Vienna, April 11th 2014

1ST ETHEREUM MEETUP

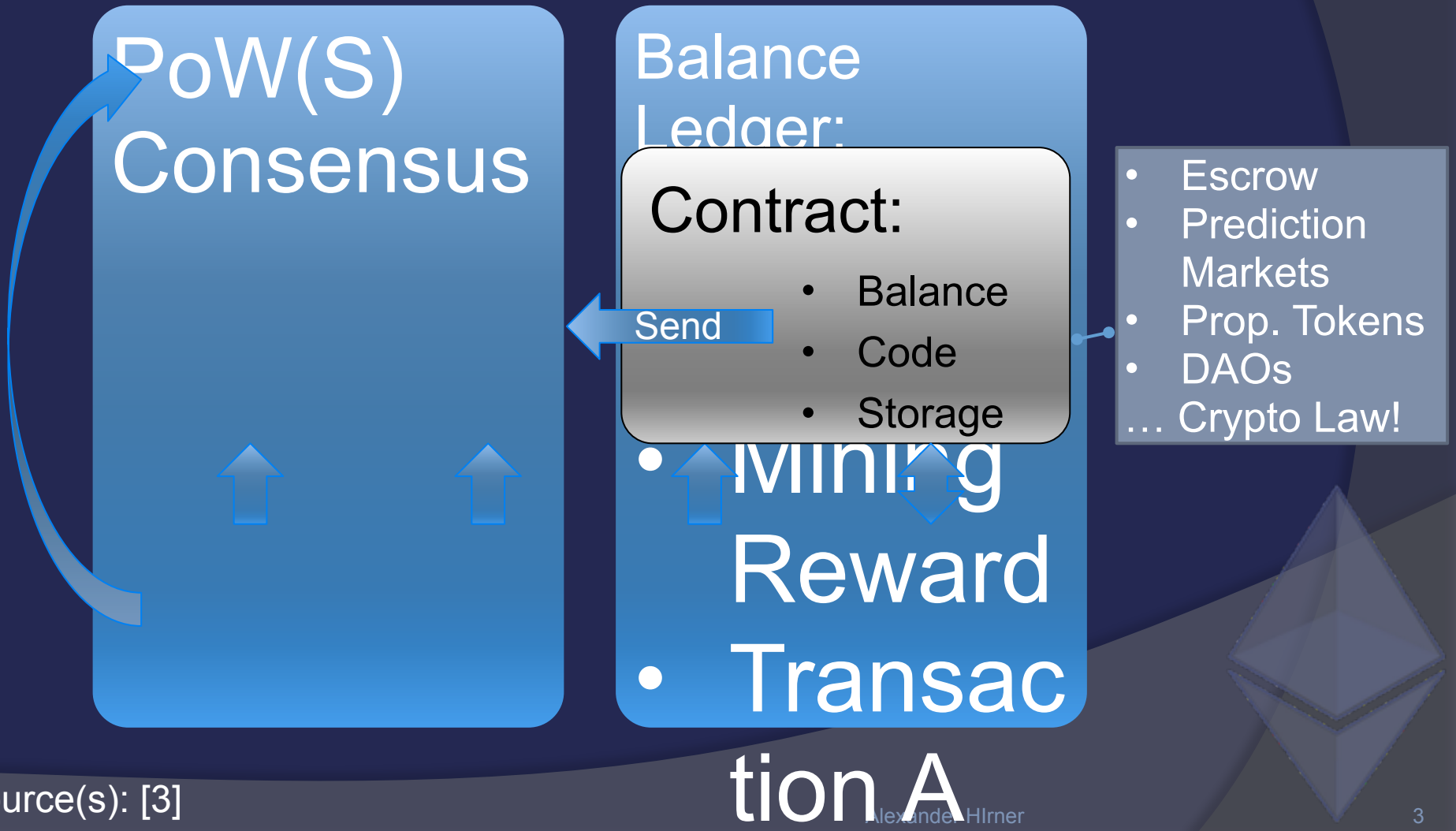
Evolution of Blockchain

- Bitcoin System

source(s): [1, 2]

