Compute Offchain, Verify Onchain: How to Build zk-DApps with Circom and ZoKrates

Planned duration: 120 minutes.

Abstract, objectives, and motivation

Zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) can mitigate the privacy and scalability limitations of blockchains and enable novel application contexts for decentralized applications (DApps). They enable the verification of off-chain computations (VOC) on private inputs, such as verifying assertions on personal data without revealing the data itself. Moreover, by verifying only a small proof of a potentially complex off-chain computation on-chain to attest its correctness, transaction costs can be reduced significantly. Zk-SNARKs find use in various applications and products, particularly in critical blockchain infrastructure building blocks like rollups, coprocessors, and bridges.

Circom and ZoKrates are high-level domain-specific languages supplemented by toolkits that simplify the process of specifying zk-SNARK-based VOCs for non-crypto-expert developers, as they conceal some of the programming complexities. In this tutorial, participants will learn the following:

- How zk-SNARKs can be applied to solve imminent problems of DApps, e.g., private data verification and transaction cost reduction.
- Which cryptographic hashing and signature mechanisms are supported by Circom and ZoKrates off the shelf
- Challenges (e.g., branching) as well as commonalities and differences between domain-specific languages for writing zk-SNARK circuits
- Create an arithmetic circuit with the Circom and ZoKrates domain-specific languages and ways to make circuits efficient (e.g., using non-deterministic advice)
- Use the ZoKrates CLI to support the deployment workflow including the generation of proving and verification keys, and the automated creation of an Ethereum verification smart contract.
- Integrating zk-SNARKs into your intended application.

Tutorial outline, timeline and intended audience:

The tutorial starts with an overview of the fundamental concepts required to gain a better understanding of zk-SNARKs. After acquiring this foundation, the audience will be introduced to various use cases where zk-SNARKs are applied to solve real-world problems. In the next step, they will be introduced to the concept of domain specific languages for the efficient generation of zk-SNARK proving and verification programs as the example of two common frameworks, Circom and ZoKrates. Finally, the tutorial concludes with a one-hour hands-on exercise that guides the audience through the whole development process of zk-SNARKs. This includes the definition of an arithmetic circuit for a certain claim, how to perform a secure setup phase, the generation of an Ethereum verification smart contract, and the execution of proof programs. By following this tutorial, you will be able to take your DApp development to the next level.

The table below provides a detailed breakdown of the workshop's different blocks and activities.

Block	Description	Duration
Motivation & Concept	- Verifiable off-chain computations - zk-SNARK properties - Overview of developing a zk-SNARK-based program - Q&A	25 Minutes
Applications	- Blockchain infrastructure: rollups, coprocessors & bridges - Other use cases: identity & federated learning - Q&A	30 Minutes
Break	Small break between presentation and hands-on activity	5 Minutes
Hands-On Exercises	- Commonalities and differences of Circom and ZoKrates Development a Circom and ZoKrates program - Simulation of a trusted setup ceremony - Ethereum verification smart contract - Automation of the proof generation process	60 Minutes

The target audience for this tutorial includes blockchain researchers and developers who are new to the topic of zero-knowledge proofs, as well as those who are already familiar with the subject and seeking additional insight on how to best leverage zk-SNARKs. We assume that attendees have experience in smart contract development, particularly for Ethereum, and possess basic programming skills.

Name, affiliation, and a short biography of each tutorial speaker

- **Alvaro Alonso (TU Berlin)** - Alvaro has a double degree in Business Administration, from UC3 Madrid, and in Computer Science from TU Berlin, where he subsequently completed his Master's degree in Computer Science. Early in his studies Alvaro got interested in zk-SNARKs and has been using ZoKrates since 2019. He joined the Information Systems Engineering (ISE) department in 2022 and is currently working as a research assistant in the ZoKratesPlus project. ZoKratesPlus is a publicly funded validation initiative on ZoKrates, an open-source technology for ZKPs developed at TU Berlin. In the past, Alvaro has worked as a data scientist and software developer for startups and large corporations. Currently, Alvaro focuses on the application and scalability of zero-knowledge proofs inside and outside blockchains. He is also interested in topics such as software architectures, distributed systems, cloud computing and quantum computing.
- **Dr. Jonathan Heiss (TU Berlin)** - Jonathan is working as a senior researcher in the Information System Engineering group. His research focuses on novel applications of zero-knowledge proofs (ZKP) and blockchains and their integration into real-world systems. His domains of interest include carbon emission management, decentralized identity, and federated learning. His research has been honored with the Best Paper

award at the International Conference on Service-oriented Computing in 2021. Jonathan has served as a TPC member for the IEEE International Conference on Blockchain since 2020, for the International Conference on Mathematical Research for Blockchain Economy from 2024, and is a scientific reviewer for various international Journals. Recently, he joined the academic advisory board of the International Association for Trusted Blockchain Applications (INATBA). He is also leading the ZoKratesPlus project.

- **Dr. Johannes Sedlmeir (SnT, University of Luxembourg)** - Johannes is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. He received his M.Sc. in mathematical physics and his Ph.D. in information systems engineering. In his research, he focuses on the effective use of emerging technologies organizations. He does so by designing innovative IT artifacts based on components such as blockchains, digital identity attestations, and (succinct) zero-knowledge proofs, e.g., in the context of financial applications, supply chains, mobility, healthcare, and e-government. He regularly serves as a reviewer for various journals and as an associate editor and technical committee member at different conferences. His research has been published in international journals such as Business & Information Systems Engineering, Electronic Markets, Information & Management, and the Journal of Network and Computer Applications.

A description of any previous tutorial experience of the speaker(s) and past versions of the tutorial

The 'Motivation & Concepts' and 'Applications' sections are sourced from a guest tutorial by Jonathan for the 2nd RedChain-Lab Workshop. At the 2023 Programmable Crypto Conference, Alvaro presented a talk on automating the proof generation process of ZoKrates proofs in a memory-safe manner. This will be covered in the final part of the 'hands-on' section. In the last 18 months, both have been consolidating their knowledge of ZoKrates through concise and easy-to-understand tutorials for the ZoKratesPlus research project. Jonathan has more than 5 years of experience teaching about verifiable off-chain computations, while Alvaro has 2 years of experience in programmable cryptography. Lastly, ZoKrates originated at ISE and its creator, Jacob Eberhardt, has been given many tutorials since its inception. The collection of his experiences is also reflected in our material to guarantee a smooth learning experience for the participants. Johannes has experience with building zk-SNARK-based applications using Circom in several domains, such as the energy sector, federated learning, and digital identity wallets. He has also taught multiple courses for computer science and business students at the undergraduate and graduate levels about the foundations and applications of zk-SNARKs.

State if a similar tutorial has been offered in other conferences (last two years) and how your tutorial differs

Although tutorials have been offered dealing with privacy and scalability issues related to blockchains and discussing corresponding solution approaches in the previous two years, this would be the first tutorial at ICBC that offers hands-on experience in developing zk-DApps. Regarding other conferences, this is the first dedicated zk-DApps tutorial to our knowledge. There are other tutorials focusing on fundamentals of zk-SNARK technology like circuit optimization (without the DApps-part). Similarly, other tutorials on DApps (without the zk-part) have been given.