Replies-ZKP_Bootcamp_Week_1

how schwartz-Zipple Lemma make a proof non interactive?

Schwartz-Zippel lemma is a basis of zkSNARKs which are non interactive.

Fox Reymann | 04/24/2023

I am sorry for easy question.Why prover and verivier is needed??

in ZKPs prover is a user that wants to prove something w/o giving all knowledge of the subject. Verifier accepts the prove. Let's say you want to enter an over 18 nightclub w/o showing your ID with full details. With ZKPs you (prover) can prove that you're over 18 to the bouncer (verifier).

Fox Reymann | 04/26/2023

I get the impression that Starknet has a less developed ecosystem. Will there be more DeFi ecosystems such as lending and stable DEX?

`stable` DEX: https://app.jediswap.xyz/#/swap. Money market: https://testnet.artemis.zklend.com/markets Sneak peak of 100 apps under development: https://community.starknet.io/t/applications-for-round-1-of-early-adopter-grants-eag/54273

Fox Reymann | 04/27/2023

I heard that STARKs use publicly-available randomness to generate parameters,I would like to know more in detail.please tell me some reference.

We are going to cover STARK theory in Week 4. Best reference: https://eprint.iacr.org/2018/046.pdf

Fox Reymann | 04/26/2023

I read there is a statement that Cairo is CASM, but is it compatible with WASM?

it surely is not

Fox Reymann | 05/01/2023

I think there were a total of 46 homework questions yesterday, do you have model answers for each?

There are 6 Cairo 1 exercises in yesterdays homework:
https://github.com/ExtropyIO/ZeroKnowledgeBootcamp/tree/main/cairo
We are going to provide answers in due course

Fox Reymann | 05/02/2023

I would like to know why you selected Cairo and Starknet in this course out of so many zk's available?

Check l2beat.com. Starkware stack is by far the largest ZK L2. Combine dYdX, ImmutableX, Apex, Sorare on StarkEx + Starknet mainnet

Fox Reymann | 04/24/2023

If there were no trusted set up, how they prove the transaction is valid or not.

STARKs use publicly-available randomness to generate parameters, eliminating the need for a trusted setup in the prove.

Fox Reymann | 04/26/2023

In general, it takes a lot of courage for a developer to learn a new language, what do you think are the motivations of the developers who build on Starknet?

I think it's all about credibility and consistency of delivery. StarkWare has ZK-Rollups that have achieved high performance in various market conditions. As you know, StarkEx is a private rollup functioning with ImmutableX, dYdX, and other projects that have proven reliable and are working well. This strongly signals that StarkNet could be one of the leading ZK-Rollups across the ecosystem.

Remember, zkEVMs will never as performant as DSLs build for ZK virtual machines.

Fox Reymann | 04/27/2023

Is the most imprtant part of zkstark is the size of 1 Tx??

I would say no trusted set up requirement, better scalability (data size) and quantum. resistance are biggest advantages

Fox Reymann | 04/26/2023

Is there a reason as to why ZK languages do not support many data types?

Cairo 1 has felt, integers, bools, short strings, tuples, structs, enums, arrays. What are you missing? Any data types can be build on top of felt.

Fox Reymann | 04/27/2023

is there any solutions for homework available so that we can check our solutions?

if you make code compile without cheating it should be ok. but we will provide answers later during the course.

Fox Reymann | 04/27/2023

is this global merkle tree of commitment notes similar to verkle tree in eth2 roadmap?

Verkle trees are an upgrade to Merkle trees, Merkle trees work on hash commitments, Verlke trees work on polynomial commitments

Fox Reymann | 05/02/2023

Just to double check, a Zcash shielded transaction encrypts both the transfer amount and the sender & receiver addresses, right?

correct

Fox Reymann | 05/02/2023

The cairo foundry doesn't seem to have changed in the last 3 months. is it common to utilize hardhat?

https://github.com/open-dust/cairo-foundry
cairo-foundry is for Cairo 0. We are now moving to Cairo 1. Please check Protostar.

Fox Reymann | 05/01/2023

What are some differences for implementing a zero-knowledge based privacy-preserving blockchain for UTXO vs account model?

in account-based currencies, even if balances are hidden or encrypted, it is difficult to hide the balance change of a particular user as those whose balances do not change can be easily ruled out from potential spenders. If (almost) all balances are changed, it is again too expensive. If only a few balances are changed, the anonymity set is not full.

ref: https://dusk.network/uploads/Full-privacy-in-account-based-cryptocurrencies.pdf

Fox Reymann | 05/02/2023

what are the differences between poly-log(N) and log(N)

log(n) is just a logarithm on f, poly-log(n) is polynomial in the log of n (https://en.wikipedia.org/wiki/Polylogarithmic_function)

Fox Reymann | 04/25/2023

What are the drawbacks of Bulletproofs, such as vulnerabilities?

Performance is not a good as SNARKS, no quantum secure.

Fox Reymann | 05/02/2023

What does "Key: 500GB" mean for SNARKs? Is that part of the proof size?

I think this is proving key size. A zk-SNARK consists of three algorithms G, P, V defined as follows: The key generator G takes a secret parameter lambda and a program C , and generates two publicly available keys, a proving key P , and a verification key V

Fox Reymann | 04/26/2023

What does it mean by "computes a witness for the compiled program"?Do you have to setup it everytime for a unique witness value?

Computing the witness is done after the trusted setup, so no second trusted set up is required. But yes, you have to compute new witness for every new input value.

Fox Reymann | 04/25/2023

what is the break out rooms and teams?

you gonna be assigned into a group with 3-4 more students and you're going to have a time to work on homeworks together in breakout rooms, this is a feature of Zoom

Fox Reymann | 04/24/2023

what is the current legal status of Tornado Cash?

we focus on clearly technical topics here, sorry, don't want to start a political debate

Fox Reymann | 05/02/2023

what is the name of this programming language ? main.zok ?

ZoKrates, like the tool

Fox Reymann | 04/25/2023

What's difference between ZoKrates and circom in terms of developing apps? (expression, cost, etc...)

ZoKrates is a toolbox for zkSNARKs on Ethereum. Circom is general ZKP language for all ZKP usecases. Can also be used on Ethereum. I would say Zokrates is simpler to start with (hence with start with it ;))

Fox Reymann | 04/26/2023

what's the difference between STARK and SNARK ?

many, in general proof is created in a different way. we are going to explain both and compare them

Fox Reymann | 04/25/2023

When and how is the zero-knowledge proof part come in, in the ZKRollup process?

Zero-knowledge rollups (ZK-rollups) bundle (or 'roll up') transactions into batches that are executed off-chain. Off-chain computation reduces the amount of data that has to be posted to the blockchain. ZK-rollup operators submit a summary of the changes required to represent all the transactions in a batch rather than sending each transaction individually. They also produce validity proofs to prove the correctness of their changes.
ref: https://ethereum.org/en/developers/docs/scaling/zk-rollups/