UNIVERSITI PUTRA MALAYSIA

BLOCKCHAIN-BASED ELECTRONIC HEALTH RECORD SYSTEM

Saleh Abdulaziz Saleh Habtor

FSKTM 2019 16

BLOCKCHAIN-BASED ELECTRONIC HEALTH RECORD SYSTEM

By

SALEH ABDULAZIZ SALEH HABTOR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Information Security

JUNE 2019

DEDICATIONS

For my Mom, No one has ever been given more loving and unconditional support than I have been given by you. I love you, too.

For my Dad, without your unconditional love, your unwavering guidance and support, all of this could never have happened.

To all who give me consolation, advice, and help me...

To all who step with me in my work step by step...

I dedicate my efforts product and what I produced...

To them I dedicate this work

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Information Security

BLOCKCHAIN-BASED ELECTRONIC HEALTH RECORD SYSTEM

By

SALEH ABDULAZIZ SALEH HABTOR

JUNE 2019

Supervisor: Zuriati Ahmed Zukarnain Prof. Dr.

Faculty: Computer Science and Information Technology

Health records nowadays considered as an important legal document that hold a lot of patients' sensitive information like diseases, medications, personal details and more. The patient's sensitive information is subject to data breaches by hackers on regular basis, also, these patient's records need to be exchanged between different medical institutions that patients visit each time. As a result, the protection of this records in rest and in motion is a must; to preserve patient's privacy and to achieve health record security goals of confidentiality, integrity and availability. The existing health record systems does not have the balance between data privacy, ease of use and secure way to access data, so conflicts between data privacy and data accessibility are common to occur. Blockchain works as shared ledger that store each transaction happened in the network, this ledger is immutable, shared and transparent. The blockchain technology provide suitable solution by enables data storage on decentralized platform. This technology can be used in the healthcare domain to provide appropriate access control mechanism and maintain the privacy of health records. In this project, we are proposing a decentralized blockchain-based

electronic health record system which also called Decentralized application or DApp in short, that provide an efficient way to access records by health practitioners and maintain confidentiality of patient sensitive information. The system uses Ethereum blockchain and its smart contracts to achieve most secure access control for data security.

Abstrak tesis yang dikemukakan kepada Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Sarjana Keselamatan Maklumat

BLOCKCHAIN-BASED ELECTRONIC HEALTH RECORD SYSTEM

Oleh

SALEH ABDULAZIZ SALEH HABTOR

JUNE 2019

Penyelia: Zuriati Ahmed Zukarnain Prof. Dr.

Fakulti: SAINS KOMPUTER DAN TEKNOLOGI MAKLUMAT

Rekod kesihatan pada masa kini dianggap sebagai dokumen undang-undang penting yang memegang banyak maklumat sensitif pesakit seperti penyakit, ubat, butiran peribadi dan banyak lagi. Maklumat sensitif pesakit tertakluk kepada pelanggaran data oleh penggodam secara teratur, juga, rekod pesakit ini perlu ditukar di antara institusi perubatan yang berbeza yang dikunjungi pesakit setiap kali. Akibatnya, perlindungan rekod ini dalam rehat dan gerakan adalah satu kemestian; untuk mengekalkan privasi pesakit dan untuk mencapai matlamat keselamatan rekod kesihatan kerahsiaan, integriti dan ketersediaan. Sistem rekod kesihatan sedia ada tidak mempunyai keseimbangan antara privasi data, kemudahan penggunaan dan cara selamat untuk mengakses data, jadi konflik antara privasi data dan akses data adalah perkara biasa berlaku. Blockchain berfungsi sebagai lejar bersama yang menyimpan setiap transaksi yang berlaku dalam rangkaian, lejar ini tidak berubah, dikongsi dan telus. Teknologi blockchain menyediakan penyelesaian yang sesuai dengan membolehkan storan data pada platform terdesentralisasi. Teknologi ini boleh digunakan di domain penjagaan kesihatan untuk menyediakan mekanisme kawalan akses yang

sesuai dan mengekalkan privasi rekod kesihatan. Dalam projek ini, kami mencadangkan sistem rekod kesihatan elektronik berasaskan blockchain yang berpusat di desentralisasi yang juga dipanggil aplikasi Desentralisasi atau DApp secara ringkas, yang menyediakan cara yang cekap untuk mengakses rekod oleh pengamal kesihatan dan mengekalkan kerahsiaan maklumat sensitif pesakit. Sistem ini menggunakan blok Ethereum dan kontrak cerdas untuk mencapai kawalan capaian yang paling selamat untuk keselamatan data.