Evolution of Blockchain

- Ethereum System



source(s): [3]

Use Cases: Finance

- Saving Accounts (distributed access controls)
- *Every* Financial Contract (CFDs, Collateralization, Derivatives)

ACTUS

Old Acc. Paradigm

- Fair Value Fraud
- Proprietary Valuation
- Window Dressing

- → obfuscation
- → compliance costs (& bribery)
- → bonus 'engineering'
- → stress tests

New Paradigm

- Transparency
- Programmability
- Less to dress-up

- → self informed valuation
- → algorithmic auditing (low costs)
- → higher informed system wide consensus

- → high dimensional

source(s): [3] [9]

Use Cases: Social Perspective

- Remittance Market quasi [!] solved
- Ethereum expands Possibilities:
  - Identity: Anonymity ←→ Pseudonymity ←→ Non-Anonymity
  - Webs of Trust ←→ Reputation (‘democratic tribunals’)
  - Rule based public Good Funding (dominant assurance contracts)
  - … and Management (e.g. Deodands, sharing economy)
  - Factum Law + accompanying, distributed Services (trusted data feeds, micro arbitration) increases certainty

Ethereum Society, ‘Cryptocracy’:
à Distributed Entrepreneurship
→ Lower Barriers of Entry & Better Allocation of Resources
à Social Inclusiveness & Mobility

source(s): [10 - 16]

Example: HLL Crowd Funding

Contract:

- Balance
- Code
- Storage

Storage Doc:

Storage[1000++]: **state**, fundee, project name, expiry timestamp, limit

Storage[1100]: nr. of funders

Storage[1101..2000]: funder addresses

Storage[2000++]: funder balances

```
1   if msg.sender < 2000:
2       return(0)
3
4   state = contract.storage[1000]
5   if state == 0:
6       contract.storage[1000] = 1
7       contract.storage[1001] = msg.sender
8       contract.storage[1002] = msg.data[0]
9       contract.storage[1003] = block.timestamp + 30 * msg.data[1] * 86400 / 24
10      contract.storage[1004] = msg.data[2]
11  elif state == 1:
12      if block.timestamp > contract.storage[1003]:
13          n = contract.storage[1100]
14          i = 1101
15          while i < 1101 + n:
16              funder = contract.storage[i]
17              send(funder, contract.storage[funder] * 0.99, tx.gas - 100)
18          paytheresttocrowdfundingplatform = contract.storage[-1]
19          contract.storage[1000] = 2
20          return(0)
21      else:
```

source(s): [17, 18]

Example: HLL Crowd Funding

Contract:

- Balance
- Code
- Storage

Storage Doc:

Storage[1000++]: **state**, fundee, project name, expiry timestamp, limit

Storage[1100]: nr. of funders

Storage[1101..2000]: funder addresses

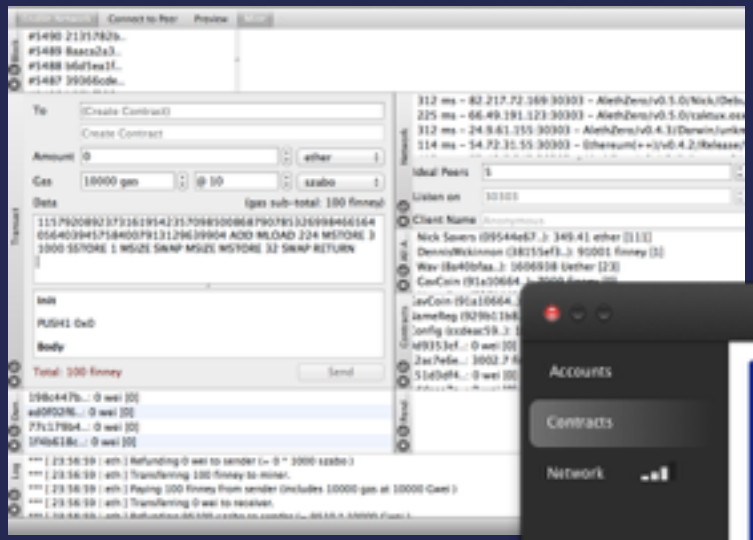
Storage[2000++]: funder balances

```
21      else:
22          n = contract.storage[1100]
23          fbalance = contract.storage[msg.sender]
24          if fbalance > 0:
25              contract.storage[msg.sender] = fbalance + msg.value
26          elif n > 2000 - 1100:
27             send(msg.sender, msg.value, tx.gas - 100)
28          else:
29              contract.storage[1100] = n + 1
30              contract.storage[n] = msg.sender
31              contract.storage[msg.sender] = msg.value
32      if contract.balance >= contract.storage[1004]:
33          send(contract.storage[1001], contract.balance * 0.99, tx.gas - 100)
34          paytheresttocrowdfundingplatform = contract.storage[-1]
35          contract.storage[1000] = 3
36          return(1)
```

