Zero-Knowledge Proofs for Blockchains

Sushmita Ruj
School of Computer Science and Engineering
University of New South Wales, Sydney, Australia
Email: sushmita.ruj@unsw.edu.au

***Abstract*—Zero-knowledge proofs (ZKP) are used to prove the correctness of computations without revealing any other information. Zero-knowledge proofs have origins in Interactive proof systems which were introduced in the 1980's. Last decade has seen a big leap from theory to practice, thanks to applications such as blockchains, anonymous credentials etc. Initially used for privacy preserving transactions in Zcash, these have been used in various ways in blockchain designs like Monero, ensuring anonymity of users, designing scalable Layer-2 solutions, verifiable computation in decentralised blockchain oracles and many more. These are being increasingly used in blockchain applications.**

The aims of this tutorial are as follows: (1) Provide background, history, evolution and theoretical foundations, (2) Discuss desirable properties of ZKP for blockchains and its applications, (3) Present some well known ZKP systems and show how they are used in blockchains, and (4) Introduce the audience to a myriad of open problems in this space.

The tutorial will be self contained, no knowledge of cryptography or blockchain will be assumed.

***Index Terms*—Interactive proofs, cryptography, blockchains, privacy, anonymity**

I. Introduction

Privacy is an important requirement in digital systems for regulatory reasons and protection against malicious attackers [1]. Therefore, privacy preserving computation has become very important. Zero-knowledge proofs (ZKP) not only provide privacy but verifiability for computations. ZKP were first presented in the seminal paper by Goldwaser, Micali and Rackoff [2] . There has been extensive research ever since. Some practical applications emerged as early as 1991 in group signatures and in the early 2000s with anonymous credentials. Zero-knowledge has recently got a big boost for verifiable computation and blockchains.

Currently ZKP is used in privacy preserving transactions in Cryptocurrencies such as ZCash [3], and Monero [4]. These are being extensively used in Layer-2 [5] solutions including ZK-Rollups. Decentralised blockchain oracles use ZKP and other derivatives. Zero-knowledge Succinct arguments of knowledge (SNARKs) are being extensively developed and implemented.

II. Content and Structure

The Half-Day Tutorial consists of the following sections.

A. Introduction and motivation

We start with a basic overview of blockchains [6]. This section provides many motivating examples of applications of zero-knowledge proofs in blockchains. We discuss the need of blockchain in privacy preserving and anonymous transactions. Discuss the motivation of ZCash and Monero. Then we will discuss Layer-2 blockchains, in particular about ZK-Rollups.

This motivation will set the stage for the foundation of ZKP.

B. ZKP Foundations

We discuss the history of ZKP [7] and provide definitions of Interactive proof systems and zero-knowledge property. We present one concrete classical construction from vertex coloring.

We then discuss non-interactive proof systems and how to use Fiat-Shamir transform to convert a interactive proof to a non-interactive proof. We then discuss the desirable properties of ZKP for the applications that we discussed in the introduction.

This leads to our discussion on Succinct Non-interactive ARguments of Knowledge (SNARKs) [8]. SNARKs are being extensively used in Blockchains and have been one of the hottest topic of discussion in cryptography and blockchains.

In this Section we discuss various desirable properties of SNARKs, importance of transparent set up and Scalable Transparent Argument of Knowledge (STARKs). We also discuss important properties like efficiency and post-quantum security.

This leads to our next discussion about SNARKs and their constructions. This discussion is important as we want to find the appropriate SNARK for a particular blockchain application.

C. SNARKs: Building blocks and designs

This section uses a simple example to demonstrate the construction of a SNARK. We show the steps to construct a SNARK. We discuss about Arithmetization, preprocessing SNARKS (and the different constructions). We discuss different types like Groth16 [9], Plonk [10], Bulletproofs [11], STARKs [12] highlighting the differences.

We provide background on the different paradigms for constructions from a functional commitment scheme and a interactive oracle proof. We provide a high level idea of the constructions.

Along with the mathematical ideas, we discuss about available softwares, libraries and source code.

D. ZKP applications for Blockchains

Equipped with the tools and techniques, we address how ZKP is used for the applications that we mentioned in the Introduction. We present a view of the ZKP systems used in

2833-292X/24/$31.00 ©2024 IEEE
DOI 10.1109/DSN-S60304.2024.00028

various applications, the type of construction used with reasons for the choice. We discuss about different variants of ZKP like recursive snarks and distributed snarks and their use in blockchains.