ACKNOWLEDGMENTS

First and foremost, praise be to Allah through whose mercy (and favors) all good things are accomplished. ("My Lord, increase me in knowledge." . Surat Taha 20:114).

I would like to thank my parents. I am deeply indebted to them for their unconditional support and sacrifice for so many years. I would like to express the greatest appreciation and sincerest gratitude to my supervisor, Prof. Dr. Zuriati Ahmed Zukarnain, for her guidance through all the steps of research and writing dissertation.

I thank and appreciate the valuable effort of my lecturers at Faculty of Computer Science and Information Technology (FSKTM), Universiti Putra Malaysia (UPM), Malaysia.

This thesis was submitted to the Information Security Department, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of **Master of Information Security**.

Zuriati Ahmed Zukarnain, PhD
Prof. Dr.
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia

Date: June 25, 2019

DECLARATION

I hereby confirm that:

- This thesis is my original work;
- Quotations, illustrations and citations have been duly referenced;
- This project report has not been submitted previously or concurrently for any other degree at any other institutions;
- Intellectual property from the project report and copyright of project report are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- Written permission must be obtained from supervisor before project report is published (in the form of written, printed or in electronic form);

(Signature)

SALEH ABDULAZIZ SALEH HABTOR
(GS50516)
Date: June 25, 2019

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

This chapter give an overview of the research topic and explains the motivation for this work. The problem statement is then identified followed by the, research objectives and scope. At the end of this chapter the organization of dissertation is provided.

1.1 Background and Motivation

Electronic Medical Record (EMR), or Electronic Health Record (EHR), is a collection of health information related to patients that stored in a digital or electronic format that is available electronically, this information or record can be exchanged between different health institutions (Gunter and Terry, 2005). Records can be shared through the internet between different information systems (Gunter and Terry, 2005). EHRs contain a lot of medical information like medication, medical history, allergies, demographics, laboratory tests, X-rays, vital signs, and personal information like name, weight, age, and billing information.

EHRs were never designed to manage multi-institutional, life time medical records (Ekblaw et al., 2016). Patients through their whole life visit multiple health institutions, which makes them leave a copy of their health records scattered on various hospitals and healthcare providers, by doing this it become difficult to use, track and access the past health data, because it's not well stored an organized. Exchanging EHRs between health providers in easy and secure manner is required to ensure that providers have up-to-date information about their patients. Data exchanging or sharing is essential to makes it easier for health provider to effectively treat their patients (Zhang et al., 2018).

1.2 Problem Statement

Data privacy means to guaranteeing that users have the authority over access to data, while accessibility to data refers to guaranteeing unconstrained access to data. There are naturally occurring conflicts among privacy and data access, and medical care is a domain where this conflict can occur. The primary issue is how to give proper access to sensitive data (health records), with privacy preserving , anonymity, and prevent misuse of information.

A decentralized access control system built for the electronic health record system has therefore been proposed. Classical access control systems like DAC, MAC and RBAC are created for systems under common administrative control and rely on a centralized user identity database (Miltchev et al., 2008). In the centralized server system, they are effective and safe, but, they struggle to accommodate users with the size of the system expanding to grow rapidly. Although some studies has involved in the construction of decentralized access control systems (Ouaddah et al., 2017; Ruj et al., 2014; Han et al., 2010) in different fields, most of them have one or more shortcomings, they are vulnerable, slow or highly complicated.

By using blockchain technology, access to patients records by health care practitioners will be more secure, and eliminates the data breaches that exploits classic access control.

1.3 Research Objectives

The objective of this project is to design a Decentralized web Application (DApp) for Electronic Health Records that utilize the blockchain technology to produce a decentralized, secure, scalable and efficient access control for electronic health record system.

1.4 Research Contributions

The contribution of this work is as follow:

1. Develop a new electronic health record system.
2. Implement a blockchain based access control model.

1.5 Research Scope

This project focus on implement a suitable access control mechanism in the blockchain to manage access and identify users on the health recored system.

