In This Series

End-to-end dissection of how a virtual currency mixer (like Tornado Cash) is constructed. Topics include fundamental cryptographic primitives and implementation.

• Cover concepts of finite fields, cryptography, and zero-knowledge proof.

• Show full-stack smart contract development workflow (Languages: JS, Solidity, Circom) .

• With ZK proofs, data on blockchain is no longer public (obfuscated).

Disclaimer

• Notice: On August 8, 2022, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash for uncontrolled laundering. Decision follows May 6 designation for Blender.io.

• Declaration of non-association

• Declaration of compliance with OFAC

• Copyrighted material

• No assumption of responsibility for loss

Purpose

Demonstration of the inner workings of a virtual currency mixer:

• Allows the public to identify similar services in the future.

• Increases technical knowledge in modern cryptography and its application in smart contract programming.

• Introduces a full-stack workflow for smart contract developers working on other decentralized applications.

• Bring privacy to good use cases.