Second Year Report

Orfeas Stefanos Thyfronitis Litos

University of Edinburgh
o.thyfronitis@ed.ac.uk

Primary Supervisor: Prof. Aggelos Kiayias
Secondary Supervisor: Prof. Kousha Etessami

Abstract. This is a summary of the progress I have made in my PhD studies on Blockchains and Cryptography to date and the plan of action for the forthcoming year. It also includes a tentative proposal for my thesis topic.

1 Progress to date

1.1 Work during past year

This year I have steadily increased my knowledge in multiple fronts, as well as started dedicating more and more fruitful time to producing novel research. To begin with, I have studied content curation, a concept that refers to methods and techniques used to evaluate and rank user-generated content in social media platforms and online forums. Our work on this subject culminated in the authoring and successful publication of 'A Puff of Steem: Security Analysis of Decentralized Content Curation' [**?**]. In this paper we define an abstract system within which one can express a wide variety of concrete curation mechanisms. Furthermore, we leverage this system to analyse the quality of content curation of the Steemit[1] platform. This work exemplifies the lack of quality decentralised content curation mechanisms by highlighting the problems that arise by the use of the particular curation method employed by Steemit.

Furthermore, I have obtained a solid (but not yet complete) understanding of the 'Universal Composability' [1] framework, which is a cryptographic model designed to facilitate proving secure a cryptographic protocol that runs concurrenly with other protocols. This makes proofs and protocols composable in the sense that a protocol that has been proven UC-secure can be run securely on a system that runs many independent

[1] https://steemit.com

copies of this protocol and other arbitrary algorithms and protocols, not known at the time of proof.

In parallel I have studied several 2nd layer blockchain solutions, a set of techniques that aim to increase the scalability of blockchains by allowing multiple transactions to happen without having to add them to the blockchain. In particular, two parties that want to financially interact with each other often but do not trust each other can lock some of their funds in a new channel by adding a single transaction to the blockchain, transact an unlimited number of times within this channel off-chain and finally unlock the funds with the balance that corresponds to the latest state of the channel with another on-chain transaction. The knowledge gained through this study is currently being used in order to model and prove secure the 'Lightning Payment Channels' [2], the most widely used 2nd layer solution, within the UC framework. I am currently close to the completion of the proof of security and subsequently of this project.

Another related topic of interest for me has been understanding the blockchain itself. In this subject, I have studied several formalisations of blockchains (e.g. 'Bitcoin Backbone' [3]) and particular blockchain constructions (e.g. 'Ouroboros' [4]) and implementations (e.g. 'bcoin.js'[2]). My contribution consists of an ongoing project to design a new functionality that describes the requirements that any distributed ledger should fulfill in the simplest form possible.

Moreover, I have been aquainted with several cryptographic primitives and have developed and proven secure new ones to aid the formalisation of Payment Channels. Through personal and group work, I have amassed knowledge on low-level symmetric encryption primitives and hash functions and I understand the majority of concepts connected to the paradigm of simluation-based security.

Last but not least, I have developed my teaching and transferrable skills through creating exercises for other students and delivering presentations in conferences, workshops and meetings.

1.2 Meetings with supervisor

Since 1/5/2018, we have had approximately one meeting per 10 days. The vast majority lasted for one hour and were one-to-one. These meetings have greatly helped me resolve questions with regards to the cryptographic methodology in general, simulation-based security, and the UC framework usage in particular. They helped me gain intuition on why

[2] https://bcoin.io

certain approaches are taken and enabled me to develop my reasoning techniques with respect to them. Furthermore, Prof. Kiayias provided me with invaluable modelling ideas that catalysed the process of achieving our research objectives. Additionally, the Cryptography and Security group (headed by Prof. Kiayias) meets every week. Members of the group report on their progress there and interesting, informative discussions take place.

1.3 Conferences, seminars, workshops

I have attended or am attending the following:

- Real World Crypto 2019[3]
- Summer School on real-world crypto and privacy 2019[4]
- Security and Privacy group weekly seminar
- Symmetric Cryptography weekly workshop
- IOHK Miami Summit 2019[5]

1.4 Achievements

This is a list of my achievements for the past year:

- Gave a presentation on the basics of Bitcoin for SIGCoin in the University of Edinburgh.
- Gave an invited talk at 'Bitcoin Wednesday Amsterdam'[6] on 'Trust is Risk'.
- Gave a presentation at IOHK Miami Summit 2019[7] on 'Lightning Payment Channels'.
- Was accepted and gave a presentation at Tokenomics 2019[8] on 'A Puff of Steem: Security Analysis of Decentralized Content Curation'.
- Improved my teaching skills in my role as Tutor for the Computer Security course.
- Improved my skills in creating assignments for students in my Teaching Assistant role for the Computer Security course.
- Learned more LaTeX, JavaScript, Python and gained general programming knowledge.

