Advanced Noir programming

A learning group for ZK and SNARK application development

Daniel Szego
In: https://www.linkedin.com/in/daniel-szego/

Logistics: ZK Learning Group

Every month, third thursday in 2025, from 18 (CET)

One hour, presentation + short discussion

Different topics on zero knowledge proof,

- mostly from programmer and application developers perspective
- with some theory

Coordination:

- Discord channel: LF Decentralized Trust
  https://discord.com/channels/905194001349627914/1329201532628898036
- Meetup.com: https://www.meetup.com/lfdt-hungary/events/305634614/
- Repo with all the contents:https://github.com/LF-Decentralized-Trust-labs/

https://github.com/Daniel-Szego/zk-leraning-group

Quizzes and small programming challenges, LFDT merchs at the end

Logistics: Hunting for the SNARK

February - Introduction, Theory : Definitions and building blocks

March - Theory : Polynomial commitments

April - Theory : Interactive oracle proofs

May - Programming : Circom

June - Programming : Circom

July - Programming : Noir - basics

August - Programming : Noir - advanced

September : Applications : Off-chain transaction

October : Applications : Proving solvency

November : Applications : Rollup

December : Wrap up, Applications

Subject to change based on community discussion ….

Agenda

- *zkSNARK*
- *Aztec and Noir*
- *Noir examples: data*
- *Noir examples: control structures*
- *Noir examples: extensions, libraries*
- *Noir in applications*
- *Challenge*
- *Links, resources, literature*

(zk)SNARK - Succinct Non-interactive ARgument of Knowledge

Computation: arithmetic circuit : *C(x, w) -> F*

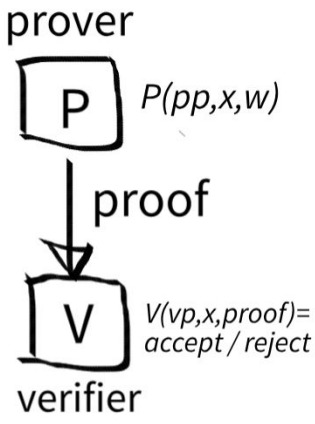
- *x* public input
- *w* private input, witness
- high level computation
- arithmetic circuit
- polynomials

Prover algorithm: *P (pp, x, w) -> proof*

Verifier algorithm: *V (vp, x, proof) -> accept / reject*

Properties:

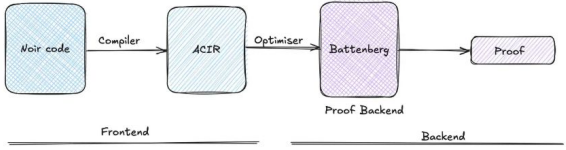
- *Succinct:*
- *Complete:*
- *Knowledge sound:*
- *Zero knowledge*



Aztec and Noir

Noir:

- Rust like syntax
- Limited cryptographic experience
- Intermediate representation (ACIR)
- Different backends
- Platform agnostic, abstract circuit
- Different proving backends:



Aztec:

- L2 rollup system on ethereum
- Private function possibility
- Executing on user device
- Public and private state
- UTXO Ledger - private
- Account balance based ledger - public

https://github.com/noir-lang/awesome-noir/

Noir examples - data

Data types

Simple types:

- Fields (256 bit prime field),
- integers,
- booleans
- (strings)

Complex type:

- Arrays
- Tuples
- Structs

All types are complied to fields

Data types https://noir-lang.org/docs/noir/concepts/data_types

Online playground https://www.noir-playground.app/

Noir examples - control structures

Control structures:

- If then
- For loops
- While loops (*unconstrained*)
- General loops (*unconstrained*)

Logical operations: Logical, bitwise, comparisons

Functions

- main function
.. subfunction
- Unconstrained function*: no constraints, no circuit generated*
- Methods

Control structures: *https://noir-lang.org/docs/noir/concepts/control_flow*

Online playground *https://www.noir-playground.app/*

Noir examples - extensions, libraries

Additional data type :

- BigNum
- Floating number
- Complex numbers
- Fixed points
- Date and time

Data type manipulation:

- Matrix
- Statistics
- Text

Cryptography:

- Elliptic curve
- Hashes
- Encryption
- Signatures

Awesome Noir *https://github.com/noir-lang/awesome-noir*

Online playground *https://www.noir-playground.app/*

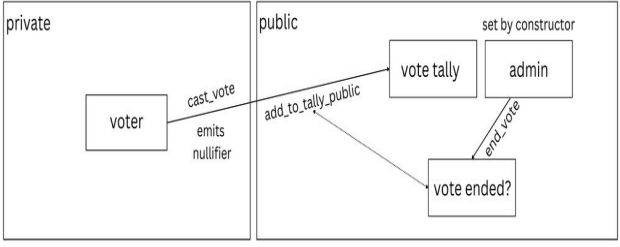
Noir in applications

Develop business logic for ZK calculation

E.g. Simple Fibonacci calculation

Custom application:
- custom backend prover
- NoirJS
- Solidity prover

Aztec smart contract:
- Noir contracts in Aztec
- Aztec utils for Noir
- Storage contract
- Public, private, internal functions
- Public and private state



Aztec starter kit: https://github.com/AztecProtocol/aztec-starter

Challenge

Developer challenge:

Develop a sudoku puzzle with
the help of Noir

Links, Resources, Literature

Aztec starter kit
https://github.com/AztecProtocol/aztec-starter

Noir online playground
https://www.noir-playground.app/

Noir documentation
https://noir-lang.org/

Awesome Noir, repository with examples
https://github.com/noir-lang/awesome-noir

Noir Explained: Features and Examples
https://oxor.io/blog/2024-06-18-noir-explained-features-and-examples/

NoirJS
https://noir-lang.org/docs/reference/NoirJS/noir_js/

Happy Hunting for the SNARK :)

Q & A

Daniel Szego

In: https://www.linkedin.com/in/daniel-szego/