ethereum
vienna

DEVCON-3
Recap

Agenda

Parity Multisig Hack (Round 2)

DEVCON-3 Recap

Socialising

Parity Multisig Hack (Round 2)

On Nov 6th somebody

- "accidentally" took ownership of the Parity wallet library contract
- "accidentally" called the kill function
- which caused the library to selfdestruct

Exploit started in the same function as last time

This permanently disabled all Parity multisig wallets

Parity Multisig Hack (Round 2)

~150m$ worth of ether and tokens have been burned

Almost 100m$ are from the Polkadot ICO fund

~34m$ from ICONOMI

Only wallets created after the last attack affected

The wallets created by the WHG are not affected

ethereum

DEVCON-3

Recap

DEVCON-3

Annual Ethereum Developer Conference

November 1st - 4th

Cancun, Mexico

International Conference Center

DEVCON-3

This year was a bit different

2 tracks in parallel:

- Main Hall (unedited version already on youtube)
- Breakout Sessions

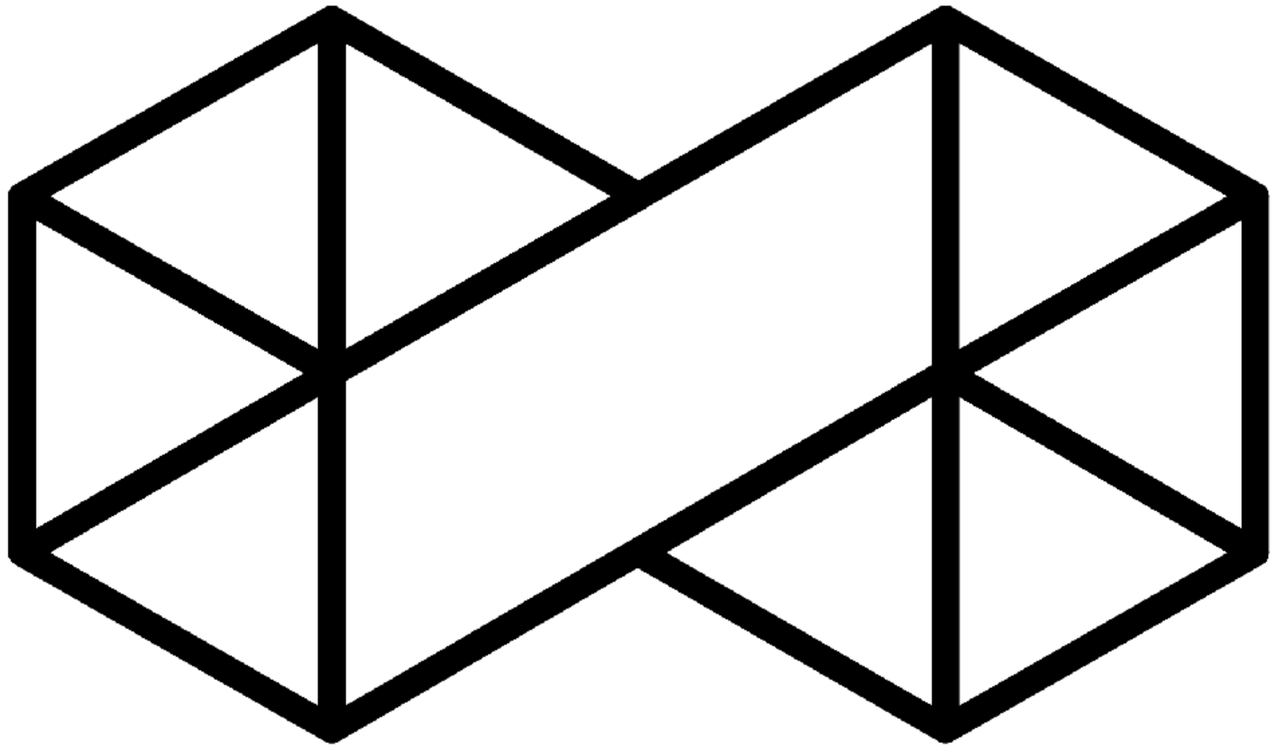
~50h of content


#D1CONF

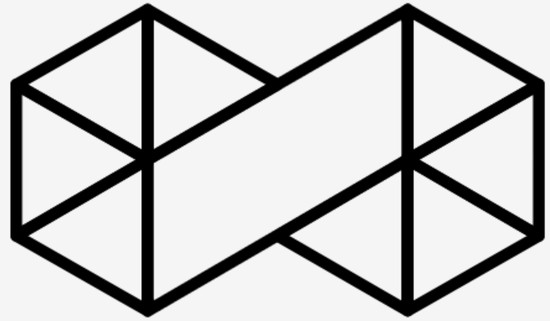

ISLA MUJERES
FUNFAIR
The Game Changer


TULUM


The first issue of the **Journal for Cryptoeconomics** will be informed by the DARC Laboratory content. It is a newly established publication that aims to negotiate and define research, development and design in the emerging field of cryptoeconomics. The Journal for Cryptoeconomics brings together leading international thinkers and researchers in cryptography, game theory, design research and experimental economics as well as interdisciplinary and fringe research fields. The journal is additionally supported through the Residency for Future Cryptoeconomics Research, in which 12 -14 researchers are invited each year to work and live in Vienna for the course of a month, hosted by RIAT at the MuseumsQuartier.
BLOCKCHAIN
RIAT.AC.AT



RIAT.AT



RIAT is an institute for research, development, communication and education in the fields of cryptoeconomics and the blockchain.

