Blockchain Promises to Address Democracy

Behind and Beyond Bitcoin

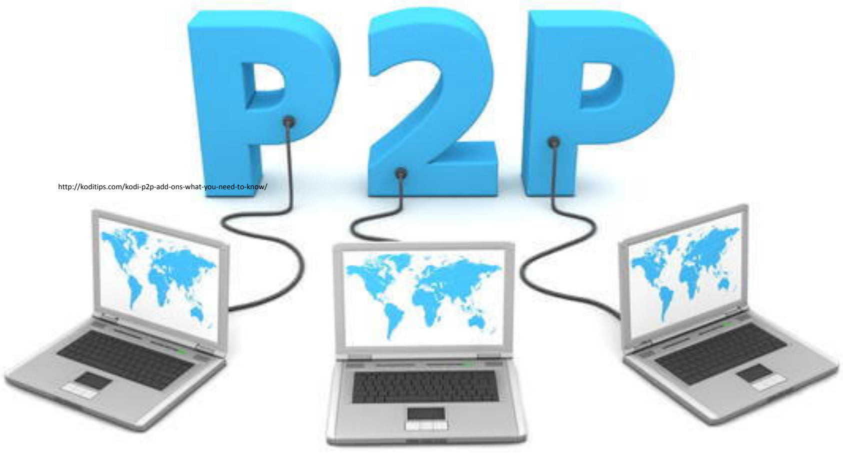
If all you have is a hammer…

http://www.homespothq.com/

… everything looks like a nail

Well… we may have other tools

https://ongoingoperations.com/2013/05/09/web-applications-work-hosted-virtual-desktops/



http://koditips.com/kodi-p2p-add-ons-what-you-need-to-know/

https://www.ocrmobile.com/fr/ocr-api-cloud-salesforce.html

But the new toy has to be tried!

http://www.homespothq.com/

What is the Blockchain like?

A shared database (of tokens):

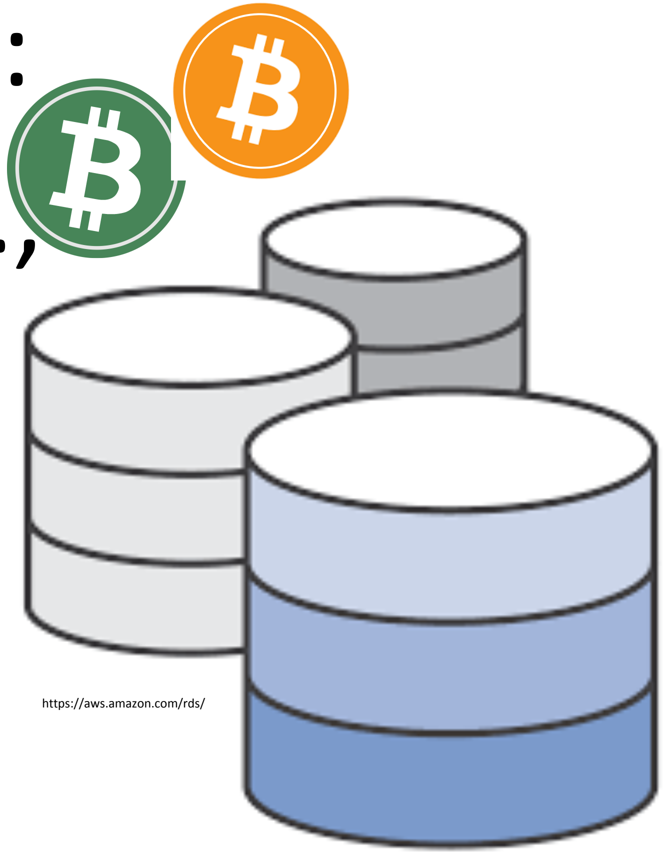
- Token (legally) =
  - donation,
  - “not a security”, ☺
  - “not an investment”

https://aws.amazon.com/rds/

What are the tokens in fact?

