent C Hu, D Richard Kuhn, and David F Ferraiolo. Attribute-based access control. *Computer*, (2):85–88, 2015.

[17] James BD Joshi, Walid G Aref, Arif Ghafoor, and Eugene H Spafford. Security models for web-based applications. *Communications of the ACM*, 44(2):38–44, 2001.

[18] Sunny King. Primecoin: Cryptocurrency with prime number proof-of-work. 2013.

[19] Peter L. Montgomery Kirsten Eisenträger, Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In *Topics in Cryptology - CT-RSA 2003*, volume 2612 of *LNCS*, 2003.

[20] Andrew Yehuda Lindell. Anonymous authentication. *Journal of Privacy and Confidentiality*, 2(2):4, 2007.

[21] Loi Luu, Viswesh Narayanan, Kunal Baweja, Chaodong Zheng, Seth Gilbert, and Prateek Saxena. SCP: a computationally-scalable byzantine consensus protocol for blockchains. Technical report, Cryptology ePrint Archive, Report 2015/1168, 2015.

[22] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 397–411. IEEE, 2013.

[23] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.

[24] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[25] Lan Nguyen and Rei Safavi-Naini. Dynamic k-times anonymous authentication. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security - ACNS 2005*, volume 3531 of *LNCS*, pages 318–333. Springer, 2005.

[26] Marc Pilkington. Blockchain technology: principles and applications. *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*, 2016.

[27] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. DACC: Distributed access control in clouds. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 91–98. IEEE, 2011.

[28] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak. Privacy preserving access control with authentication for securing data in clouds. In *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, pages 556–563. IEEE, 2012.

[29] Pierangela Samarati and Sabrina Capitani de Vimercati. Access control: Policies, models, and mechanisms. In *International School on Foundations of Security Analysis and Design*, pages 137–196. Springer, 2000.

[30] Ravi S Sandhu, Edward J Coyne, Hal L Feinstein, and Charles E Youman. Role-based access control models. *Computer*, 29(2):38–47, 1996.

[31] Ravi S Sandhu and Pierangela Samarati. Access control: principle and practice. *Communications Magazine, IEEE*, 32(9):40–48, 1994.

[32] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE, 2014.

[33] Stuart Schechter, Todd Parnell, and Alexander Hartemink. Anonymous authentication of membership in dynamic groups. In *International Conference on Financial Cryptography*, pages 184–195. Springer, 1999.

[34] Adi Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[35] Melanie Swan. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

[36] Tim Thomas. A mandatory access control mechanism for the unix file system. In *Aerospace Computer Security Applications Conference, 1988., Fourth*, pages 173–177. IEEE, 1988.

[37] Sarah Underwood. Blockchain beyond bitcoin. *Communications of the ACM*, 59(11):15–17, 2016.

[38] Marko Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*, pages 112–125. Springer, 2015.

[39] Lei Xu and Dongdai Lin. Refinement of Miller's algorithm over Edwards curves. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2010*, volume 5985 of *LNCS*, pages 106–118. Springer, 2010.

[40] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Proceedings of the 29th conference on Information communications - INFOCOM 2010*, pages 534–542. IEEE Press, 2010.

[41] Guy Zyskind, Oz Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.