TweetWallet

Control your crypto with smart contracts and social media.

Premises

1. Key management by individuals is essential for decentralized peer-to-peer e-cash: be your own bank.
2. But private key management is very painful.
3. Tech giants offer best practicable security, ease of use, and identity management: 2-factor auth, machine-learned fraud detection, human judgement, etc.
4. Is there a middle ground for programmable money?

Previous implementations were good ideas, but were centralized

ChangeTip (aquihired by AirBnB in 2016) facilitated Bitcoin tips via centralized bots on social media accounts: Reddit, Twitter, Facebook, Github, Twitch, Slack, etc.

Transactions were not “on-chain,” but in ChangeTip’s database

Potential solution: Smart contracts and oracles

1. Offload key management to (1) smart contracts, (2) oracles and (3) security experts at the tech giants.
2. Solution: Ethereum smart contracts relying on oraclize.it to prove ownership of online accounts.

Demo!

Challenges

1. Privacy
2. Oraclize.it is a trusted third party; oracles remain a big question mark in crypto
3. Online (social media) accounts often trusted third parties
4. SSL / TLS / TLS Notary proofs are very, very difficult
5. Basic technical implementation challenges in smart contract development are significant

Tools used

1. Truffle framework / Web3js - development
2. Oraclize - oracle service
3. Oraclize Remix IDE - development and testing
4. Go Ethereum Client / Ethereum Ropsten Testnet - deployment
5. Metamask - signing transactions
6. Etherscan - third-party verification of transactions

Recap: the basic idea

A vision where probabilistic solutions to private key management using (1) oracles and (2) trusted sources of online identity offer a compromise between ultrasecure blockchains and ease of use.

Thanks!

Find this code on GitHub - github.com/toneloc/tweet-wallet

Find me after the Meetup, or on Twitter - @tonklaus