Realized with either:

- colored coins, i.e., Bitcoins (satoshis) made special
- a fungible amount in ETH smart contracts



https://aws.amazon.com/rds/

How to use tokens?

- Tokens
  - Informal agreement (on something external)
  - Intrinsic:
    - The key of a car
    - Currency of a closed community

https://aws.amazon.com/rds/

Types of Tokens

- In the database:
  - – Intrinsic tokens: makes the blockchain work (BTC, ETH, …)
    - Incentive for miners
    - Transaction cost
    - Pre-mined or generated
  - – Asset/Utility tokens
    - Claims on assets
      - – Goods, music, votes
      - – Created, bought, transferred, redeemed
      - – Can represent assets, or replace assets (if legally supported)

https://aws.amazon.com/rds/

Properties and Limitations

- Not guiding decision but making decisions
- Shared / Common memory (Consensus as a service)
- Public, Secure: Permission(less)
- Decentralized
- Persistent (10 years)
- Eliminates need of trust
  - No need of escrow

https://aws.amazon.com/rds/

Lost if you
lose your keys

Mastercard

eCash

UBS

1998

Marius Silaghi

Properties and Limitations

- Not guiding decision but making decisions
- Shared / Common memory (Consensus as a service)
- Public, Secure: Permission(less)
- Decentralized
- Persistent (10 years)
- Eliminates need of trust

- Fix update rate: 10min, 14s,…
- Max update size: 1MB, 1.5MGas

https://aws.amazon.com/rds/

Many applications can work with these parameters.

… more or less.

3-6 BTC-ETH transactions/s

Expensive court system: use only for disagreements ("ETH founders")

List by FutureThinkers.org

20 Applications of Blockchain - I

1. Banking --- sending Remittances: ABRA, Barclays, Ubin
2. Cybersecurity (eliminates middleman): Namecoin, Blocksign
3. Supply Chain Management: Fluent/Hijro, Blockverify,
4. Forecasting (placing bets): Augur
5. IOT devices network (eliminate centralized communication)
6. Insurance (identity verification): Aeternity
7. Private Transportation / Ridesharing (stable contracts): Arcade City, La’Zooz
8. Cloud Storage: storj.io
9. Charity (prove that recipients receive the funds): BitGive
10. Voting: followmyvote.com, MiVote

List by FutureThinkers.org

20 Applications of Blockchain - II

GOVCOIN™

11. Government (avoid corruption, put data online): Dubai
12. Distribute public benefits (universal income): GovCoin, Circles
13. Healthcare (secure sharing of data): Tierion
14. Energy Management: TransactiveGrid
15. Music Licensing: Mycelia, Ujo Music
16. Retail (smart contracts): OpenBazaar, OB1
17. Real Estate (speed transactions and verification of ownership): Ubitquity
18. Crowdfunding (trust via smart contracts, tokens with values, rules enforced in code): Consensys
19. News (decentralized and less fake): DNN, Leeroy

20 Political Parties: DemocracyEarth

TIERION

MYCELIA

UJO MUSIC

OpenBazaar

UBITQUITY

OB1

CONSENSYS

DNN

Democracy.Earth

We hear talk about

- A virtual society

- Startup cities

Virtual Society?

Bitnation (2000 people citizenship),
Bitpesa (foreign currency exchange),
Darknet: cjdns, Tor (NSA supported), Freenet

(Exchanges have to comply with countries!)

Decentralizing pillars of a virtual society:

1. communication,
2. laws,
3. production,
4. finance (currency/contracts)

Seems to be almost done!

Principle working with decentralization

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.”

by Buckminster Fuller

https://www.youtube.com/watch?v=yGmGWZCE4h0 diaspora*

It has been tried in the past…

- “Diaspora” practically failed for lack of funding

- Blockchains add funding to play!

Pre-requisites for Meaningful Voting

- – Institutional commitment
- – Identity verification
- – Ballot counting

Difficult!

