



ethereum
vienna

The DAO



ethereum

Agenda

General Introduction

Updates

The DAO

Socialising



ethereum
vienna

Updates

Workshop #1

Tomorrow: May 24th 17:00

January Workshop + Mix

- Basic Solidity
- Mix IDE
- Geth contract interaction (if time)

Too many RSVPs

Exercises (specification, solution) will be on github afterwards

Workshop #2

In June

Transforming an idea into a contract

- Libraries
- Standard Contracts (namereg, tokens, ...)
- Deployment using a framework, node.js

If you want to participate

 rsvp on meetup

 take the anonymous survey for date finding

Geth 1.4

Security Alert - DDOS - Update to geth 1.4.4 !

Push instead of Pull

Canary finally removed

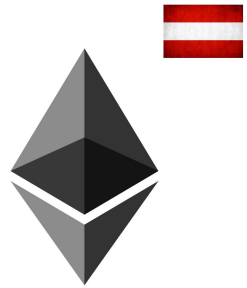
Casper

In all ordinary scenarios only one block to bet on

Betting exists so

- a block can still be included in case of an attack

- find consensus that there was no block at a height



Blockchain Contest

in the making: DAOs and HW

WHO ?



+ Sponsors

WHEN ?

- 30 Sept. (call for submissions)
- ~ Mid Oct. (finalist presentation)

WHAT ?

- Training
- 
- Fame
- Capital

→ sign-up to
“special announcements” in
meetup group



ethereum
vienna

The DAO
decentralised autonomous organisation

What is the DAO?