1.6 Organization of Dissertation

This research comprises of five chapters. Chapter 1 is the introduction chapter covers the background of the study, identifies and discusses the problem statement, research objectives, explains the scope of research, ends with a brief description of the organization of the dissertation. Chapter 2 introduces the literature review on electronic health record systems importance and security concerns that face these systems, then Discuss the classic access control mechanisms, after that blockchain technology explained and how to utilize this technology to solve the security gaps that electronic health records have. Chapter 3 focuses on the research methodology and presents the web application framework in detail. What follows are the proposed research technique, and implementation by employing JavaScript and Ethereum blockchain. The results are presented and discussed in Chapter 4 while Chapter 5 offers the conclusions of the study and makes recommendations for further related research.

REFERENCES

Anicas, M. 2014, An Introduction to OAuth 2, https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2.

Antonopoulos, A. M. 2014. *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc.".

Atherton, J. 2011. Development of the electronic health record. *AMA Journal of Ethics* 13 (3): 186–189.

Bach, L., Mihaljevic, B. and Zagar, M. 2018. Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1545–1550. IEEE.

Baliga, A. 2017, In Persistent, In *Persistent*.

Bell, D. E. and La Padula, L. J. 1976, Secure computer system: Unified exposition and multics interpretation, Tech. rep., MITRE CORP BEDFORD MA.

Botelho, B., Vaughan, J. and Rouse, M. 2018, MongoDB, https://searchdatamanagement.techtarget.com/definition/MongoDB.

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A. and Accenture, L. 2016. Blockchain: Securing a New Health Interoperability Experience. *Accenture LLP* .

Bryson, D., Penny, D., C. Goldenberg, D. and Serrao, G. 2018. Blockchain Technology for Government. *MITRE* .

Buterin, V. et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* .

Castro, M., Liskov, B. et al. 1999. Practical Byzantine fault tolerance. In *OSDI*, 173–186.

Cavalli, E., Mattasoglio, A., Pinciroli, F. and Spaggiari, P. 2004. Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics* 73 (3): 297–303.

Chohan, U. 2017, What is Bitcoin Double Spending?, https://whatis.techtarget.com/definition/consensus-algorithm.

Chong, K. 2017, What is MetaMask and why is it important, https://www.quora.com/What-is-MetaMask.

Christidis, K. and Devetsikiotis, M. 2016. Blockchains and smart contracts for the internet of things. *Ieee Access* 4: 2292–2303.

Citrix. 2019, Role-based access control, https://docs.citrix.com/en-us/citrix-hypervisor/users/rbac-overview.html.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. et al. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2 (6-10): 71.

Cruz, J. P., Kaji, Y. and Yanai, N. 2018. RBAC-SC: Role-based access control using smart contract. *IEEE Access* 6: 12240–12251.

Culver, K. 2016. Blockchain Technologies: A whitepaper discussing how the claims process can be improved. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

Dagher, G. G., Mohler, J., Milojkovic, M. and Marella, P. B. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society* 39: 283–297.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. and Wang, F. 2017. Secure and trustable electronic medical records sharing using blockchain. In *AMIA Annual Symposium Proceedings*, 650. American Medical Informatics Association.

Dwork, C. and Naor, M. 1992. Pricing via processing or combatting junk mail. In *Annual International Cryptology Conference*, 139–147. Springer.

Ekblaw, A., Azaria, A., Halamka, J. D. and Lippman, A. 2016. A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference*, 13.

Ethereum. 2019a, Ethereum Homestead Documentation, http://www.ethdocs.org/en/latest/.

Ethereum. 2019b, Solidity, https://solidity.readthedocs.io/en/v0.5.3/.

Evered, M. and Bögeholz, S. 2004. A case study in access control requirements for a health information system. In *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32*, 53–61. Australian Computer Society, Inc.

Farzandipour, M., Sadoughi, F., Ahmadi, M. and Karimi, I. 2010. Security requirements and solutions in electronic health records: lessons learned from a comparative study. *Journal of medical systems* 34 (4): 629–642.

Fernando, J. 2004. Factors that have contributed to a lack of integration in health information system security. *The Journal on Information Technology in Healthcare* 2 (5): 313–328.

Fu, A., Yu, S., Zhang, Y., Wang, H. and Huang, C. 2017. NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users. *IEEE Transactions on Big Data* .