[3] https://rwc.iacr.org/2019/index.html
[4] https://summerschool-croatia.cs.ru.nl/2019/
[5] https://iohksummit.io/
[6] https://www.bitcoinwednesday.com/events/bitcoin-wednesday-65/
[7] https://iohksummit.io/
[8] http://tokenomics2019.org/

– Learned the internals of Bitcoin.
– Contributed to the bcoin.js library.
– Contributed to https://blockchain-course.org/.
– Contributed to Prof. Kiayias lecture notes on Cryptography.
– Improved my knowledge on computer networks.

2 Plan of action

2.1 Goals for following year

My primary goal at present is to complete and submit the Payment Network paper. A number of other projects are under consideration. These include the following:

– A combination of content curation with off-chain transactions. The aim of this project is to create a social networking blockchain-backed platform similar to Steemit, but where not every vote interacts with the blockchain. This will enable scalability for the particular application of decentralised content curation.
– Completion of the project of simplifying the Ledger functionality. The aim would be to create a functionality that is equivalent to the current form of the Ledger functionality (as found in 'Ouroboros Genesis' [5]), but which would achieve a cleaner separation of the application and the consensus layer of ledgers. The usecase for this functionality would be for researchers that are interested in creating new blockchain applications but prefer not to understand in depth how the consensus layer works, but use a simple abstraction for it instead.
– Classification of decentralised content curation mechanisms. As we learned while working on Steemit, designing such mechanisms is no easy task. The solutions used in conventional centralised social networks are not directly applicable to the decentralised setting. An interesting frontier to pursue would be a characterisation of the design space of such algorithms. An interesting result of such research would be to reach some form of impossibility result with respect to what quality of curation is possible. Taking this a step further, we could collaborate with machine learning experts to look for satisfactory decentralised content curation mechanisms.
– Creation of virtual payment channels on Bitcoin [6]. A virtual payment channel is a channel that can be opened and closed without touching the blockchain; It uses two pre-existing payment channels as its 'blockchain'. This enables off-chain transactions between Alice and

Charlie, even though they do not have an on-chain channel. If they both have an on-chain channel with Bob, they first ask for the help of Bob to create a virtual Alice - Charlie channel that 'sits on top of' the Alice - Bob and the Bob - Charlie channels. Subsequently Alice and Charlie can perform off-chain payments to each other without requiring the intermediation of Bob for every single transaction. This construction is particularly hard (i.e. interesting) to achieve in Bitcoin, given the very limited, non-Turing-complete scripting language it uses.

– Design of a new blockchain that natively enables payment channels. Most existing fully decentralised blockchains were designed before the severe issue of scalability was discovered. Their design implicitly assumes that all transactions are to be put on-chain. As a result, most existing 2nd layer solutions use compatibility tricks and complex techniques that are hard to analyse and verify, not to mention the overhead they incur. There is a lack of research yet on how to design a blockchain from first principles that embraces the concept of 2nd layer solutions. This is a topic that inspires me, given that it can help blockchains achieve their full potential.

Of course it is impossible to achieve all the aforementioned goals in the next year. A more realistic goal would be to complete or have satisfactory progress in 3 of the projects described. I will consider a project as completed once a relevant paper that contains a satisfactory degree of results has been accepted in a respected conference.

2.2 Thesis completion plan

I aim to submit the Lightning Payment Network paper until the end of May 2019. Subsequently I would like to devote at most 6 months to writing and submitting a paper on designing virtual payment channels on Bitcoin. In the meanwhile I would like to pursue the Ledger functionality project with the aim of publishing another paper. After that, I plan to dedicate the rest of my studentship to the following two projects: that of classifying content curation systems and that of designing a payment network-enabled blockchain.

I expect that my thesis will be on formalising, securing and optimising 2nd layer payment networks. Given on the one hand that it is a new area of blockchain research and is likely to be the main means through which blockchains will manage to scale to the needs of a global market, and on the other hand that this past year I have thoroughly understood several

approaches to their construction and analysis, I believe that choosing this as the topic of my thesis is both a realistic target and a possibly influential and useful result for both the blockchain community and the general population.

References

1. Canetti R.: Universally composable security: A new paradigm for cryptographic protocols. In Proceedings 2001 IEEE International Conference on Cluster Computing: pp. 136–145: IEEE (2001)
2. Poon J., Dryja T.: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments
3. Garay J., Kiayias A., Leonardos N.: The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques: pp. 281–310: Springer (2015)
4. Kiayias A., Russell A., David B., Oliynykov R.: Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference: pp. 357–388: Springer (2017)
5. Badertscher C., Gaži P., Kiayias A., Russell A., Zikas V.: Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security: pp. 913–930: ACM (2018)
6. Nakamoto S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)