Hint: don't just stop with handing over the cash ;)

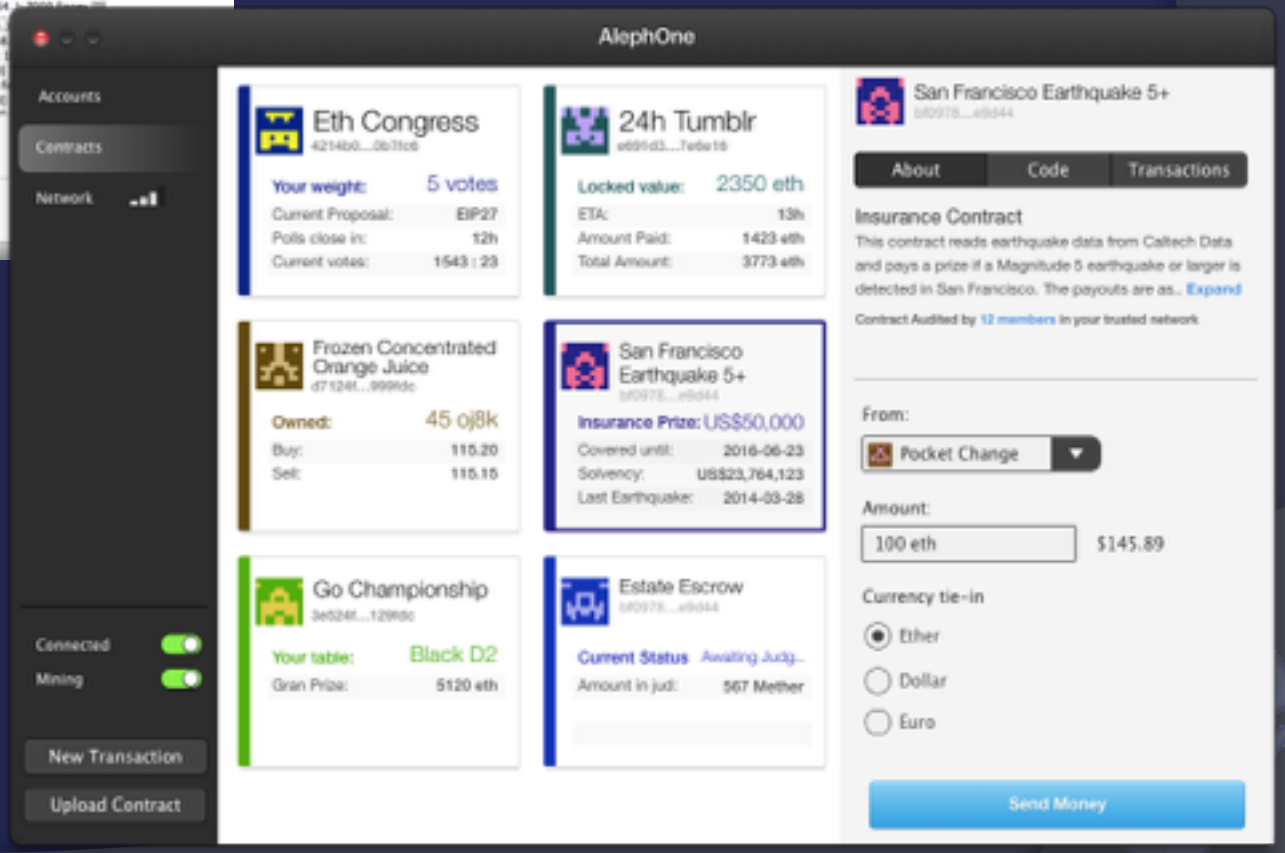
source(s): [17, 18]