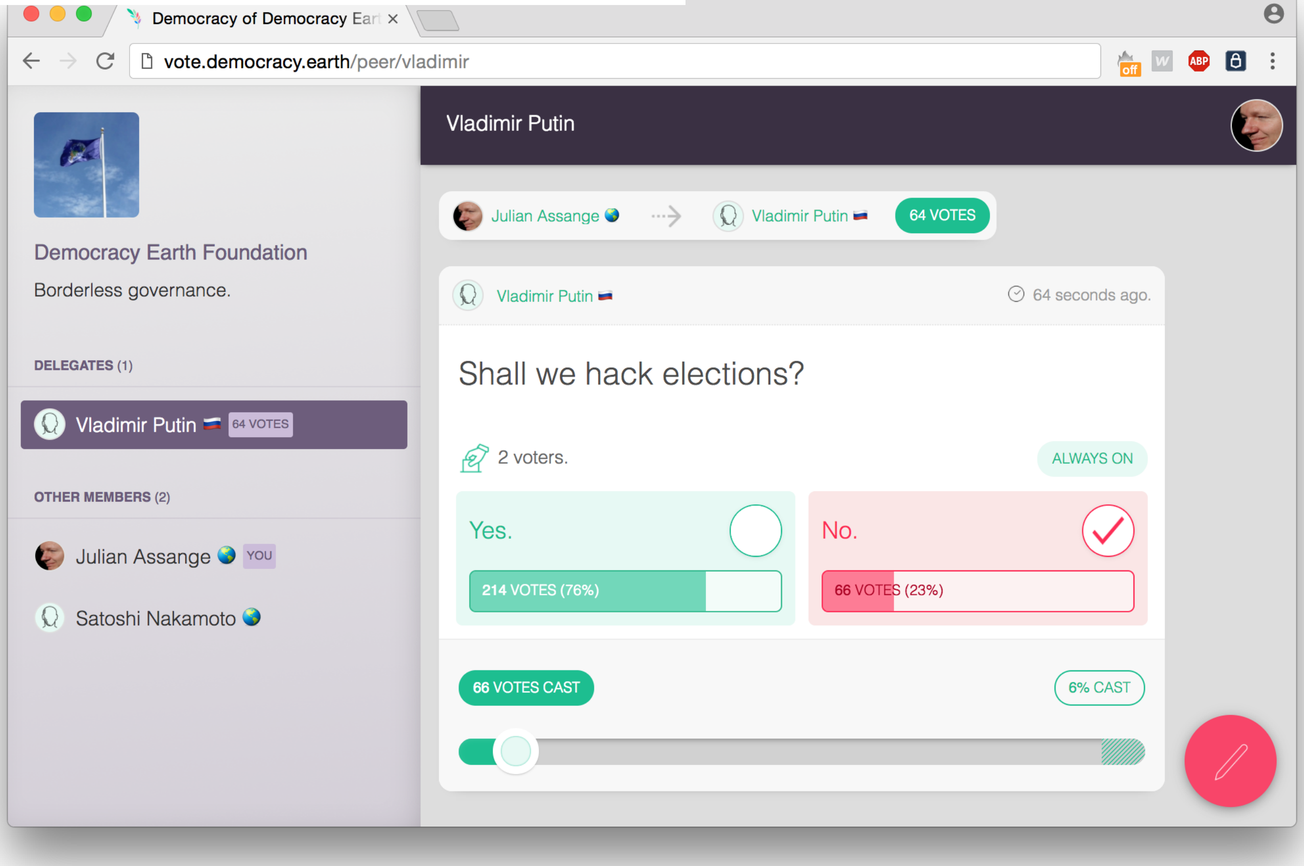
From team games!
Horizon State
Humans with Purpose

Mivote.org.au

Democracy.Earth

BLOCKSTACK

Sovereign


Democracy of Democracy Ear

vote.democracy.earth/peer/vladimir

Democracy Earth Foundation

Borderless governance.

DELEGATES (1)

Vladimir Putin 64 VOTES

OTHER MEMBERS (2)

Julian Assange YOU

Satoshi Nakamoto

Vladimir Putin

Julian Assange → Vladimir Putin 64 VOTES

Vladimir Putin 64 seconds ago.