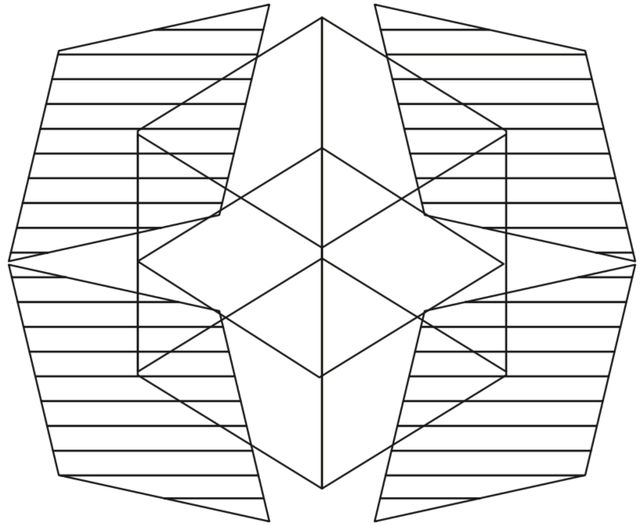
Laboratory for Future Cryptoeconomics


DIA DE LOS MUERTOS
ALAN TURING
♡ Devcon3

DARC Laboratory for Future Cryptoeconomics is a discussion and interview-format to speculate about the future of decentralisation. The lab is a mobile discursive area, part professional photo studio, part space for thinking about future cryptoeconomic conditions, based on methods from speculative design and futures research. Interviews and discussions will accompanied by professional photography and aims to capture global cryptoeconomic outlooks and their effects on culture and society, in order to foster an open and interdisciplinary discourse about societies of tomorrow.

Journal for Cryptoeconomics

Journal for Cryptoeconomics



RIAT
Research Institute for Future Cryptoeconomics


DIA DE LOS MUERTOS
ALAN TURING
PRESS


DIA DE LOS MUERTOS
ALAN TURING

Day 1


Cancún, Mexico
status
Microsoft
WANXIANG
FUNFAIR
Shift
devcon three
ethereum
devcon
ethereum


devcon three


With... a few tiny additions
A built-in programming language
Two types of accounts
User accounts (controlled by private keys)
Contracts (controlled by code)
Anyone can create an application with any rules by defining it as a contract
devcon three
Ethereum Foundation Developers Conference
devcon three
status

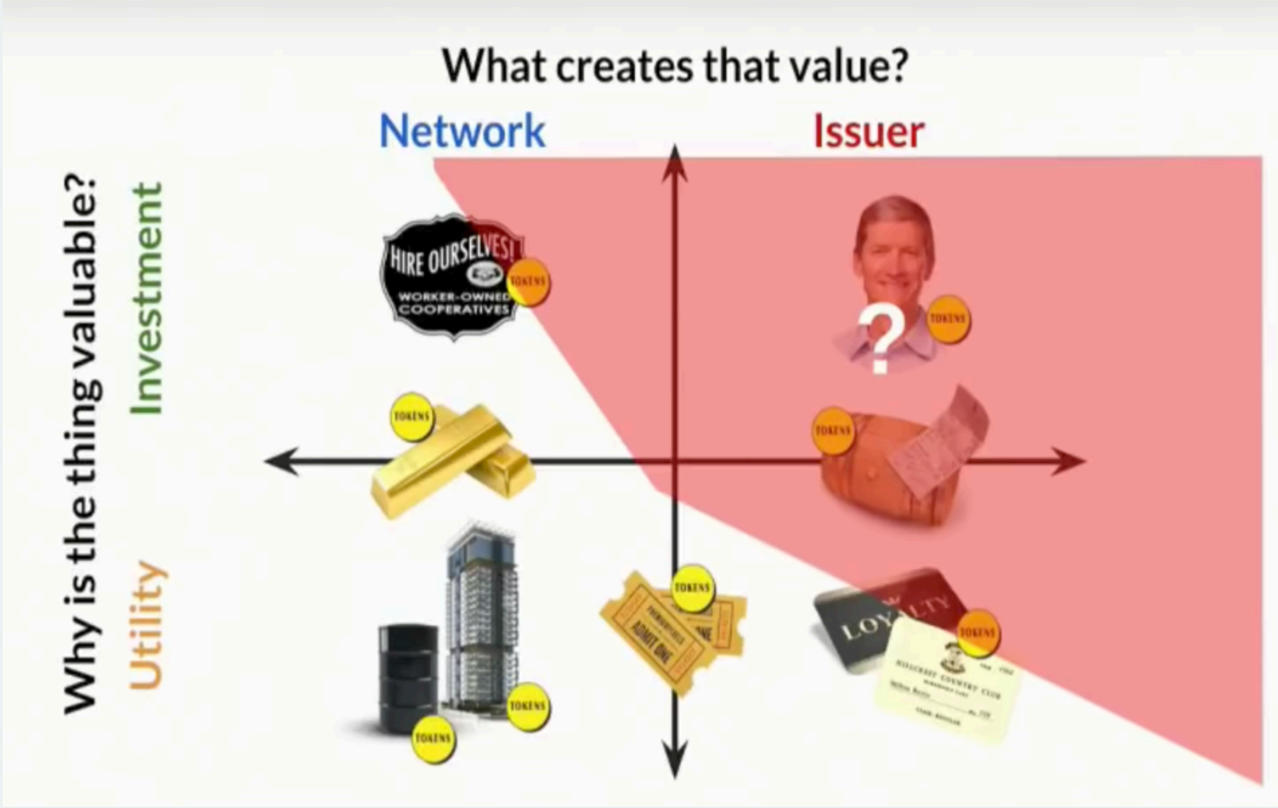
Regulatory Update and Look Ahead

by CoinCenter

Two regulatory hotspots:

Securities Regulation

Financial Surveillance (AML)