Usability



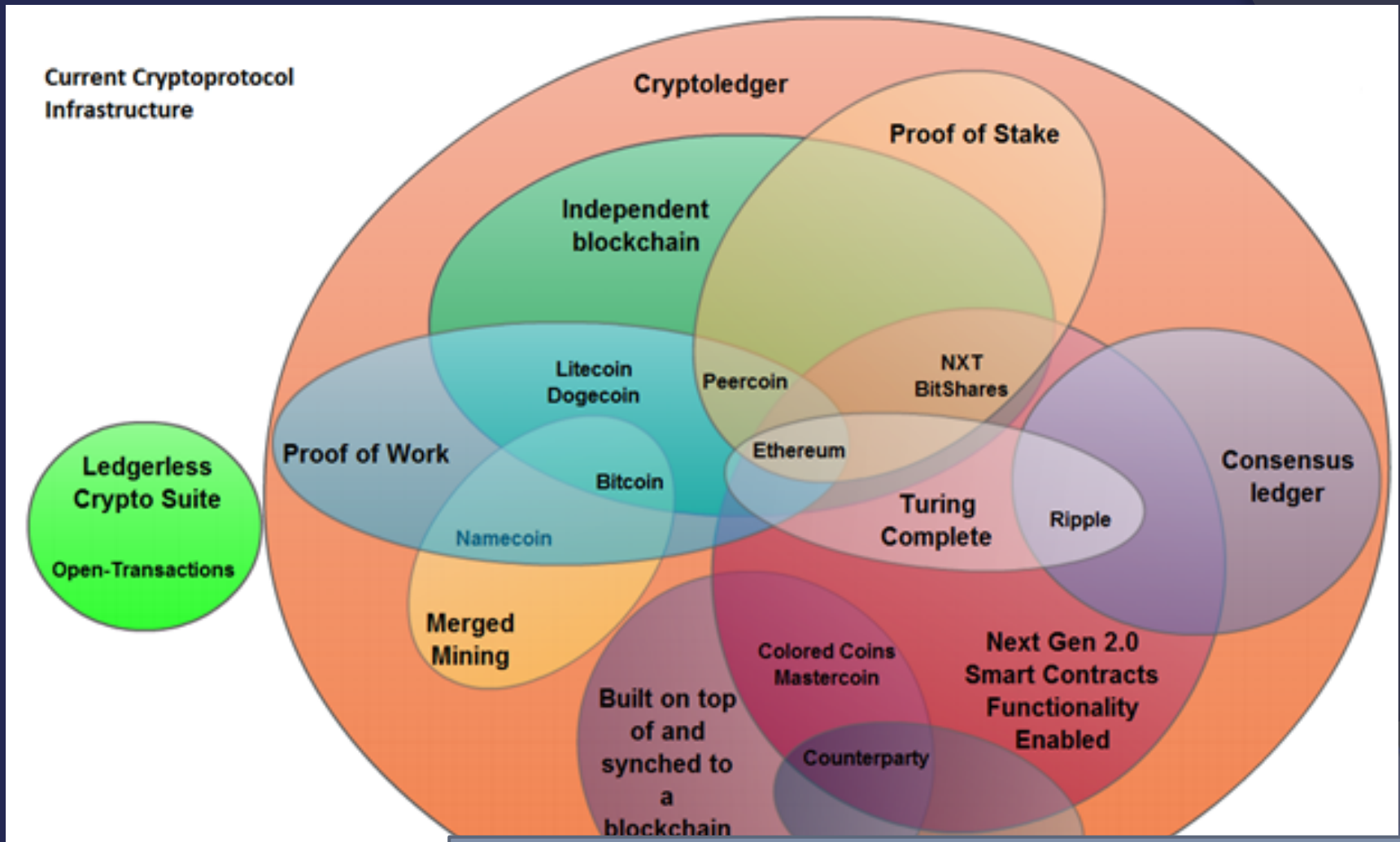
- Aleph POC 4 (out of .. a lot more)

- Final UI … Mockup
  - HTML/CSS UI for Contracts
  - Torrent/.. distributed dl
  - Android like AppStore feel



source(s): [19]

One *Blockchain* to rule them all?