E. Conclusion and open Problems

This section discusses open problems in research, development and possible new applications. We delve into ZKP beyond blockchains. Though questions are allowed throughout the talk, we reserve sometime in this section for discussion.

III. Target Audience and Suitability to DSN

Papers and tutorials on blockchains have previously appeared in DSN. Though several aspects of blockchains have been addressed, a tutorial on Zero-knowledge proofs on blockchains have not appeared before. The importance of Zero-knowledge proofs are acknowledged by the blockchain and distributed computing/networks community, but there are not many compact tutorials which gives an overall idea about ZKP and its use in blockchains.

We hope that DSN audience working in other areas like communication, distributed computing and networks will use this in solving dependability, security and privacy problems in these systems.

Blockchain researchers/practitioners who are starting in this direction will find many open questions. Blockchain researchers already working on other aspects and applications will find how to improve privacy using ZKP and will be equipped with a toolset to use. Theory researchers specially in networks and distributed computing will find many ideas applicable to their research. We firmly believe that there are many more applications of ZKP in blockchains and other domains that can only be explored when we go beyond the Cryptography community.

IV. Speaker Bio

Sushmita Ruj is Faculty of Engineering Lead of UNSW Institute for Cybersecurity, IFCYBER and Senior Lecturer in the School of Computer Science and Engineering at UNSW, Sydney. Her research interests are in applied cryptography, post quantum cryptography, blockchains and privacy enhancing technologies. She designs practical, efficient, and provably secure protocols that can be deployed in real-world applications. She has won several competitive grants like Samsung GRO Award, NetApp Faculty Fellowship, Cisco Academic Grant. She is an Associate Editor of the Transactions on Information Forensics and Security. She has published in venues like IACR Crypto, PETS and AsiaCCS and IEEE and ACM Transactions. She was a key contributor in the Cybersecurity Working Group of the National Blockchain Roadmap of Australia and the first working group on Blockchains set up by the Reserve Bank of India. Before joining UNSW, she was a Senior Research Scientist at CSIRO's Data61 where she led a 1M AUD project on Data Sharing which received a Merit Award at the NSW Innovation Awards. She was previously an Associate Professor at Indian Statistical Institute and an Assistant Professor at Indian Institute of Technology, IIT, Indore and worked at the University of Ottawa, Canada and Lund University, Sweden. Sushmita is a senior member of both ACM and IEEE. More details can be found on her Homepage: https://research.unsw.edu.au/people/sushmita-ruj

References

[1] M. Conti, S. K. E, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018. [Online]. Available: https://doi.org/10.1109/COMST.2018.2842460

[2] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, R. Sedgewick, Ed. ACM, 1985, pp. 291–304. [Online]. Available: https://doi.org/10.1145/22145.22178

[3] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," *IACR Cryptol. ePrint Arch.*, p. 349, 2014. [Online]. Available: http://eprint.iacr.org/2014/349

[4] N. V. Saberhagen, "Cryptonote v 2.0," 2013.

[5] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: a survey," 2021.

[6] A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction*. Princeton University Press, 2016. [Online]. Available: http://press.princeton.edu/titles/10908.html

[7] A. Nitulescu, "zk-snarks: A gentle introduction," https://www.di.ens.fr/ nitulesc/files/Survey-SNARKs.pdf.

[8] J. Thaler, "Proofs, arguments, and zero-knowledge," *Found. Trends Priv. Secur.*, vol. 4, no. 2-4, pp. 117–660, 2022. [Online]. Available: https://doi.org/10.1561/3300000030

[9] J. Groth, "On the size of pairing-based non-interactive arguments," in *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, ser. Lecture Notes in Computer Science, M. Fischlin and J. Coron, Eds., vol. 9666. Springer, 2016, pp. 305–326. [Online]. Available: https://doi.org/10.1007/978-3-662-49896-5_11

[10] A. Gabizon, Z. J. Williamson, and O. Ciobotaru, "PLONK: permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge," *IACR Cryptol. ePrint Arch.*, p. 953, 2019. [Online]. Available: https://eprint.iacr.org/2019/953

[11] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*. IEEE Computer Society, 2018, pp. 315–334. [Online]. Available: https://doi.org/10.1109/SP.2018.00020

[12] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," *IACR Cryptol. ePrint Arch.*, p. 46, 2018. [Online]. Available: http://eprint.iacr.org/2018/046