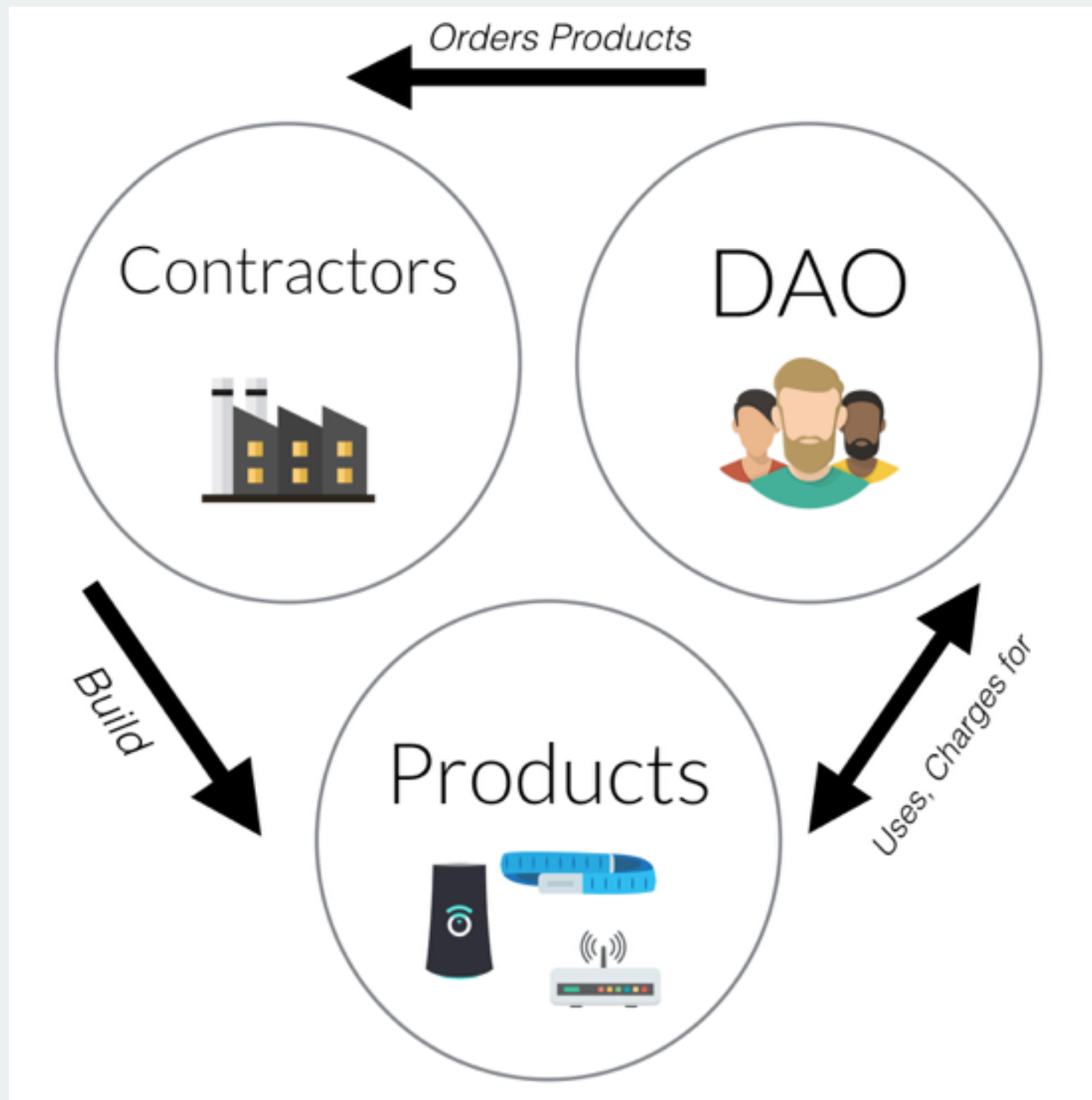
Does not produce anything by itself

Funds proposals

Distributes revenues to
its owners



What is the DAO?



What is the DAO?

Owners of the DAO - token holders (TH)

TH vote on proposals

- Voting power proportional to investment
- Necessary quorum scales with proposal size
- TH can “split” the DAO if they’re unsatisfied

History of the DAO

Developed by slock.it

Standard DAO Framework

Developed to fund themselves

FOSS (LGPL)

DAO Funding

Anybody can fund the DAO

At the beginning: 100 Token per ether

Now: 100 Token per 1.45 ether (1.5 tomorrow)

Excess ether from higher price goes to **extraBalance**

Total Raised: 11.47M eth (~ 163,000,000\$)

Ends on May 28th

How does the DAO work?

TH submits a proposal to the DAO

pays a deposit to combat spam / gain priority

Start of debating/voting period

TH discuss and vote on the proposal

If quorum is reached

Nay - proposal is dismissed

Yea

proposal is executed

reward tokens are generated (1 per wei, held by the DAO)

DAO Proposals

Sends a message to a **recipient**

amount

transactionData (to call functions)

=> Proposals can be contracts

description, debatingPeriod

Special case: New **curator**, curator = recipient

How does the DAO work?

If successful venture

contractors send revenue to DAOrewardAccount

DAO can with a proposal to itself

move it to the rewardAccount for the TH

move it into its own funding

Curator

Every DAO has one curator

Controls a whitelist of where funds can be sent

Should protect against various attacks

If some TH are unsatisfied with curator

- submit a proposal to replace curator

- special proposal, regular voting

Splitting

If the new curator proposal is accepted
the recipient in the proposal becomes the curator
otherwise the curator remains the same

but if you voted yes for the new curator

Splitting

but if you voted yes for the new curator
you can split from DAO

Your ether is sent to the new DAO with the new curator

Reward Tokens are transferred to the new DAO

Reward Tokens represent rights to reward income

Old DAO Token (**not** Reward Tokens) are burned

DAO Token

DAO Token implement the Token Standard

=> Native support in Mist / UI Wallet

Will be tradable on exchanges

If you used the token to vote in a ongoing proposal:

not tradable

no splitting

“Withdrawing” ether

Propose yourself to be the curator (will probably fail)

Split the DAO

Make a proposal to send everything to yourself

Execute the proposal

Stalker Attack

Somebody else joins your split with more token
but you are the curator

Attacker can only propose to send ether to you
But the attacker can block all proposals