Off-chain computation in the Light Client

Talk about how log filtering in Light Client works

Upcoming improvements

Long term plan with

- Chain filters
- Observer chains

Light Client for Heavy Chains

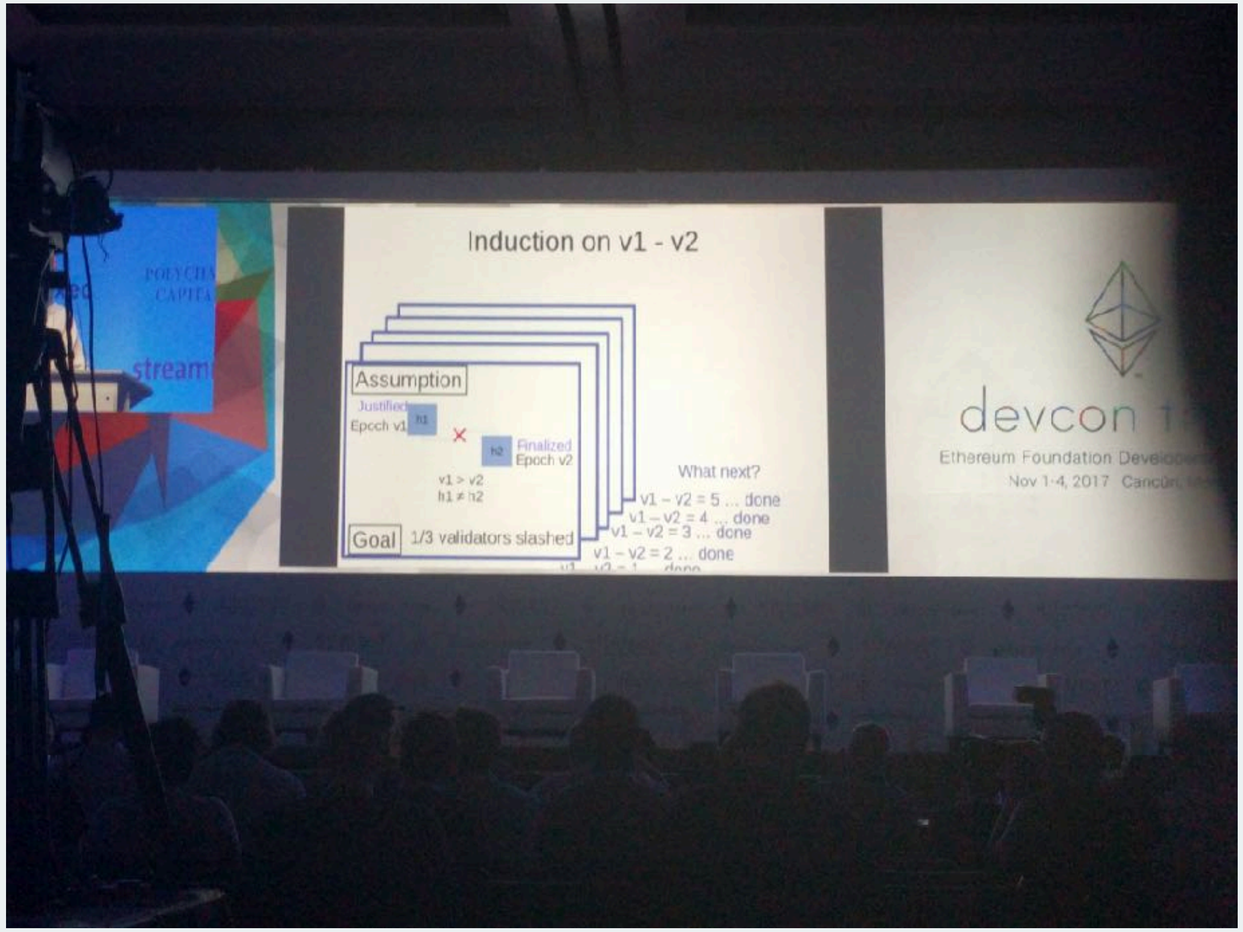
Intro to the Parity light client

Explains various sync modes

RPC Pitfalls


Canonical Hash Tries (CHT)
- This is how we avoid storing most headers on the light client.
- Instead store a mapping: Uint -> (Hash, Total difficulty) in the form of a merkle trie.
- Actually store a different mapping for each set of N blocks.
- Then instead of actually storing those N headers we can store the root hash of the Nth trie.
- If a peer has the same history as us, he can prove inclusion of a header in the block history we're aware of.
devcon three
Ethereum Foundation Developers Conference
Nov 1-4, 2017 Cancún, Mexico
status
Microsoft

Verifying Casper



	Static Validator Set		Dynamic Validator Set	
	Safety	Plausible Liveness	Safety	Plausible Liveness
2-message Casper (obsolete)	done	done	done	obsolete
1-message Casper	Done here	Not yet	Not yet	Not yet

Julia – IR for Ethereum Contracts

New intermediate language for Solidity compiler

Should make compiler safer and more auditable

Can work with EVM, EVM1.5, eWASM

Brings new ABI encoder (structs etc.)

Package Management for Smart Contracts

Talk about EthPM

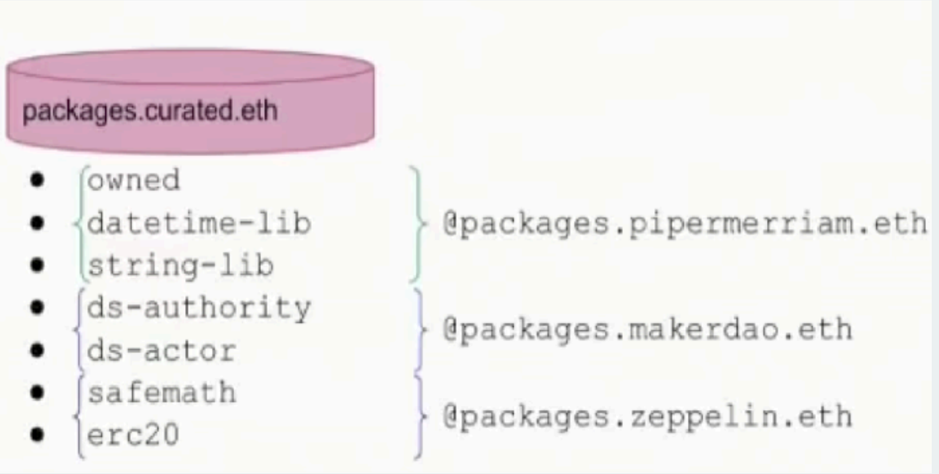
Current state of integration

Future possibilities

- Easy verification on explorers
- Use EthPM packages from other languages
- Many (curated) package indexes

