QUANTIFYING AND IMPROVING THE SECURITY OF BLOCKCHAIN SYSTEMS

A Dissertation Outline Presented

by

A. PINAR OZISIK

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

September 2019

College of Information and Computer Sciences

QUANTIFYING AND IMPROVING THE SECURITY OF BLOCKCHAIN SYSTEMS

A Dissertation Outline Presented

by

A. PINAR OZISIK

Approved as to style and content by:

Brian N. Levine, Chair

Philip S. Thomas, Member

Yuriy Brun, Member

Nikunj Kapadia, Member

James Allan, Chair
College of Information and Computer Sciences

ABSTRACT

QUANTIFYING AND IMPROVING THE SECURITY OF BLOCKCHAIN SYSTEMS

SEPTEMBER 2019

A. PINAR OZISIK

B.Sc., BRANDEIS UNIVERSITY

M.S., UNIVERSITY OF MASSACHUSETTS

Directed by: Professor Brian N. Levine

Blockchains, such as Bitcoin, Ethereum and Litecoin, are among the most successful peer-to-peer systems on the Internet. Bitcoin has been adopted more widely for e-commerce than any previous digital currency. Ethereum is also quickly gaining prominence as a blockchain that runs Turing-complete distributed applications. Even though these systems have advantages, including decentralized operation, there also exist many limitations that decrease the security and privacy of blockchains.

In this thesis, I analyze and improve the security of blockchain systems. In the first chapter, I analyze a blockchain system's algorithm for setting block discovery difficulty. Difficulty is updated glacially in most systems (e.g., every two weeks in Bitcoin). However, the of churn of mining power can cause problems when the difficulty is not set often. Mining power can change due to miners' updating to new hardware, diurnal changes in electricity rates, or swings in the exchange rate of a currency. For example, Bitcoin Cash has seen enormous variance in mining power since its creation. I propose two alternatives to accurately update difficulty: one that solely uses information that is currently available in blockchain networks, and another based on status reports regularly broadcast from some or all miners of their partial proof-of-work (POW). Status reports can also be used for emergency difficulty adjustment, an algorithm the network resorts to when a block takes unusually long to discover.

Status reports add overhead into networks because they require the broadcast of additional information. In order to reduce traffic, in the second chapter, I introduce a novel method of interactive set reconciliation for the distribution of status reports. Even without status reports, this protocol works for the efficient distribution of blocks. The approach, called Graphene, couples a Bloom filter with an IBLT. Then I evaluate performance analytically and show that Graphene blocks are always smaller.

In the third chapter, I analyze the feasibility of double-spend and selfish mining attacks on blockchain systems. The hash rate of miners is the primary quantitative factor that determines the security of any POW based blockchain consensus algorithm. Most analyses generally assume that the hash rate of honest and malicious miners is known. However, I show that hash rate estimation is difficult and introduces high variance. Therefore, I argue that these double-spend and selfish mining attacks are difficult to carry out with high precision, and use reinforcement learning techniques to realistically evaluate these attacks without full knowledge of mining power.

TABLE OF CONTENTS

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

INTRODUCTION

Contributions

The following is a summary of the contributions in each chapter of this proposal.

1.

Collaborators

CHAPTER 1

TARGET ESTIMATION

1.1

Overview

CHAPTER 2

GRAPHENE

CHAPTER 3

RL APPLIED TO BITCOIN

CHAPTER 4

RELATED WORK

CHAPTER 5

TIMELINE

BIBLIOGRAPHY

[1] Acquisti, Alessandro. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (2004), ACM, pp. 21–29.

[2] Andrés, Miguel E, Bordenabe, Nicolás E, Chatzikokolakis, Konstantinos, and Palamidessi, Catuscia. Geo-indistinguishability: Differential privacy for location-based systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (2013), ACM, pp. 901–914.

[3] Ben-Sasson, Eli, Chiesa, Alessandro, Garman, Christina, Green, Matthew, Miers, Ian, Tromer, Eran, and Virza, Madars. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *Proc. IEEE Symp. Security & Privacy* (May 2014), pp. 459–474.

[4] Beresford, A.R., and Stajano, F. Mix zones: user privacy in location-aware services. In *Proc. Pervasive Computing and Communications Wrkshps* (2004), pp. 127–131.

[5] Bissias, George, Ozisik, A Pinar, Levine, Brian N, and Liberatore, Marc. Sybil-Resistant Mixing for Bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (2014), pp. 149–158.