With complicated countermeasure the victim can steal
all funds from the attacker (see DAO wiki)

extraBalance

Extra ether gained through price increase
stored in extra account

can only be moved to main account when the DAO
has spent as much of its funding

DAO Risks

Withdrawing takes 38 days - ether price risk

but still floor of 1 ether per 100 tokens for early buyers

The crowd making bad decisions without you noticing

Bugs

Legal Risk

Investments fail miserably

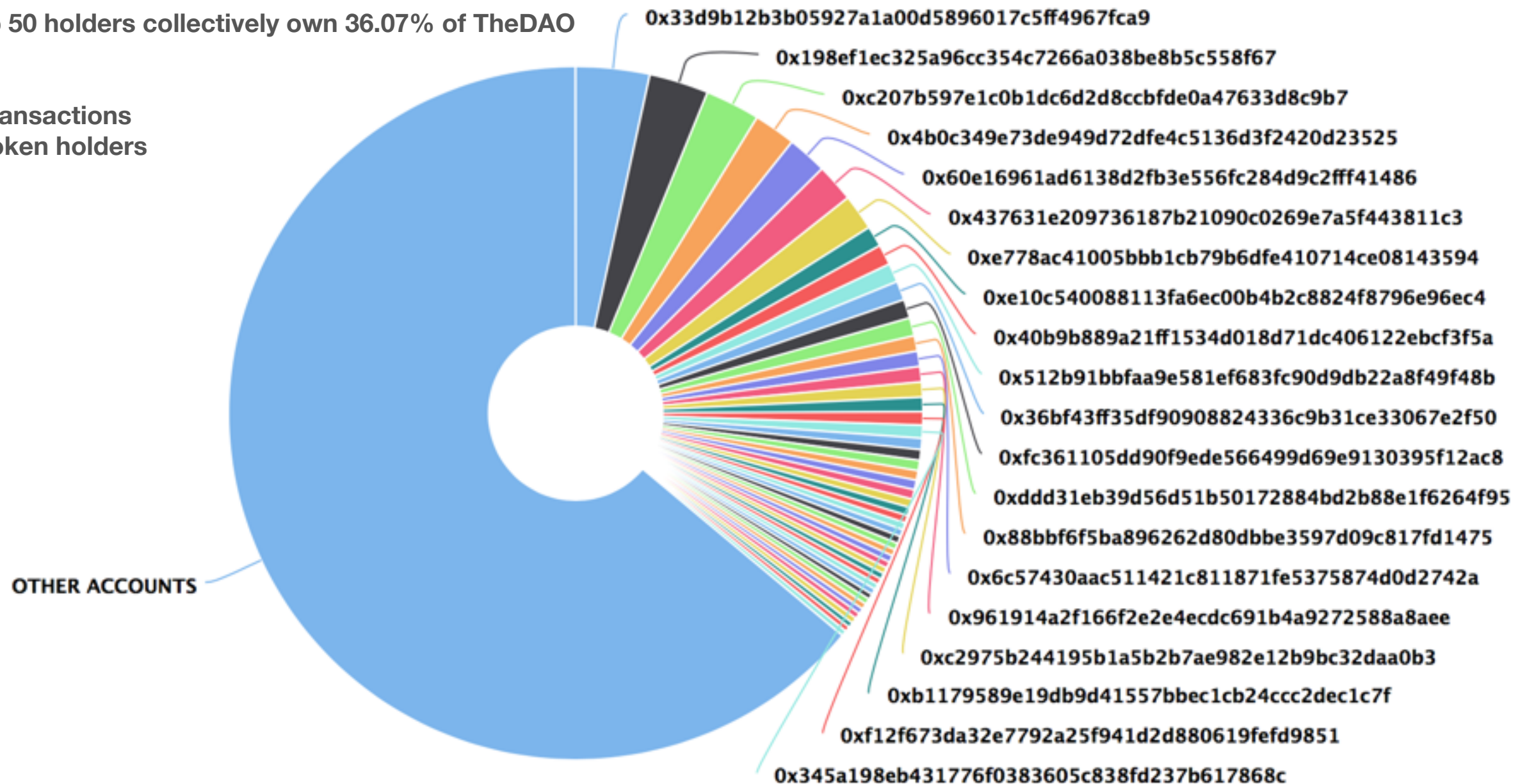
DAO Token Holders

TheDAO Top 50 Token Holders

Source: Etherscan.io

The Top 50 holders collectively own 36.07% of TheDAO

49000 transactions
22018 token holders



DAO.LINK

provides regulatory, tax, VAT solutions for Contractors

Partnership with bity.com

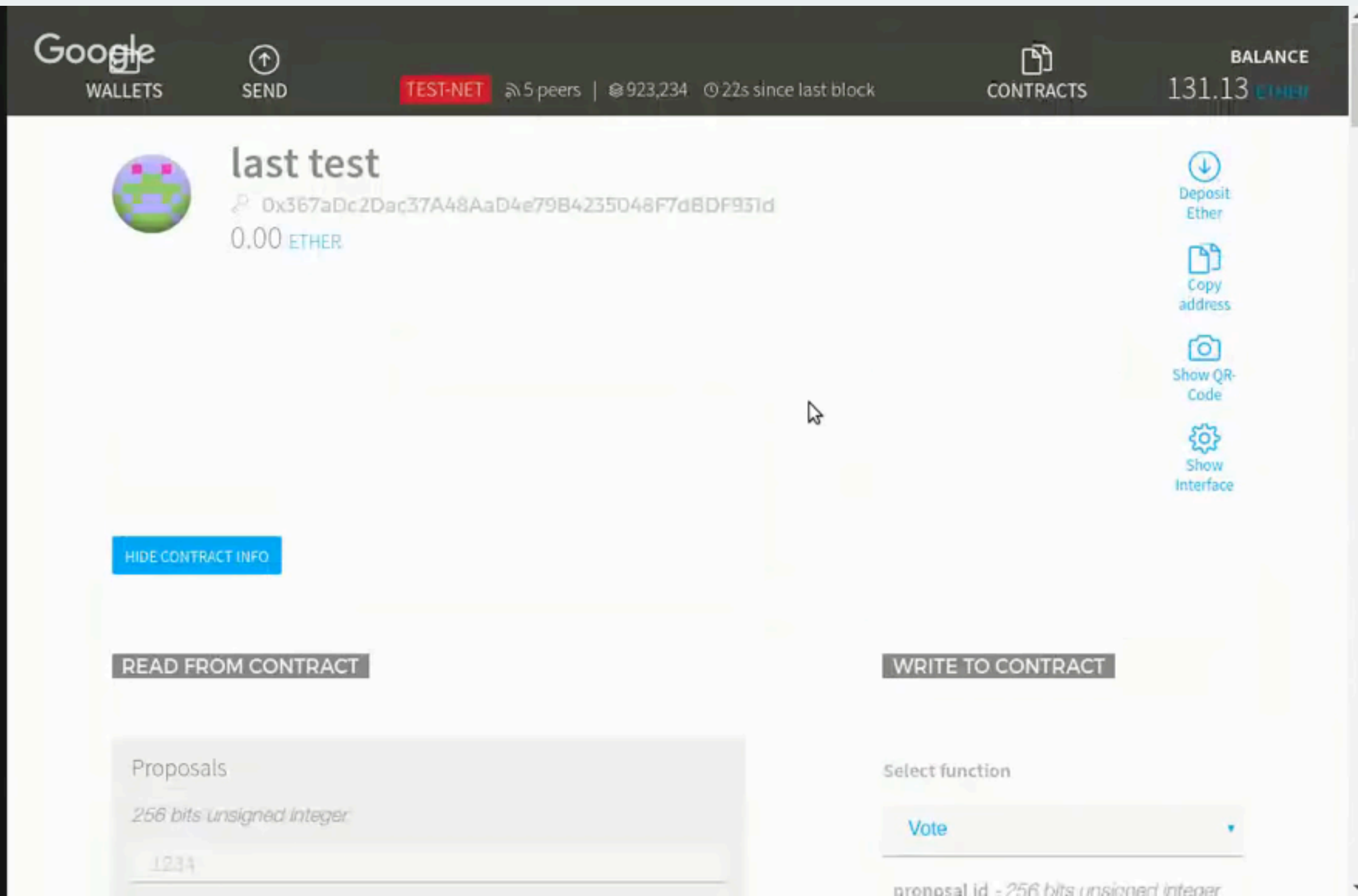
DAO.LINK contracts the DAO in the contractors stead