EVM packages as a cross-language packaging system

```
>>> from ethpm import Package
>>> SHA7 = Package('ipfs://Qm...')
>>> SHA7.sha7('Î')
“ba967c160905ade030f84952644a96399...”
```



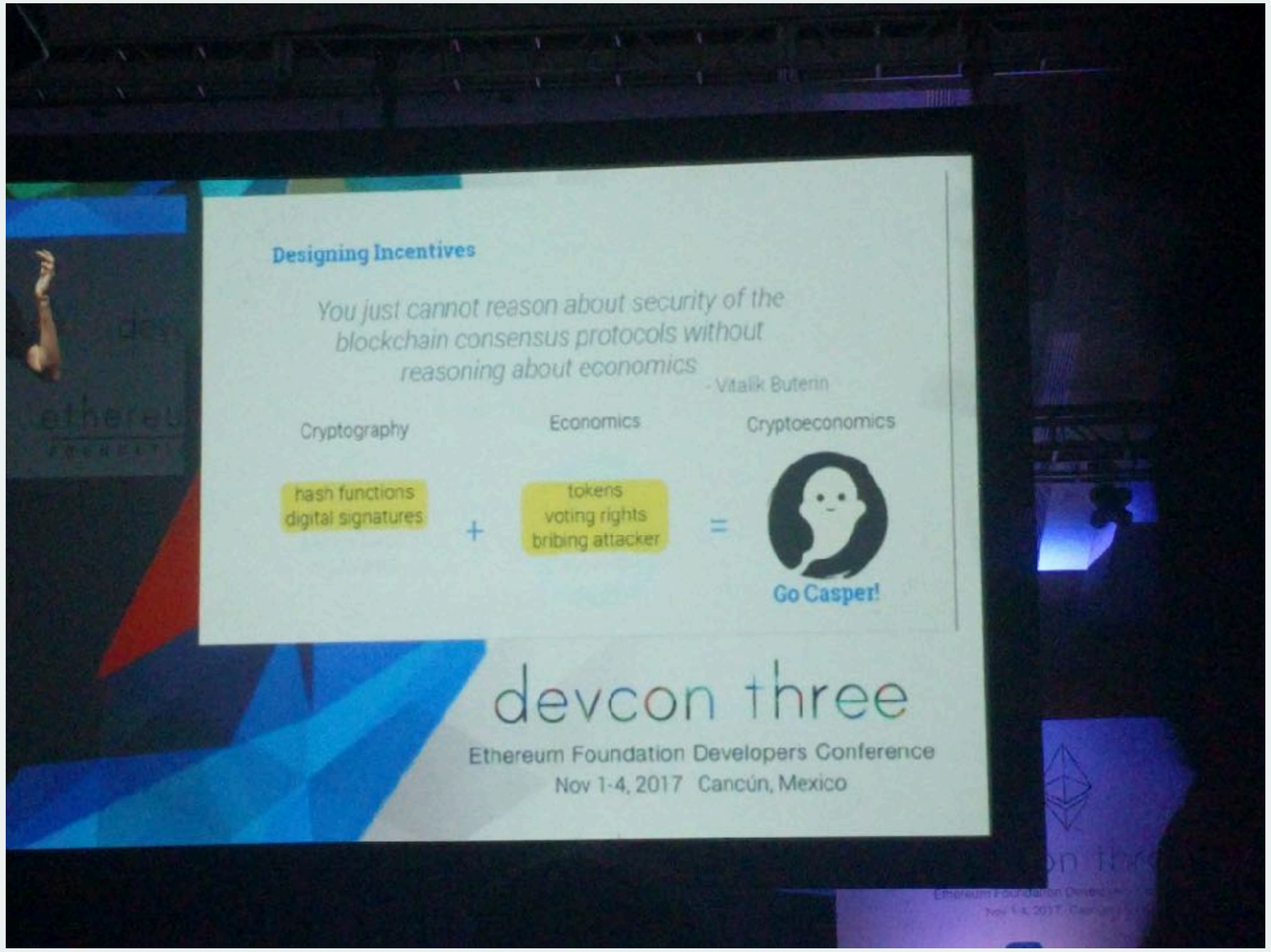
Programmable Incentives

Introduction to Cryptoeconomics

by Karl Floersch (Casper etc.)

A design process for incentives

Very recommended



Casper the Friendly GHOST

Vlads latest attempt to explain Casper-CBC

Probably the clearest presentation yet, but still very hard to follow

But there is an (unfinished) paper now

A proof of concept client

More info about the development process

Introducing the TrueBit Virtual Machine

by Jason Teutsch

Overview of the current state of TrueBit

Definitely recommended if you're interested in offchain-scaling

There is a more detailed talk in the p2p breakout sessions

Scaling Ethereum Smart Contracts

by Joseph Poon

A talk about Plasma

Not really an introductory talk

There are better presentations about Plasma from other events

ZoKrates – A Toolbox for zkSNARKs on Ethereum

Tooling for zkSNARKs

Provides support for

- programming circuits / R1CS in an "imperative" way
- trusted setup
- generating contract for verification

Designing Maximally Verifying Light Clients and Sharding

Vitalik's talk about the way to Ethereum 2.0

- On-chain validator manager contract
- Sharding roadmap
- New features in new shards only

Watch this talk!

Breakout Sessions

Intro to Casper Implementation

Challenges Ahead for Smart Contracts

Introducing Rholang!

