



## SECURITY REVIEW

X

**test-new**

Prepared for  
Prepared by  
Dates Audited

test-new  
Audit Hunt  
September 2 - September 10, 2023

## Review deliverables for ZK tutorial

I have been asked by the grants team to review <https://github.com/w3f/Grants-Program/blob/master/applications/zkverse.md>

Deliverable 1 Report: <https://github.com/w3f/Grant-Milestone-Delivery/pull/835>

Deliveries <https://github.com/Zkvers/substrate-zk/blob/master/zk-tutorials/ZKSNARKS.md>

<https://github.com/Zkvers/substrate-zk/blob/master/zk-tutorials/ZKSNARKS.md> and

[https://github.com/Zkvers/substrate-zk/blob/master/zk-tutorials/proof-system/groth16/theory\\_to\\_practice.md](https://github.com/Zkvers/substrate-zk/blob/master/zk-tutorials/proof-system/groth16/theory_to_practice.md) as part of the milestone 1 for

<https://github.com/w3f/Grants-Program/blob/master/applications/zkverse.md>

## Reimplement TXQR in Rust

We want an implementation of TXQR in Rust for Parity signer and probably subkey. We'd encourage some public discussion of the exact design features of TXQR, since maybe we'd find some small improvements.

<https://github.com/maciejhirsz/uos/issues/7> <https://github.com/paritytech/parity-signer/issues/457>  
<https://github.com/paritytech/parity-signer/issues/320>