The University of Sydney

School of Information Technology

INFO5993 Research Methods - Assignment I

Report on Database Searching Result, Annotated Bibliography, Proposing methodologies

Author:
Lin Han

Supervisor:
Dr. Vincent Gramoli

September 3, 2017


SIDERE MENS EADEM MUTATO

1 Introduction

Blockchain is the one of the most cutting edge technologies in the world nowadays. Not limited to digital currencies like Bitcoin, Etherum, and etc., blockchain enables innovations in wide range of fields, such as distributed cloud storage, digital identity, and smart contracts.

This report is trying to give a overview of the research base about blockchain and zero knowledge contingent proof, namely famous conferences and journals, research groups and people. Also, a list of possible unaddressed problems will be given to show possible research directions for my research project. In addition, five core articles or books in this area will be identified along with their annotated bibliography. At the end of this report, a summary of potential research methods will be given on the addressed questions.

2 Research Base

2.1 List of A*, A Conferences and Journals

A* conferences and journals:

1. ACM Symposium on Principles of Distributed Computing - PODC
2. ACM Symposium on Operating Systems Principles - SOSP
3. IEEE Transactions on Parallel and Distributed Systems - TPDS

A conferences and journals:

1. IEEE International Symposium on Network Computing and Applications - NCA
2. EuroSys
3. IEEE/IFIP International Conference on Dependable Systems - DSN

2.2 Research Groups

1. Initiative for Cryptocurrency and Contracts (IC3)

2. University of Sydney Concurrent Systems Research Group

3. Cornell University Systems and Networking Research Group

3 Research Problems

Based on the research and the current progress of RedBelly Blockchain by CSRG, there are three potential problems identified to research which can enrich current RedBelly Blockchain:

1. Is it possible to make use of an existing zero knowledge proof library in a blockchain system that does not require delay between block creation?

2. Is it possible to constraint the library in the number of participants to which messages should be broadcast so that the transaction remains consistent?

3. Is it possible to make the content of a transaction private (by using for example public key cryptosystems) so that only the payer and the payee can benefit from the transaction?

The above three problems mainly focuses on the zero knowledge contingent proof in blockchain, in detail, the possibility of its integration with RedBelly Blockchain and mobile devices.

4 Core Articles and Books

4.1 Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies Without Scripts[1]

4.2 On the Danger of Private Blockchains[4]

4.3 The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium[7]

4.4 The Blockchain Anomaly[6]

4.5 (Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains[3]

4.6 Zerocash: Decentralized anonymous payments from bitcoin[8]

4.7 The electronic cash system based on non-interactive zero-knowledge proofs[10]

4.8 Succinct non-interactive zero-knowledge proofs with preprocessing for LOGSNP[5]

4.9 Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs[2]

4.10 Zero Knowledge Contingent Payment[9]

References

[1] Wacław Banasik, Stefan Dziembowski, and Daniel Malinowski. *Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies Without Scripts*, pages 261–280. Springer International Publishing, Cham, 2016.

[2] Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer, and Madars Virza. Secure sampling of public parameters for succinct zero knowledge proofs. In *Security and Privacy (SP), 2015 IEEE Symposium on*, pages 287–304. IEEE, 2015.

[3] Tyler Crain, Vincent Gramoli, Mikel Larrea, and Michel Raynal. (leader/randomization/signature)-free byzantine consensus for consortium blockchains. *CoRR*, abs/1702.03068, 2017.

[4] Vincent Gramoli. On the danger of private blockchains. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*, 2016.

[5] Yael Tauman Kalai and Ran Raz. Succinct non-interactive zero-knowledge proofs with preprocessing for logsnp. In *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*, pages 355–366. IEEE, 2006.

[6] Christopher Natoli and Vincent Gramoli. The blockchain anomaly. In *Proceedings of the 15th IEEE International Symposium on Network Computing and Applications (NCA'16)*, pages 310–317. IEEE, Oct 2016.

[7] Christopher Natoli and Vincent Gramoli. The balance attack or why forkable blockchains are ill-suited for consortium. In *Proceedings of the 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'17)*. IEEE, Jun 2017.

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

[9] Bitcoin Wiki. Zero knowledge contingent payment, 2011.

[10] Fucai Zhou, Yuxi Li, Qingshi Zhou, Jingwei Miao, and Jian Xu. The electronic cash system based on non-interactive zero-knowledge proofs. *International Journal of Computer Mathematics*, 93(2):239–257, 2016.