The University of Sydney

School of Information Technology

INFO5993 Research Methods - Assignment I

Report on Database Searching Result, Annotated Bibliography, and Proposing methodologies

Author:
Lin Han

Supervisor:
Dr. Vincent Gramoli

September 18, 2017

SIDERE MENS EADEM MUTATO

1 Introduction

Blockchain is one of the most cutting edge technologies in the world nowadays. Not limited to cryptocurrencies 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, cryptocurrencies, and zero knowledge contingent payments, 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, several 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]

In this paper, the authors stated the possibility and method to create non-trivial efficient smart contracts using the standard transactions only by constructing efficient Zero-Knowledge Contingent Payment protocol for a large class of NP-relations. In particular, their protocol can be used to sell a factorization *(p,q)* of an RSA modulus

$$n = pq$$

.

The paper shows that their techniques can be used to implement the contract called ẗrading across chains.̈ Though their experiment is limited to theory construction, it still stated a constructive way to implement Zero-Knowledge contingent payments in Cryptocurrencies without Scripts. For my own research problems, their method may be a solution to RedBelly Blockchain whose scripts is still quite a draft now.

4.2 On the Danger of Private Blockchains[5]

In this paper, the authors explore the use of the Ethereum blockchain protocol in the context of a private chain where the set of participants is controlled. The paper argues that foundations are needed in order to precisely capture the guarantees of the consensus protocols of novel blockchain systems before one can deploy them safely. To this end, the authors define the termination of consensus to characterize when blockchain transactions commit and describe the existence of the Blockchain Anomaly in existing proof-of-work private chains. During the development of mobile wallet of RedBelly Blockchain, the same consideration is needed though mobile devices runs a light version of the whole node.

4.3 The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium[8]

In this paper, the authors build up their analysis on captures the tradeoff between the network delay and the mining power of the attacker needed to double-spend in the GHOST protocol with high probability. The authors quantify their analysis in the settings of the Ethereum testnet of the R3 consortium where we show that a single machine needs to delay messages for 20 minutes to double spend while a coalition with a third of the mining power would simply need 4 minutes to double spend with 94% of success. The article is a good argument on the non-forkable issue of blockchain.

4.4 The Blockchain Anomaly[7]

In this paper, the authors present the Blockchain Anomaly, an execution that they experienced when building their own private chain at NICTA/Data61. Even though this anomaly has never been acknowledged before, it may translate into dramatic consequences for the user of blockchains. Named after the infamous Paxos anomaly, this anomaly makes dependent transactions, like “Bob sends money to Carole after he received money from Alice” impossible. This anomaly relies on the fact that existing blockchains do not ensure consensus safety deterministically: there is no way for Bob to make sure that Alice actually sent him coins without Bob using an external mechanism, like converting these coins into a fiat currency that allows him to withdraw. We also explore smart contracts as a potential alternative to transactions in order to freeze coins, and show implementations of smart contract that can suffer from the Blockchain anomaly and others that may cope with it. Though the condition limits to specific private chain, the same anomaly may occurs during zero-knowledge contingent payments which is needed to be further investigated.

4.5 (Leader/Randomization/Signature)-free Byzantine Consensus for Consortium Blockchains[4]

In this paper, a new resilience optimal Byzantine consensus algorithm targeting consortium blockchains is proposed. To this end, it first revisits the consensus validity property by requiring that the decided value satisfies a predefined predicate. Then the paper presents a new modilar Byzantine consensus algorithm that relies neither on a leader, nor on signatures, nor on randomization. It consists of a reduction of multivalued Byzantine consensus to binary Byzantine consensus satisfying this validity property. In summary, the idea is to spawn concurrent instances of binary consensus but to decide only after a sequence of two of these instances. The binary consensus instances result in a bitmask that the reduction applies to a vector of multi-valued proposals to filter out a valid proposed value that is decided. At the end, the paper presents an underlying binary Byzantine consensus algorithm that assumes eventual synchrony to terminate. This is the base idea of RedBelly Blockchain's consensus, as well as the base rock that should be strictly followed when I develop the mobile wallet.