DAO Interaction

UI in development

In the meantime: UI Wallet contract interface

DAO Interaction




Google
WALLETS

SEND

TEST-NET 5 peers | 923,234 22s since last block

CONTRACTS

BALANCE
131.13 ETH

 **last test**
0x367aDc2Daç37A48AaD4e79B4235D48F7d8DF931d
0.00 ETH

Deposit Ether

Copy address

Show QR-Code

Show Interface

HIDE CONTRACT INFO

READ FROM CONTRACT

WRITE TO CONTRACT

Proposals

256 bits unsigned integer

1234

Select function

Vote

proposal id - 256 bits unsigned integer

DAO Source Code

github.com/slockit/dao

Deep dive in the DAO smart contracts with Slock.it
CTO Christoph Jentzsch

https://www.youtube.com/watch?v=5BkQ0te_TA0

DAO Community

daohub.org

Details about the DAO

Forums

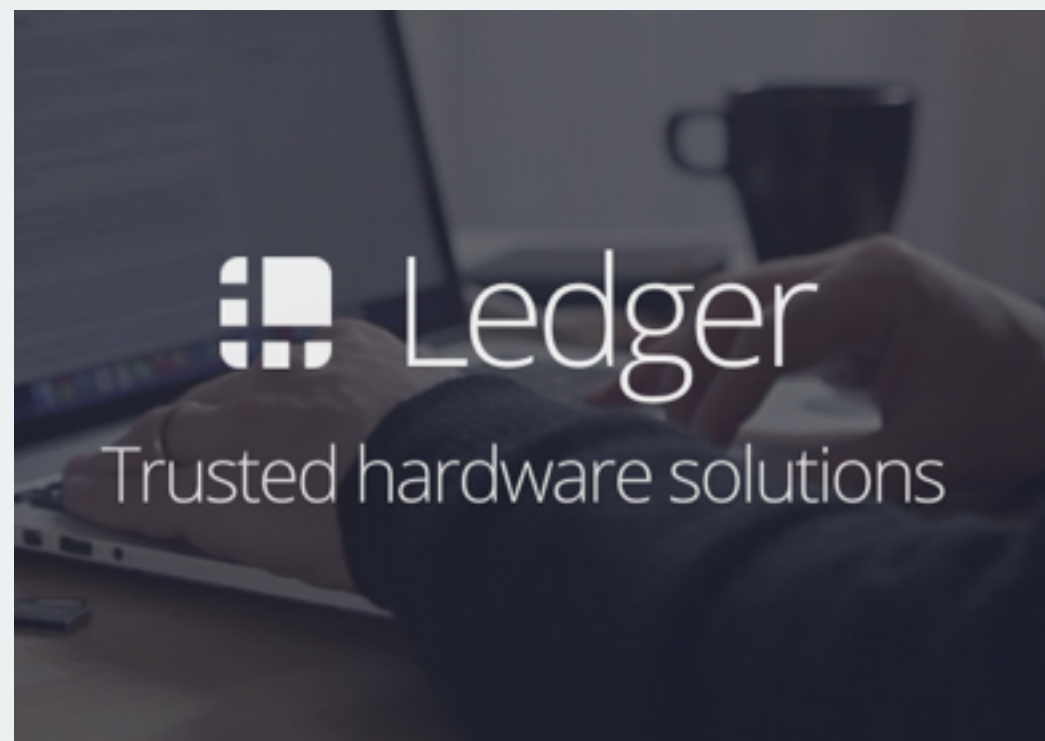
DAO Upgrades

DAO can update itself

Requires majority vote

All ether and rewardToken sent to new contract

DAO Proposals



DAO Troubles

/u/daoattack

Proposed a number of attacks to the DAO

Too much power and trust in the curator

=> solo splits ?

=> minimal yes quorum

github.com/ahirner/ethereum