In this post I would like to introduce and explain briefly ShareLock, which we believe,@omershlo and me, that can bring privacy-enhanced transactions to Ethereum TODAY

.

For more details please have a look at thepaper and the Github repo.

tl,dr: ShareLock is a novel coin mixer, which unlike previous proposals is deployable on today's Ethereum. It does not rely on account abstraction or relayer services.

A few weeks ago @HarryR posted a super exciting, plain-spoken and honest post here: Privacy/Anonymity on Ethereum is Doomed This is a good start if you are not familiar with the privacy issues we are having on Ethereum.

Ethereum still lacks a commonly used privacy-enhancing overlay. For instance, in this regard, Bitcoin is ahead of Ethereum, since we can use Chaumian CoinJoin developed by Wasabi wallet. Even if there were several proposals, they did not work and did not get traction. And this is not by accident.

[

|643px;x391px;

929×565

]
(https://lh6.googleusercontent.com/gU2nzKMyEEUMb1JKN_8GwuVqN_TvpPRuYP2MyZRLyStnltfuSvIU8SRRw3gtE0KkANJR1xgDWjnUpNXVfh7ANff9SE9NgIKSgVHzUl0CvaUDmF9o6jDp5eNFkBK_pb-m8cgo)

Möbius, Miximus by @barryWhiteHat, MixEth and other mixer proposals work as follows:

1. Users deposit equal amount of coins into a smart contract.
2. They withraw mixed coins from a fresh address by providing some non-linkable cryptographic proof (zkSNARK, ring signature etc.) to prove that they deposited previously.

The problem with this design is that at step 2. transactions cannot be issued without leaking privacy as of today. Either Alice funds herself the fresh address or she sends the tx via a relayer service. The details and the framework for a relayer service is not established. OR

we could wait for the account abstraction which would allow recipients to pay for the incurred gas costs. Account abstraction might come in 2020, 2021, … who knows?!

ShareLock chose a different design:

[

|519px;x422px;

678×551

](https://lh4.googleusercontent.com/a2nMN-oJnSmB7z1yr556dK5NyuQojoWGahdu7eX6UO677qBUaB9eQQdxHuZZi7PcqzwUMkzIVIITXuZf10ykgbfT-V6DnUPFas49y9ZUcMVK3gklCPy2mvtIM_BVFdstPtwUOLBFYl4)

Users still need to deposit to a contract, this seems inevitable in mixing for account-based cryptocurrencies, since txs cannot have multiple outputs. Then they run off-chain a distributed key generation (DKG) protocol and threshold sign the list of the addresses derived from the threshold public keys.

Any of the participants, or say a wallet company, we call this party an activator could poke the contract with the threshold signed transaction to make the contract sending out the mixed coins to the addresses yielded from the DKG.

If parties are unable to threshold sign the "poke" transaction, then after a time-out they are able to withdraw their dirty coins (unmixed) back to their original addresses.

Since security is proven in the UC framework one could just pick her favourite threshold ECDSA protocol. In the paper we sticked to the GG'19 paper. However one could also use threshold BLS in order to avoid interactivity in the off-chain signing phase.

How does ShareLock relate to other privacy-enhancing solutions? [

jpg-large

985×206 13.3 KB

](https://ethresear.ch/uploads/default/original/2X/6/61326043fdfa0ac72e7b7dd3429a7a7782cb4b96.jpeg)

ShareLock provides k-anonymity and it consumes altogether cca.140k gas. Aztec gives confidential transactions, while Zether provides both. Currently an Aztec tx consumes cca. 900k gas, while Zether around 7.2M gas (almost fills an entire block).

We envision ShareLock as a useful plugin for wallets, where one would not only have a Send button but also a Send mixed coins button. The common and widespread use of such a privacy-enhancing overlay in the community could remarkably ameliorate privacy for everyone in Ethereum.

Please let us know your thoughts, comments, questions, critiques!