Gediminas. 2018, What is HTML? The Basics of Hypertext Markup Language Explained, https://www.hostinger.my/tutorials/what-is-html.

GenesisMining. 2018, What is the Ethereum Blockchain?, https://www.genesis-mining.com/what-is-the-ethereum-blockchain.

Goranović, A., Meisel, M., Fotiadis, L., Wilker, S., Treytl, A. and Sauter, T. 2017. Blockchain applications in microgrids an overview of current projects and concepts. In *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, 6153–6158. IEEE.

Gropper, A. 2016. Powering the physician-patient relationship with hie of one blockchain health it. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

Gunter, T. D. and Terry, N. P. 2005. The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of medical Internet research* 7 (1): e3.

Han, W., Xu, M., Zhao, W. and Li, G. 2010. A trusted decentralized access control framework for the client/server architecture. *Journal of Network and Computer Applications* 33 (2): 76–83.

Haughn, M. and Rouse, M. 2017, Consensus Algorithm, https://whatis.techtarget.com/definition/consensus-algorithm.

Hayani, S. 2018, Nextjs for everyone, https://medium.freecodecamp.org/an-introduction-to-next-js-for-everyone-507d2d90ab54.

Häyrinen, K., Saranto, K. and Nykänen, P. 2008. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. *International journal of medical informatics* 77 (5): 291–304.

HealthIT.gov. 2018, What is an electronic health record (EHR)?, https://www.healthit.gov/faq/what-electronic-health-record-ehr.

Hileman, G. 2016, State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin, https://www.coindesk.com/state-of-blockchain-q1-2016.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R. and Taylor, R. 2005. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health affairs* 24 (5): 1103–1117.

HIPPA, J. 2018, Healthcare Data Breaches by Year, https://www.hipaajournal.com/healthcare-data-breach-statistics/.

Ivan, D. 2016. Moving toward a blockchain-based method for the secure storage of patient records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

Jacco. 2017, Role-Based Access Control Disadvantages, https://security.stackexchange.com/questions/151333/role-based-access-control-disadvantages/.

Jenks, T. 2018, Pros and Cons of Different Blockchain Consensus Protocols, https://www.verypossible.com/blog/pros-and-cons-of-different-blockchain-consensus-protocols.

Kaaniche, N. and Laurent, M. 2017. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications* 111: 120–141.

Karame, G. O., Androulaki, E. and Capkun, S. 2012. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, 906–917. ACM.

Khatwani, S. 2018, Different Types Of Blockchains In The Market and Why We Need Them, https://coinsutra.com/different-types-blockchains/l.

Konstantinos. 2016, MySQL Reference Manual—Using Stored Routines (Procedures and Functions), https://dev.mysql.com/doc/refman/5.7/en/stored-routines.html.

Kwon, J. and Johnson, M. E. 2012. Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association* 20 (1): 44–51.

Lai, V. 2018, What is Practical Byzantine Fault Tolerance (pBFT)?, https://crushcrypto.com/what-is-practical-byzantine-fault-tolerance/.

Lamport, L., Shostak, R. and Pease, M. 1982. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4 (3): 382–401.

Laurent, M., Kaaniche, N., Le, C.-Y. and Plaetse, M. V. 2018. An Access Control Scheme based on Blockchain Technology.

Li, N. 2011. *Discretionary Access Control*, 353–356. Boston, MA: Springer US.

Linn, L. A. and Koo, M. B. 2016. Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

LiskAcademy. 2018, Byzantine Fault Tolerance, https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/byzantine-fault-tolerance-explained.

Michal, J., Cohn, A. and Butcher, J. R. 2018. Blockchain technology. *The Journal* .

Miltchev, S., Smith, J. M., Prevelakis, V., Keromytis, A. and Ioannidis, S. 2008. Decentralized access control in distributed file systems. *ACM Computing Surveys (CSUR)* 40 (3): 10.

Mišić, J. and Mišić, V. B. 2007. Implementation of security policy for clinical information systems over wireless sensor networks. *Ad Hoc Networks* 5 (1): 134–144.

Morris, S. 2019, What is JavaScript?, https://skillcrush.com/2012/04/05/javascript/.

Nakamoto, S. et al. 2008. Bitcoin: A peer-to-peer electronic cash system .

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. 2016. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Neisse, R., Steri, G. and Nai-Fovino, I. 2017. A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 14. ACM.