Shall we hack elections?

2 voters. ALWAYS ON

Yes. 214 VOTES (76%)

No. ✓ 66 VOTES (23%)

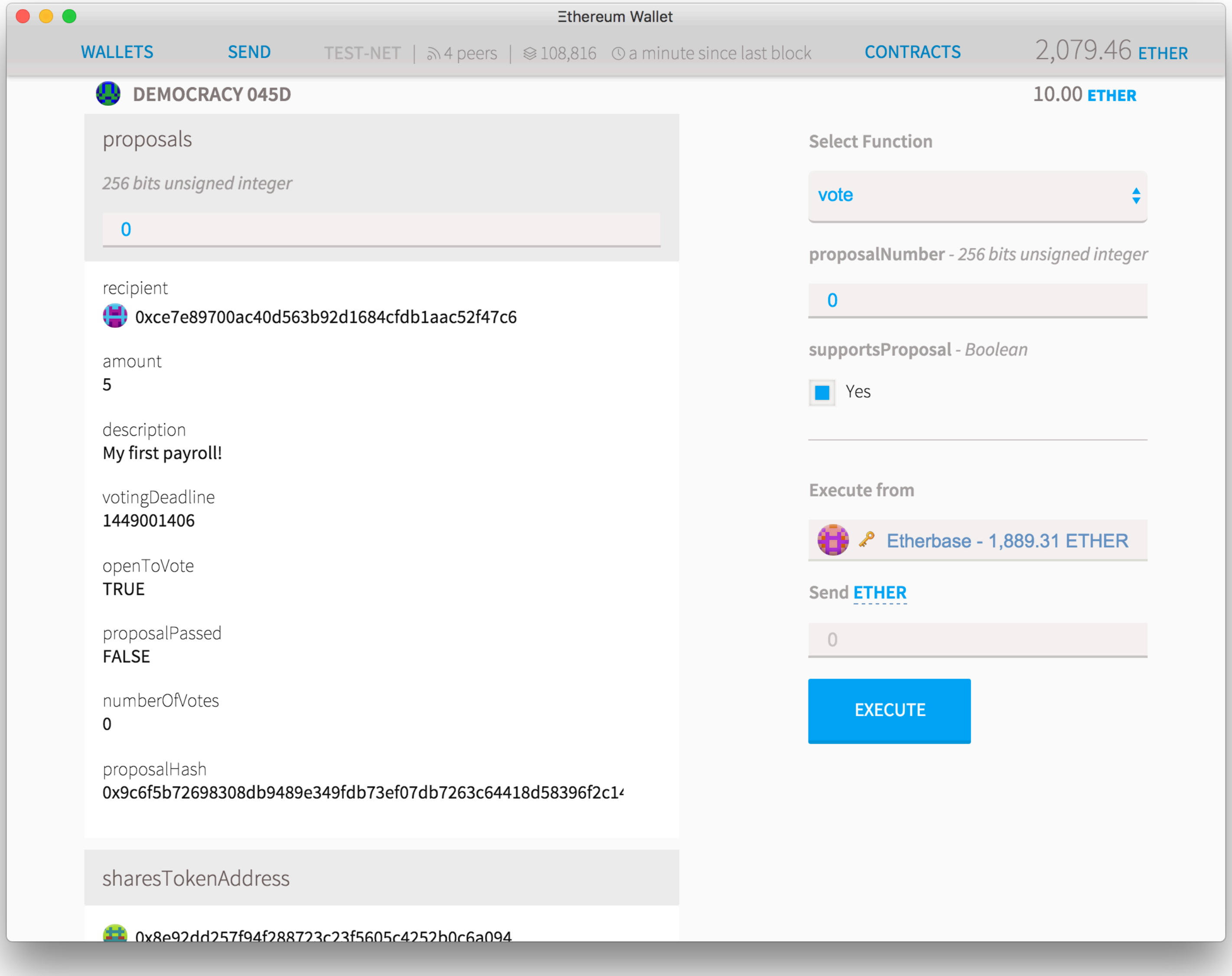
66 VOTES CAST

6% CAST

Pirate Party-like
Under development

http://sovereign.software

Mist: Build a Democracy in 100 lines ☺



DEMOCRACY 045D

10.00 ETHER

proposals

256 bits unsigned integer

0

recipient
0xce7e89700ac40d563b92d1684cfdb1aac52f47c6

amount
5

description
My first payroll!

