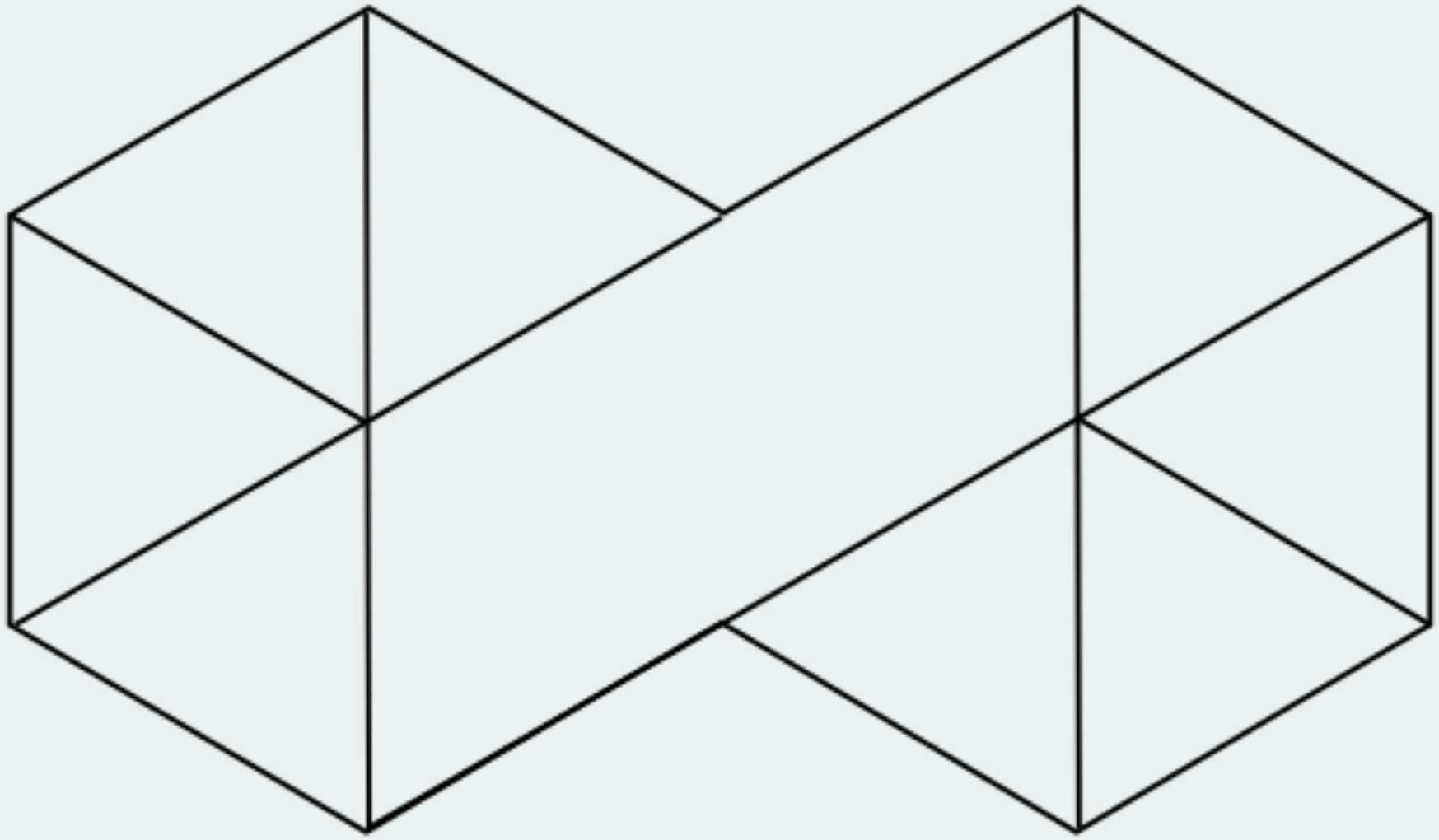
ethereum

vienna

Possibilities of homomorphic encryption



RIAT

RESEARCH INSTITUTE FOR ARTS AND TECHNOLOGY

ethereum

vienna

Possibilities of homomorphic encryption

Agenda

General Introduction

Updates

Johann Höchtl: Homomorphic Encryption

Socialising

ethereum

vienna

Updates

May Meetup

Together with first **Monero Austria** meetup (+ Dogecoin)