Ouaddah, A., Abou Elkalam, A. and Ait Ouahman, A. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks* 9 (18): 5943–5964.

Ouaddah, A., Mousannif, H., Elkalam, A. A. and Ouahman, A. A. 2017. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks* 112: 237–262.

Pandit, N. 2018, What Is ReactJS and Why Should We Use It?, https://www.c-sharpcorner.com/article/what-and-why-reactjs/.

Peterson, K., Deeduvanu, R., Kanjamala, P. and Boles, K. 2016. A blockchain-based approach to health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare*, 1–10.

Ploeg, J., Skelly, J., Rowan, M., Edwards, N., Davies, B., Grinspun, D., Bajnok, I. and Downey, A. 2010. The role of nursing best practice champions in diffusing practice guidelines: a mixed methods study. *Worldviews on Evidence-Based Nursing* 7 (4): 238–251.

Qian, X. and Lunt, T. F. 1996. A MAC policy framework for multilevel relational databases. *IEEE Transactions on Knowledge and Data Engineering* 8 (1): 3–15.

Ray, A. and Newell, S. 2010. Health information systems: Concepts, methodologies, tools, and applications .

Reinke, J. 2016, Understanding OAuth2, http://www.bubblecode.net/en/2016/01/22/understandi
oauth2/.

Remix. 2019, Welcome to Remix, https://remix.readthedocs.io/en/latest/index.html.

Richards, K., Shea, S. and Rouse, M. 2018, Access Control, https://searchsecurity.techtarget.com/definition/access-control.

Rouse, M. 2018, Digital Signature, https://searchsecurity.techtarget.com/definition/digital-signature.

Ruj, S., Stojmenovic, M. and Nayak, A. 2014. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE transactions on parallel and distributed systems* 25 (2): 384–394.

Samarin, A. 2016, Electronic Health Records implementation with blockchain, BPM, ECM and platform, http://improving-bpm-systems.blogspot.com/2016/07/electronic-health-records-ehr.html.

Sandhu, R. S. and Samarati, P. 1994. Access control: principle and practice. *IEEE communications magazine* 32 (9): 40–48.

Sharma, C. 2016, Attribute Based Access Control, https://www.slideshare.net/chandramsharma/attribute-based-access-control.

Stepien, B., Matwin, S. and Felty, A. 2011. Advantages of a non-technical XACML notation in role-based models. In *2011 Ninth Annual International Conference on Privacy, Security and Trust*, 193–200. IEEE.

Szabo, N. 1997. The idea of smart contracts. *Nick Szabo's Papers and Concise Tutorials* 6.

Tan, J. 2008. *Medical Informatics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. IGI Global.

Tar, A. 2018, Proof-of-Work, Explained, https://cointelegraph.com/explained/proof-of-work-explained?ref=5332.

Tozzi, C. 2017, Byzantine Fault Tolerance: The Key for Blockchains, https://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058.

Tran, H. 2018. Enabling a decentralized organization through smart contracts and tokens on the Ethereum blockchain .

Tutorialpoints. 2019, Node.js, https://www.tutorialspoint.com/nodejs/nodejsintroduction.htm.

Wikipedia. 2019a, Cascading Style Sheets, https://en.wikipedia.org/wiki/CascadingStyleSheets.

Wikipedia. 2019b, Microsoft Visual Studio, https://en.wikipedia.org/wiki/MicrosoftVisualStudio.

Xu, J. J. 2016. Are blockchains immune to all malicious attacks? *Financial Innovation* 2 (1): 25.

Zhang, P., White, J., Schmidt, D. C., Lenz, G. and Rosenbloom, S. T. 2018. Fhirchain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal* 16: 267–278.

Zheng. 2018, General Components of an EHR System, https://www.ukessays.com/essays/information-technology/key-components-of-electronic-health-records-information-technology-essay.php?vref=1.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. IEEE.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. and Wang, H. 2018. Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services* 14 (4): 352–375.

Zilavy, T. 2018, What Is A Hybrid Blockchain And Why You Need To Know About It?, https://medium.com/altcoin-magazine/what-is-a-hybrid-blockchain-and-why-you-need-to-know-about-it-c7b887d2bae.

Zyskind, G., Nathan, O. et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, 180–184. IEEE.