4.6 Zerocash: Decentralized anonymous payments from bitcoin[9]

This paper gives out the way to construct a full-fledged ledger-based digital currency with strong privacy guarantees using *zero-knowledge Succinct Non-interactive Arguments of Knowledge*(zk-SNARKs). In summary, they firstly formulated and construct *decentralized anonymous payments schemes*(DAP). And then, they build the Zerocash, a instantiation of the DAP scheme. In addition to its privacy features, their implementation gives out a relatively great performance - transaction less than 1kB and under 6ms to verify - compared to Zerocoin and is competitive with plain Bitcoin. The paper shows a constructive way to integrate zero-knowledge proof into cryptocurrencies. Also, the SNARKs lib can be an choice used in my own project.

4.7 The electronic cash system based on non-interactive zero-knowledge proofs[11]

The authors propose a electronic cash system utilized by zero-knowledge proof featuring CCA anonymity, unforgeability, traceability and no double-spending. The paper also gives out the proof on allowing multiple bank enrolling and user dynamically joining. The limitation of this paper obviously is that it targets at electronic cash system. But the methods it takes to make a transaction anonymous, but traceable inspires how I can adopt zero knowledge proof into RedBelly Blockchain.

4.8 Succinct non-interactive zero-knowledge proofs with preprocessing for LOGSNP[6]

In this paper, the authors show that if the prover and the verifier interacted in a (poly-logarithmic size) preamble phase, then some statements can be proved by relatively short noninteractive zero-knowledge arguments. In particular, the paper shows that in this model the satisfiability of a CNF formula

$$\Psi(w_1, \ldots, w_m)$$

of any size can be proved by a noninteractive zero-knowledge argument of poly(m) size, and the authors prove that for any language $L \in \mathcal{LOGSNP}$ the membership $x \in L$ can be proved by a non-interactive zero-knowledge argument of size polylog n. This is only a theory-proof paper illustrating a way using non-interactive zero-knowledge proof, but it can be considered as one of the alternatives integrated into RedBelly Blockchain. In this way, the traffic loads can be deduced during transactions. As a reference, Zerocash adopts this method.

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

This paper shows how public parameters for a class of non-interactive zero-knowledge proofs(NIZKs) can be generated by a multi-party protocol, such that if at least one of the parties is honest, then the result is secure (in both aforementioned senses) and can be subsequently used for generating and verifying numerous proofs without any further trust. The authors design and implement such a protocol, tailored to efficiently support the state-of-the-art NIZK constructions with short and easy-to-verify proofs. The applying assumption of this paper highly aligns with the Byzantine problems addressed by RedBelly Blockchain in which malicious parties exists. This paper may provide the solution to build zero knowledge contingent payment in RedBelly Blockchain.

4.10 Zero Knowledge Contingent Payment[10]

This wiki gives a brief introduction on how to make payments using Bitcoin which are released if and only if some knowledge is disclosed by the payee and to do this in a trustless manner where neither the payer or payee can cheat. In detail, a combination of a hash-locked transaction and a bitcoin-external protocol to set things up so that the data revealed in the hashlock release is the data they need is used in this process. Comparing to Bitcoin, RedBelly Blockchain's Scripts is still less function, however the way Bitcoin integrate Zero Knowledge Contingent Payment is a good reference for my project.

4.11 Elliptic Curve Based Zero Knowledge Proofs and Their Applicability on Resource Constrained Devices[3]

In this paper, the authors focus on the application of ZKIP protocols on resource constrained devices. They study well-established ZKIP protocols based on the discrete logarithm problem and transform them under the ECC setting. Then, they implement the proposed protocols on Wiselib and present a thorough evaluation of the protocols on two popular hardware platforms equipped with low end microcontrollers (Jennic JN5139, TI MSP430) and 802.15.4 RF transceivers, in terms of code size, execution time, message size and energy requirements. The limitation is that this paper is relatively old compared to the speed of hardware development. However, this work's results can be used as a good reference for me to integrate zero-knowledge proof into mobile wallet of RedBelly Blockchain.

5 Summary of Potential Research Method

All the three questions raised at the beginning of this report can be addressed using *Design (Prototyping) Reasearch* method, with proper *benchmarks*.

The process will go like the following:

$$Design- > Prototyping- > Test- > Benchmark- > Refine$$

During the benchmark, certain inputs and outputs will be expected according to the requirements, including timing, traffic, and etc.

In addition, for the third question *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?*, a formal theory discussion should be made.

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] Ioannis Chatzigiannakis, Apostolos Pyrgelis, Paul G. Spirakis, and Yannis C. Stamatiou. Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. 2011.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.