Hello everyone! Let me present you MixEth

, which is an efficient trustless coin mixing service for Ethereum. This is a joint work with@nagydani.

Note:

this is an early-stage work, hereby we just release the draft paper. Implementation, security proofs and many more are yet to come!

The basic idea is that unlike previous proposals (Möbius and Miximus by @barryWhiteHat) which used linkable ring signatures and zkSNARKS respectively for coin mixing, we propose using verifiable shuffles for this purpose which is much less computationally heavy. Additionally we retain all the strong notions of anonymity and security achieved by previous proposals consuming way less gas.

The protocol in a nutshell: senders need to deposit certain amount of ether to ECDSA public keys. These public keys can be shuffled by any receiver at most once using a verifiable shuffle protocol. The shuffle is sent to the MixEth contract and anyone can check whether their own public key is shuffled correctly (i.e. it is included in the shuffle). If one creates an incorrect shuffle than it can be challenged and malicious shufflers' deposits are slashed if challenge is verified. If there are at least 2 honest receivers then we achieve the same nice security properties achieved by Möbius and Miximus. At the end of the protocol receivers can withdraw funds from a shuffled public key which are public keys with respect to a modified version of ECDSA.

For more details, have a look at thedraft version of the MixEth paper.

Any feedback, comment, critique is more than welcome!