[6] Cunha, Felipe D, Alvarenga, Davidysson A, Viana, Aline C, Mini, Raquel AF, and Loureiro, Antonio AF. Understanding interactions in vehicular networks through taxi mobility. In *Proceedings of the 12th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks* (2015), ACM, pp. 17–24.

[7] Dabrowski, Adrian, Pianta, Nicola, Klepp, Thomas, Mulazzani, Martin, and Weippl, Edgar. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference* (2014), ACM, pp. 246–255.

[8] De Mulder, Yoni, Danezis, George, Batina, Lejla, and Preneel, Bart. Identification via location-profiling in gsm networks. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society* (2008), ACM, pp. 23–32.

[9] Eagle, Nathan, and Pentland, Alex Sandy. Reality mining: sensing complex social systems. *Personal and ubiquitous computing 10*, 4 (2006), 255–268.

[10] Ficek, Michal, Pop, Tomáš, and Kencl, Lukáš. Active tracking in mobile networks: An in-depth view. *Computer Networks 57*, 9 (2013), 1936 – 1954.

[11] Freudiger, Julien, Manshaei, Mohammad Hossein, Hubaux, Jean-Pierre, and Parkes, David C. On non-cooperative location privacy: a game-theoretic analysis. In *Proceedings of the 16th ACM conference on Computer and communications security* (2009), ACM, pp. 324–337.

[12] Greenwald, Glenn, and MacAskill, Ewen. Boundless informant: the nsas secret tool to track global surveillance data. *The Guardian 11* (2013).

[13] Ho, Shen-Shyang, and Ruan, Shuhua. Differential privacy for location pattern mining. In *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS* (2011), ACM, pp. 17–24.

[14] Jaqaman, Khuloud, Loerke, Dinah, Mettlen, Marcel, Kuwata, Hirotaka, Grinstein, Sergio, Schmid, Sandra L, and Danuser, Gaudenz. Robust single-particle tracking in live-cell time-lapse sequences. *Nature methods 5*, 8 (2008), 695–702.

[15] Krumm, John. A survey of computational location privacy. *Personal and Ubiquitous Computing 13*, 6 (2009), 391–399.

[16] LEE RAINIE, SARA KIESLER, RUOGU KANG, and MADDEN, MARY. Anonymity, privacy, and security online.

[17] Markov, Andreĭ. Theory of algorithms.

[18] Miers, Ian, Garman, Christina, Green, Matthew, and Rubin, Aviel D. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *Proc. IEEE Symposium on Security and Privacy* (2013), pp. 397–411.

[19] Mulder, Yoni De, Danezis, George, Batina, Lejla, and Preneel, Bart. Identification via Location-profiling in GSM Networks. In *Proc. ACM Wrkshp on Privacy in the Electronic Society* (2008), pp. 23–32.

[20] Nillius, Peter, Sullivan, Josephine, and Carlsson, Stefan. Multi-target tracking-linking identities using bayesian network inference. In *Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on* (2006), vol. 2, IEEE, pp. 2187–2194.

[21] Qin, Zhen, and Shelton, Christian R. Improving multi-target tracking via social grouping. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on* (2012), IEEE, pp. 1972–1978.

[22] Rainie, Lee. The state of privacy in post-snowden america.

[23] Razavi, Sara Modarres. *Tracking Area Planning in Cellular Networks [Elektronisk resurs] : Optimization and Performance Evaluation.* Linköping, 2011.

[24] Sankar, Lalitha, Rajagopalan, S Raj, and Poor, H Vincent. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security 8*, 6 (2013), 838–852.

[25] Shokri, Reza, Theodorakopoulos, George, Le Boudec, Jean-Yves, and Hubaux, Jean-Pierre. Quantifying location privacy. In *Security and privacy (sp), 2011 ieee symposium on* (2011), IEEE, pp. 247–262.

[26] Soroush, Hamed, Sung, Keen, Learned-Miller, Erik, Levine, Brian Neil, and Liberatore, Marc. Turning off gps is not enough: Cellular location leaks over the internet. In *International Symposium on Privacy Enhancing Technologies Symposium* (2013), Springer, pp. 103–122.

[27] Sung, Keen, Levine, Brian Neil, and Liberatore, Marc. Location Privacy without Carrier Cooperation. In *Proc. IEEE Workshop on Mobile System Technologies (MoST)* (May 2014).

[28] Wong, V. W.-S., and Leung, V. C.M. Location Management for Next-generation Personal Communications Networks. *IEEE Network 14*, 5 (Sept. 2000), 18–24.

[29] Yang, Bo, and Nevatia, Ram. An online learned crf model for multi-target tracking. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on* (2012), IEEE, pp. 2034–2041.