I thought this might be share-worthy.

Benedikt Bunz (co-author of Bulletproofs), Dan Bohen et al. proposedZether, the first privacy mechanism built specifically for Ethereum, i.e. account-based smart contract platforms. All notable blockchain privacy mechanisms developed so far (the authors refer to 10 of them), were designed for Bitcoin/UTXO-based chains.

Zether provides both confidentiality (by hiding payment amounts) and anonymity (by hiding the identities of senders and recipients).

The mechanism is practical today (no changes to Ethereum protocol required). The authors implemented it as an Ethereum smart contract and a single transaction costs 7M+ gas

, but if two already discussed EIPs were to be implemented, it would go down to 1.7M and also the contract itself could be further optimized.

crypto.stanford.edu

[

](https://crypto.stanford.edu/~buenz/papers/zether.pdf)

zether.pdf

583.80 KB