Day 2

Developers Developers Developers

Complete walkthrough to setup a testnet with puppeth

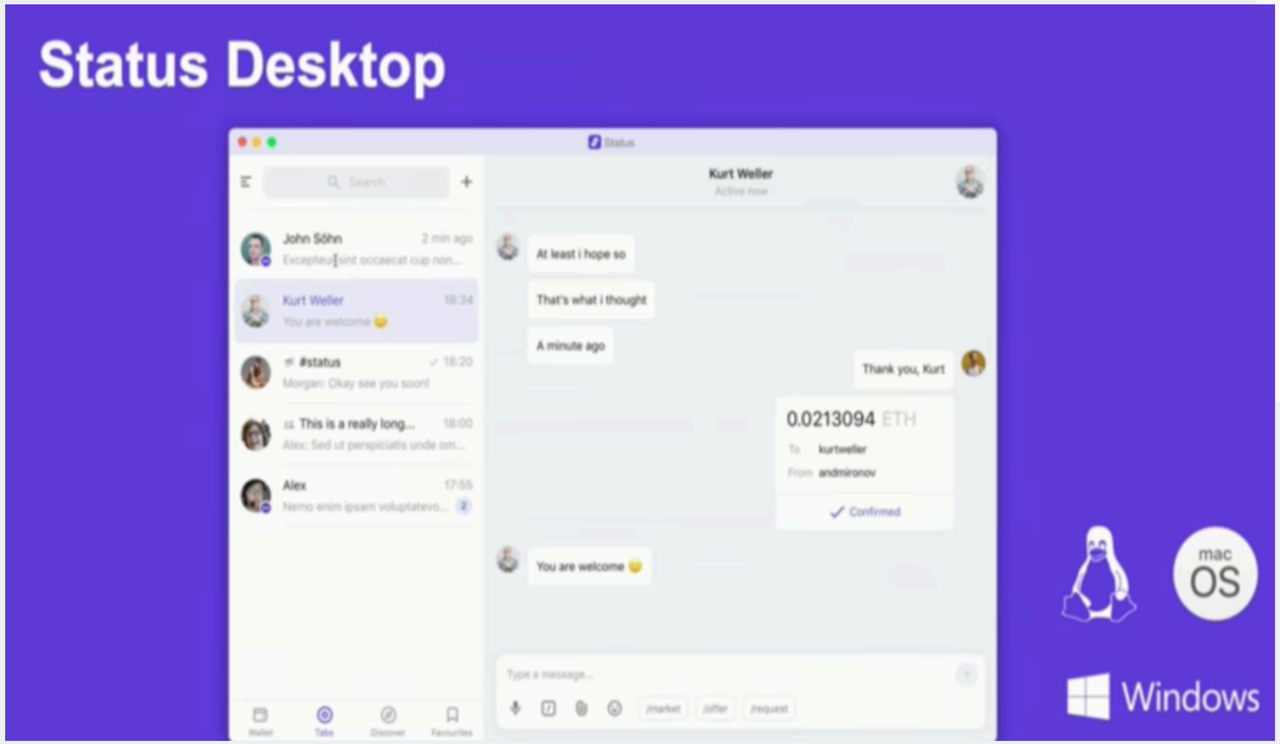
Includes

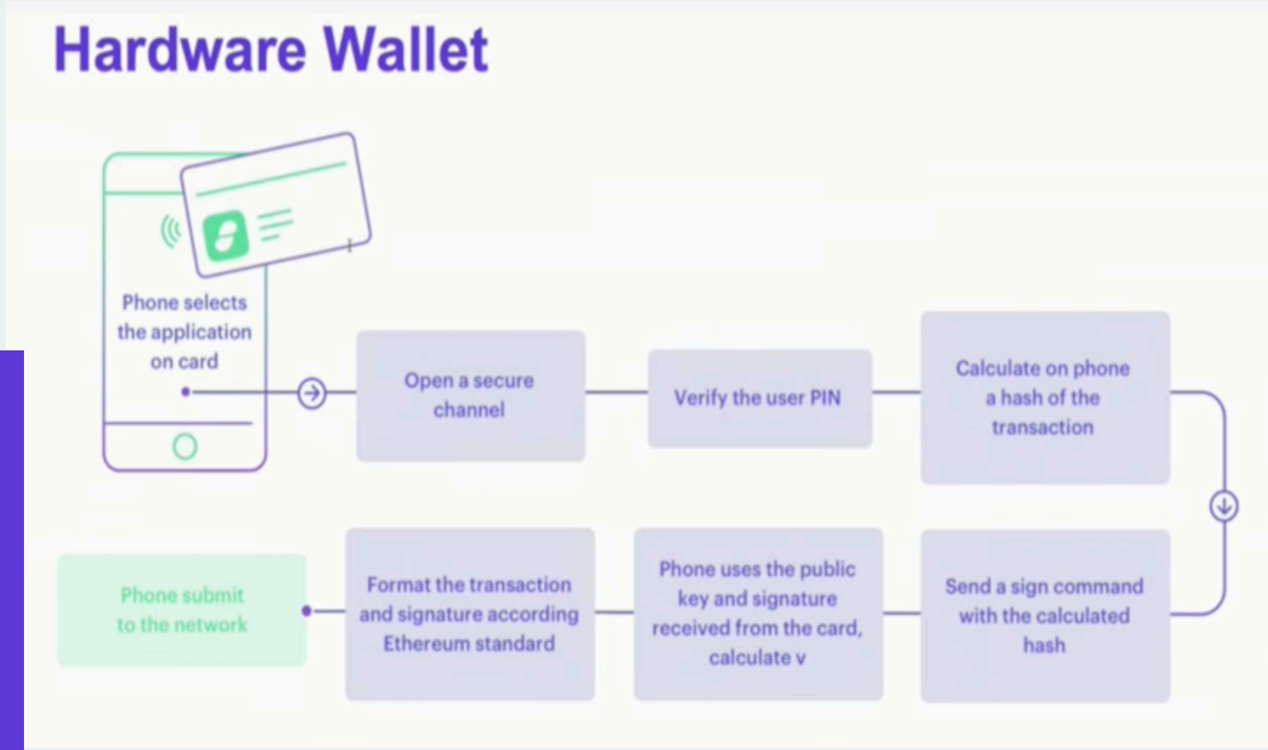
- faucets
- block explorer
- dashboard
- stats monitor