votingDeadline
1449001406

openToVote
TRUE

proposalPassed
FALSE

numberOfVotes
0

proposalHash
0x9c6f5b72698308db9489e349fdb73ef07db7263c64418d58396f2c1

sharesTokenAddress

0x8e92dd257f94f288723c23f5605c4252b0c6a094

Select Function

vote

proposalNumber - *256 bits unsigned integer*

0

supportsProposal - *Boolean*

☑ Yes

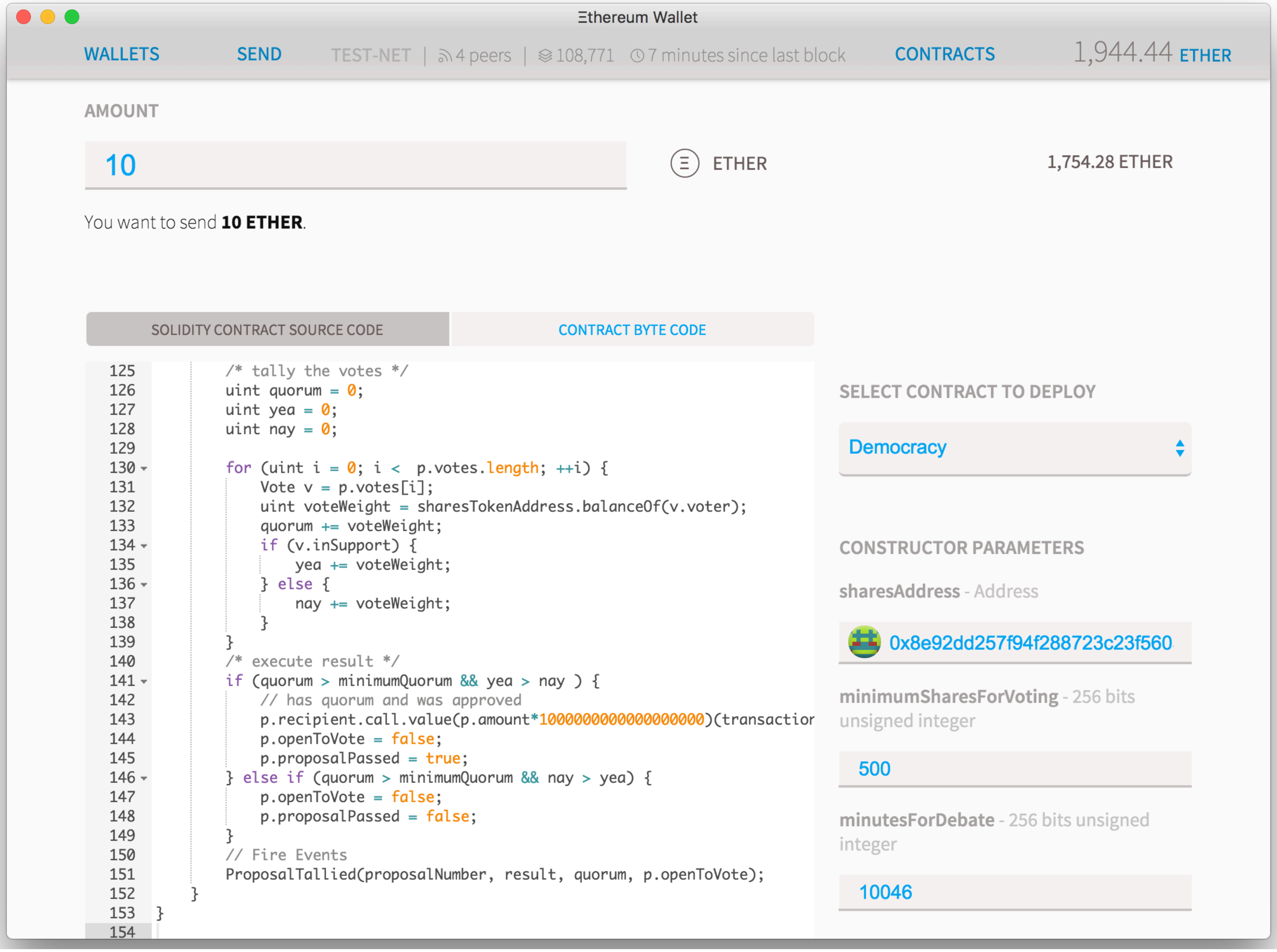
Execute from

Etherbase - 1,889.31 ETHER

Send ETHER

0

I mean … in 100 lines of code ☹


Ξthereum Wallet
WALLETS
SEND
TEST-NET | 4 peers | 108,771 7 minutes since last block
CONTRACTS
1,944.44 ETHER
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE

AMOUNT

10 ETHER 1,754.28 ETHER

You want to send **10 ETHER**.

```
        /* tally the votes */
        uint quorum = 0;
        uint yea = 0;
        uint nay = 0;

        for (uint i = 0; i <  p.votes.length; ++i) {
            Vote v = p.votes[i];
            uint voteWeight = sharesTokenAddress.balanceOf(v.voter);
            quorum += voteWeight;
            if (v.inSupport) {
                yea += voteWeight;
            } else {
                nay += voteWeight;
            }
        }
        /* execute result */
        if (quorum > minimumQuorum && yea > nay ) {
            // has quorum and was approved
            p.recipient.call.value(p.amount*1000000000000000000)(transactior
            p.openToVote = false;
            p.proposalPassed = true;
        } else if (quorum > minimumQuorum && nay > yea) {
            p.openToVote = false;
            p.proposalPassed = false;
        }
        // Fire Events
        ProposalTallied(proposalNumber, result, quorum, p.openToVote);
    }
}
```