Tim Swanson, 2014

→ Competition & Cooperation:
BTC decentralized exchange with Escrow
Side-chain implementation of Eth functionality

source(s): [20, 21]

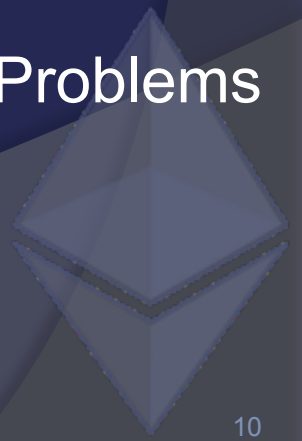
News and Community

- BTC Funding (= ETH presale) → Incorporation → Foundation like (development, bounties)

- Q1, pre Alpha
- Q4, Ethereum 1.0, Genesis Blockchain
- 201? Ethereum 2.0

- The Swiss Connection

- Likely Development Path: Ethereum DAO, 10 Big Problems in Cryptocurrency



source(s): [22 - 25]

Sources

- 1) https://bitcoin.org/bitcoin.pdf
- 2) http://bitcoinmagazine.com/11108/multisig-future-bitcoin/
- 3) https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper
- 4) http://www.projectactus.org
- 5) http://www.wired.com/2014/03/bitcoin-currency_martin/
- 6) https://www.youtube.com/watch?v=4NZCWABWplE 14:50
- 7) https://www.youtube.com/watch?v=WUEksnNgyOI&feature=youtu.be
- 8) http://www.amazon.com/Fair-Value-Accounting-Fraud-Techniques/dp/0470478586/
- 9) https://www.youtube.com/watch?v=NmAtmn7cvdo
- 10) http://bitcoinmagazine.com/9435/markets-institutions-currencies-new-method-social-incentivization/
- 11) http://forum.ethereum.org/discussion/747/i-m-not-understanding-why-dominant-assurance-contracts-are-so-special#latest
- 12) http://forum.ethereum.org/discussion/392/deodands-dacs-for-natural-systems
- 13) http://thoughtinfection.com/2014/02/22/we-are-becoming-programmable-society/
- 14) http://blog.ethereum.org/2014/02/24/daos-are-not-scary-part-1-self-enforcing-contracts-and-factum-law/
- 15) http://www.wired.com/underwire/2014/03/geeks-guide-karl-schroeder/
- 16) http://bitcoinism.blogspot.co.at/2013/12/lex-cryptographia.html
- 17) https://github.com/dafcok/ethereum
- 18) http://forum.ethereum.org/discussion/698/help-with-crowdfunding-contract
- 19) http://forum.ethereum.org/discussion/751/so-i-designed-a-concept-ui-for-the-alephzero-client
- 20) Timothy Swanson, 2014: Bitcoin Hurdles: the Public Goods Costs of Securing a Decentralized Seigniorage Network which Incentivizes Alternatives and Centralization http://www.ofnumbers.com/wp-content/uploads/2014/04/Bitcoins-Public-Goods-hurdles.pdf
- 21) http://letstalkbitcoin.com/e99-sidechain-innovation/
- 22) https://www.youtube.com/watch?v=teNzIFu5L70
- 23) http://letstalkbitcoin.com/e95-the-captain-and-the-keep/#.UzlVl9zE516 @ 15:00
- 24) https://www.youtube.com/watch?v=1QKQtoYqNbw
- 25) http://www.reddit.com/r/ethereum/comments/21atw1/vitalik_on_hard_problems_in_cryptocurrency_at/

source(s): []