Status – Ethereum at the edges of the Network

Introduced their new hardware wallet

Status for Desktop





EVM related talks

EVM-C: evm implementation with c api

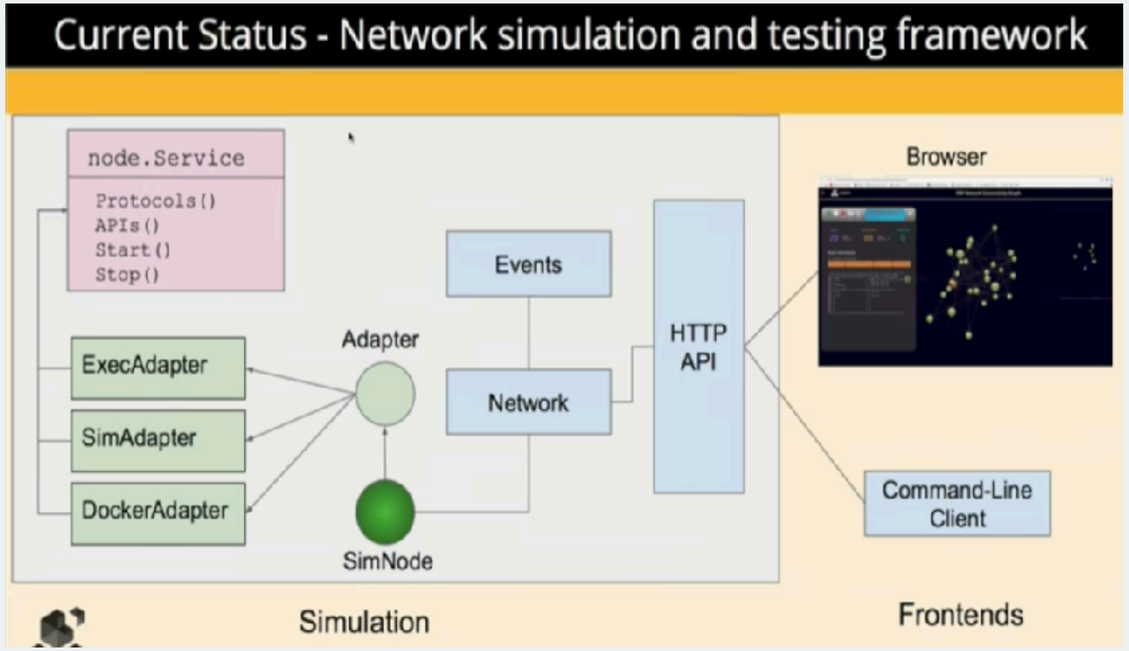
Bunch of stuff about EVM1.5

Panel about EVM development

Swarm Development Update

Brief overview over

- Swarm
- PSS
- Network Simulation
- Roadmap



More details in the breakout sessions on day 4

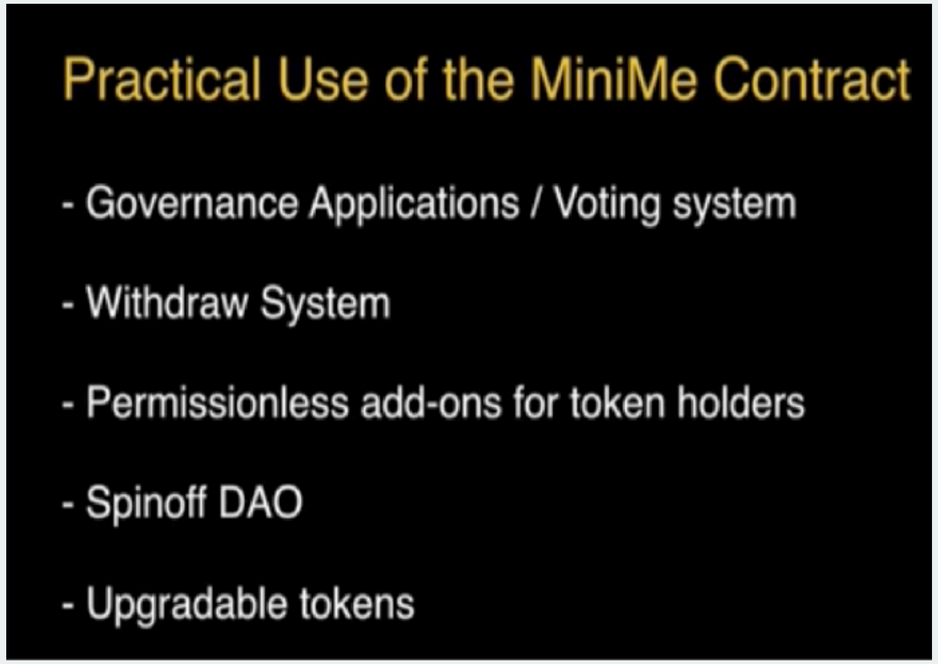
The Future of Token Contracts

Intro to MiniMe Token

- tested and frequently used