SELECT CONTRACT TO DEPLOY

Democracy

CONSTRUCTOR PARAMETERS

sharesAddress - Address

0x8e92dd257f94f288723c23f560

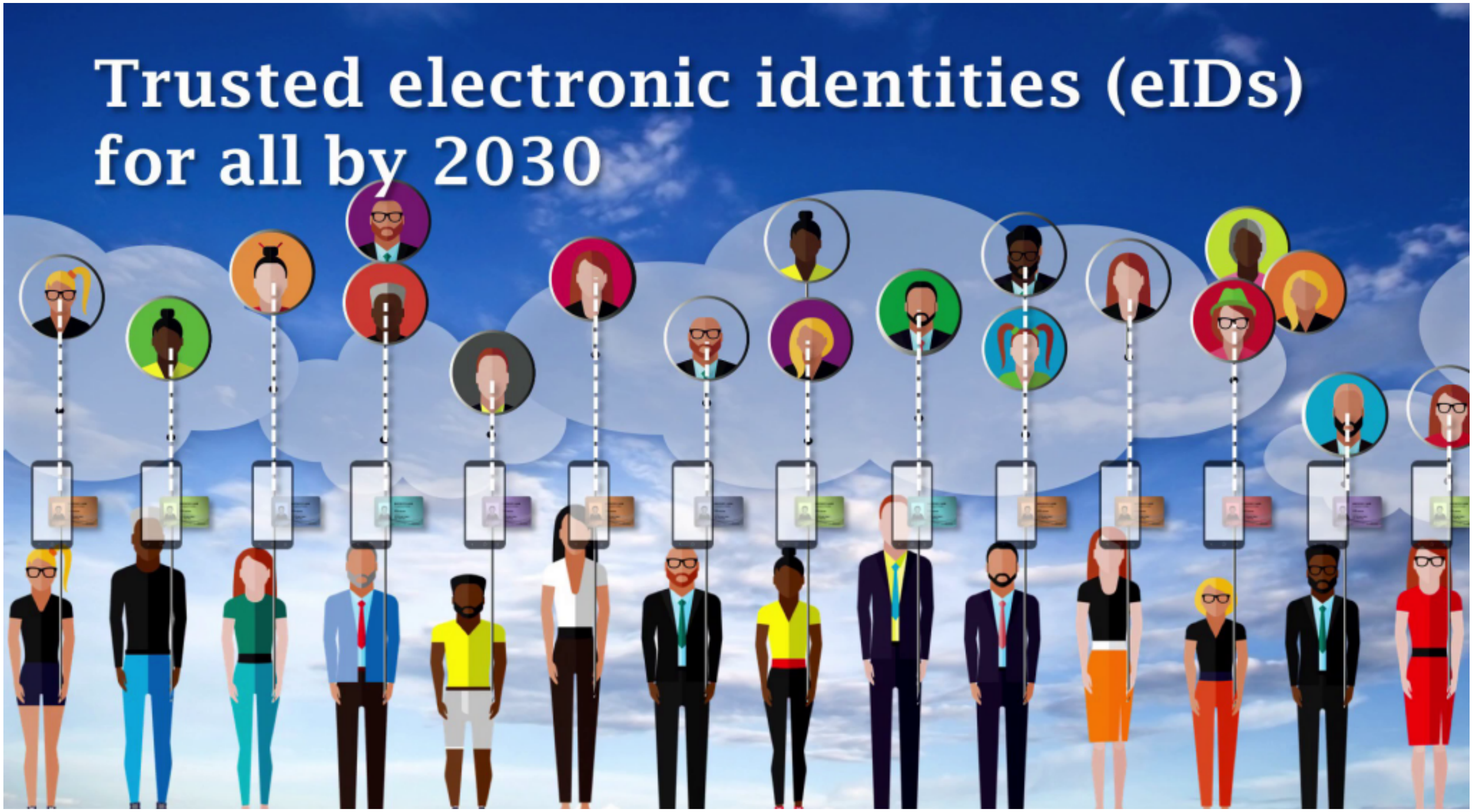
minimumSharesForVoting - 256 bits unsigned integer

500

minutesForDebate - 256 bits unsigned integer

10046

Now the Internet is a masquerade (Ehud Shapiro'WEF16)



http://opentranscripts.org/transcript/biomolecular-computing-internet-democracy/

How does it technically work?

- ICO (initial coin offering, not initial public offering ☺):
  - Laws don’t apply… Documentation may be a webpage.
  - A certain number of tokens is put on the market
  - Amount of funds gathered cannot be checked (identity of investors; amounts, see Petro scandal)

What are the Smart Contracts?

- They are addresses/accounts associated with code … in a programming language: e.g., Solidity.
  - When bitcoins/ethereum (Gas) are loaded into the account, miners run it, to get the reward.
  - This obviates the need of contracting clauses

Problems with Apps?

- Decentralized News Network, DNN: Promising freer thinking press, selected contributors, democracy, resistance to gag orders
  - Founders own 10% stakes continuously (right to write !!!!?)
  - Readers, writers, (Super!!-)reviewers, publishers (echoing classic journals)
  - Complex economy: tipping, pay for any right, get paid on reputation of agreeing with majority!!!? Payment proportional with capital. Cannot withdraw articles. Only sourced articles!!?
    - (Qvo vadis resistance to gag orders)

Problems with the chain?

- Safety/cost for consensus:
  - BTC consuming as much as Denmark
  - And grows 25% per month
    - proof-of-stake (NXT) / importance (NEM)???
      - Centralization possible
      - Qvo vadis Democracy?!
- Smart contracts… need verification
- Scalability --- the bandwidth is small:
  - Additional buzzwords: Plasma, state channels, Sharding
  - Blockchain for decentralization….
  - … Clouds for parallelism

… and, if it does not work

… take a bigger one

https://inserbia.info/today/2013/09/serbia-man-kills-his-wife-with-a-sledgehammer-than-jumps-off-a-terace/