May 11th @RIAT

Justin Ehrenhofer (Monero Dev):

RingCT and other privacy mechanisms

(will also be possible with Ethereum after Metropolis)

Workshops

Too many no-shows last time!

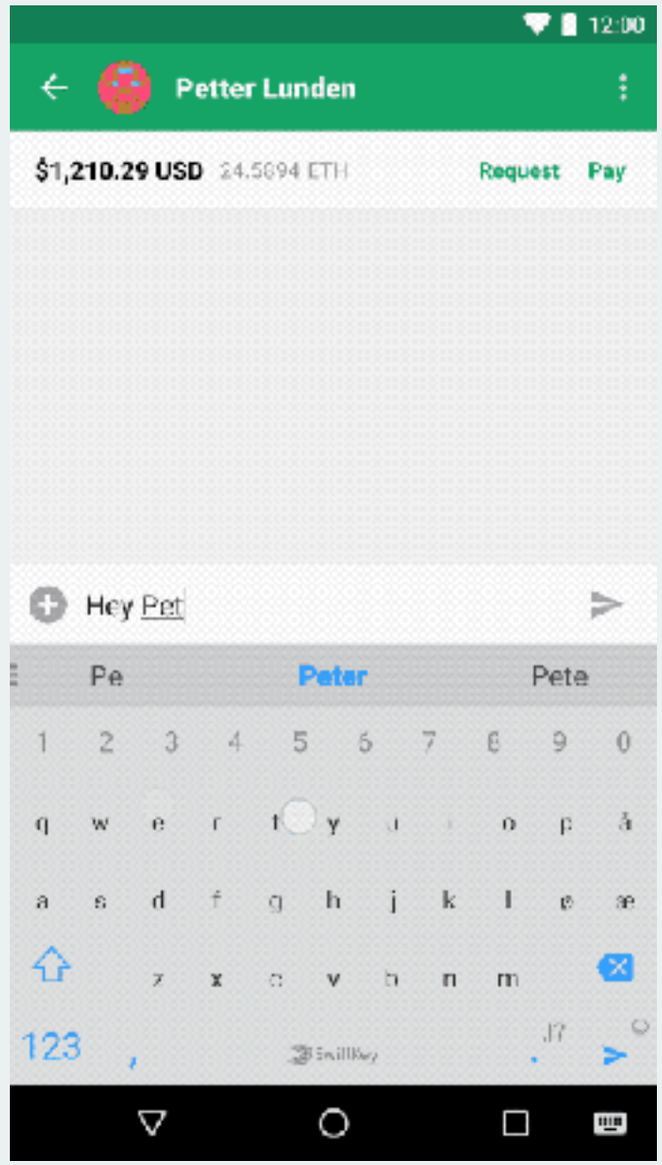
Next Beginner Workshop: May 6th

Next Advanced Workshop: May 27th

- truffle framework
- epm

Token

Mobile ethereum wallet from Coinbase



Similar to status.im but:

- No light client
- Messaging is centralised (encrypted)
- Chatbot for sending / receiving ether
- not web3.js yet (but planned)

Metropolis

June or July

Rise of Hashrate delays ice age

Implements 10 EIPs

Mainly abstractions + precompiles for crypto

Will remove the ice age, but no PoS

Stage-1 Casper

Vitalik recently published contract for stage-1 casper

repo: github.com/ethereum/casper

Finalizes a checkpoint every 100 blocks (2/3 commits)

Takes precedence over PoW

If two blocks finalize at the same block

=> at least 1/3 of stake is destroyed

github.com/ethereum-vienna-meetup/