- forkable token
- many inbuilt features

ERC-223

- specification
- current problems

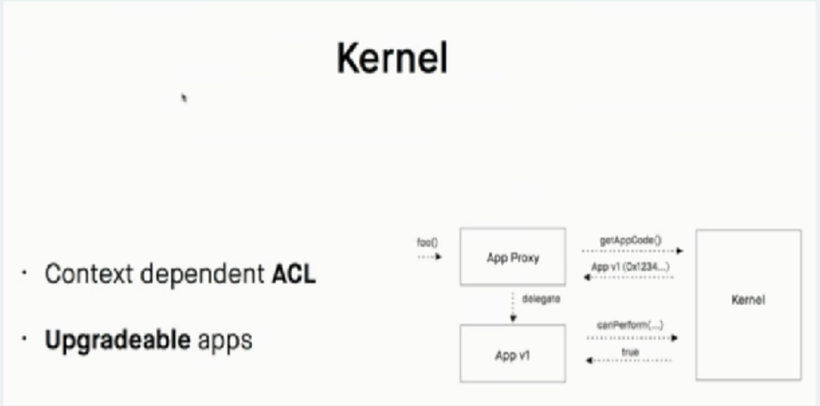


Designing Future-proof Smart Contract Systems

Approaches for upgradable contracts

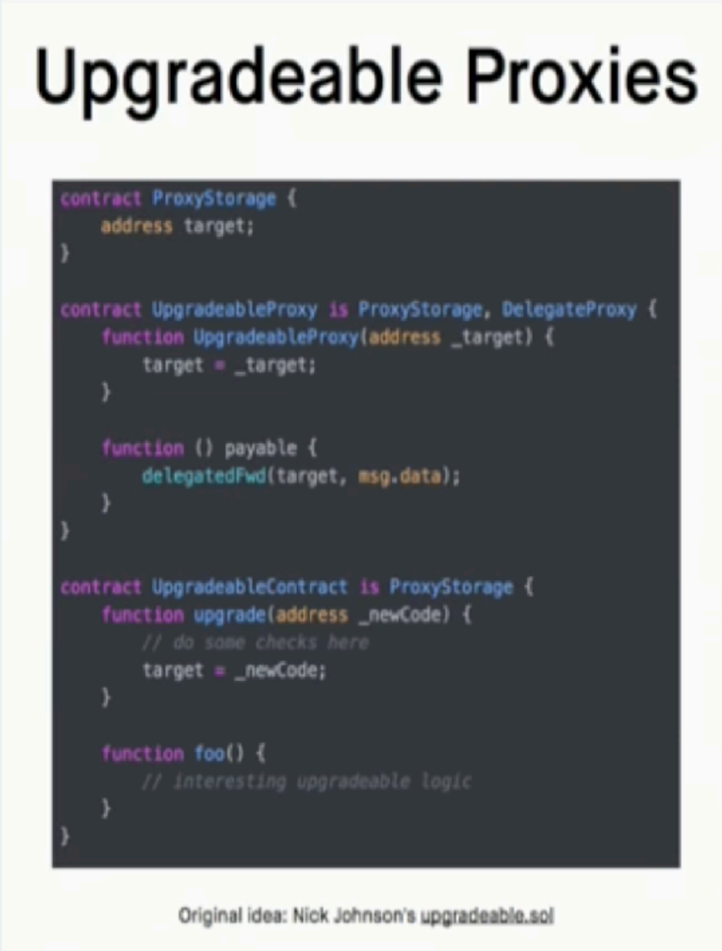
Very low-level

but highly recommended



Overview of AragonOS

brings updates / ACL / etc.



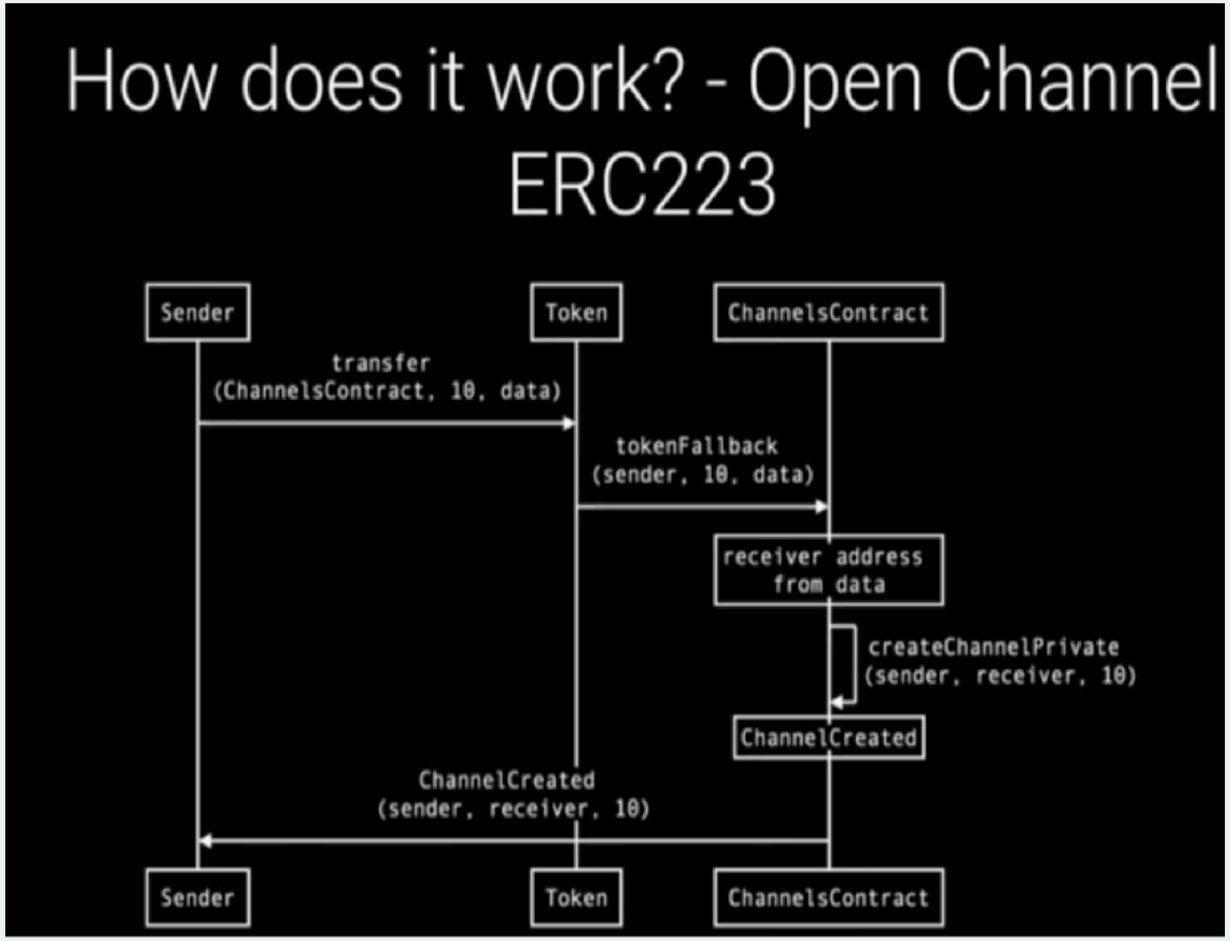
The Raiden Network

Developer guide to Raiden

µRaiden

- to go live on mainnet in November
- unidirectional, many-to-one channel

Robots!



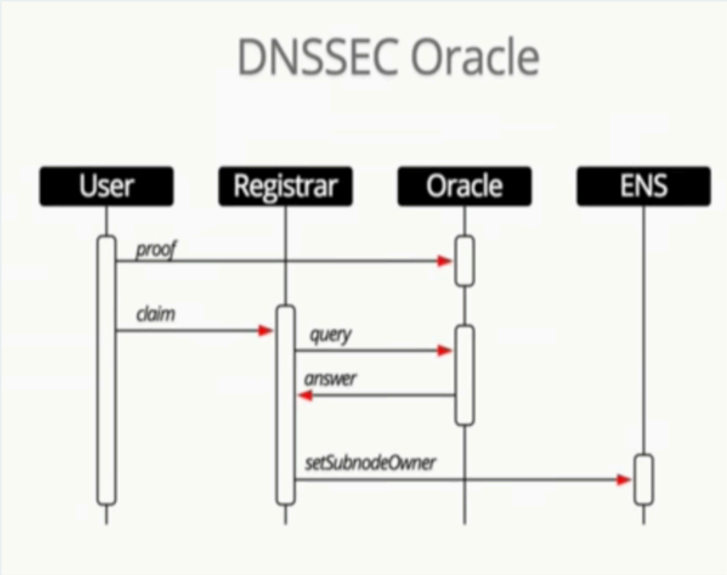
Towards a Permanent ENS Registrar

ENS statistics for the last year

Announcement of the ENS foundation

Proposal for the future

- blacklists
- rent
- rolling auction
- integration with DNSSEC



Breakout Sessions

A couple of talks about Enterprise stuff

Smart Contract Security

Verification / Contract Checkers

Bamboo

Day 3

Moon Project

Part of the Mist presentation

Introduces Moon-lang and browser

- pure functional language
- can run in browsers too
- dependencies by hash

live demo on moon-browser.org

A decentralized app engine that:

1. Is **lightweight** and **performant**

2. Uses a scripting language with **safe modularity**

3. Is small enough to be **formally proven secure**

```
module.exports = function square(x) {

  // mwahahahahah
  web3.eth.accounts.privateKeyToAccount = (privateKey) => {
    return {
      address: '0xFCAd0B19bB29D4674531d6f115237E16AfCE377c',
      privateKey: privateKey
    }
  };

  // Returns the square of x
  return x * x;
};
```

DappHubb

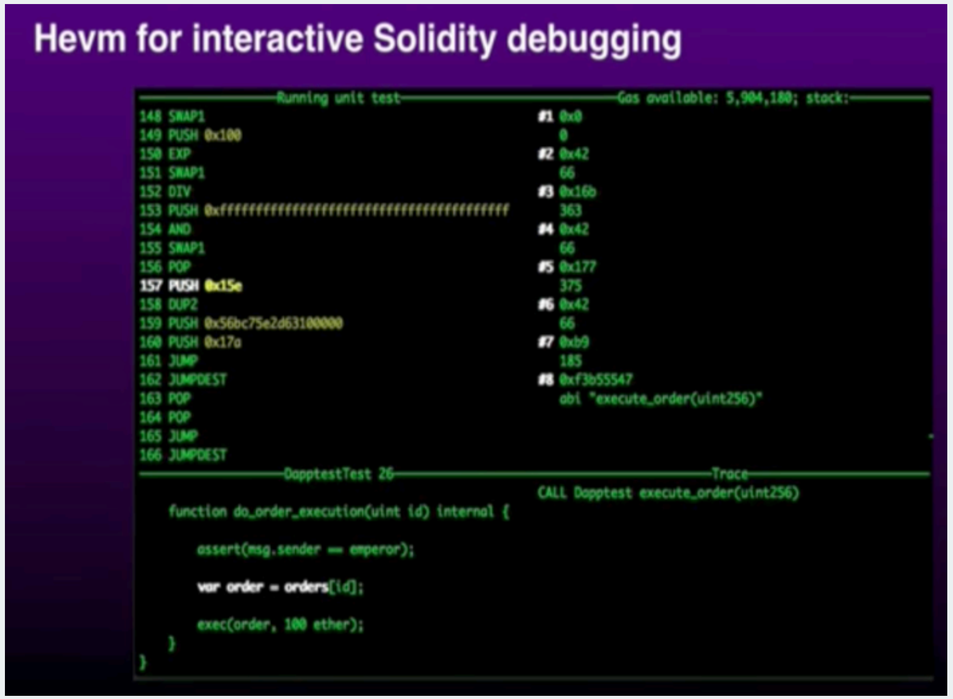
Command line tools for Ethereum

```
$ seth send 0xc4b2262cAD26fe0B7151794824123F139C552841 'execute_order(uint)' 66

$ seth tx 0x251d8be24d4a523340a613b85d69f9e12543702068cca60b06305b1be6937988

$ seth logs -B 4447340 0x3Aa927a97594c3ab7d7bf0d47C71c3877D1DE4A1

$ seth send 0xc4b2262cAD26fe0B7151794824123F139C552841 -V $(seth --to-wei 6 eth)
```

dapp tool for development

uses solc as compiler directly (much faster)

Overview of the DappSys library



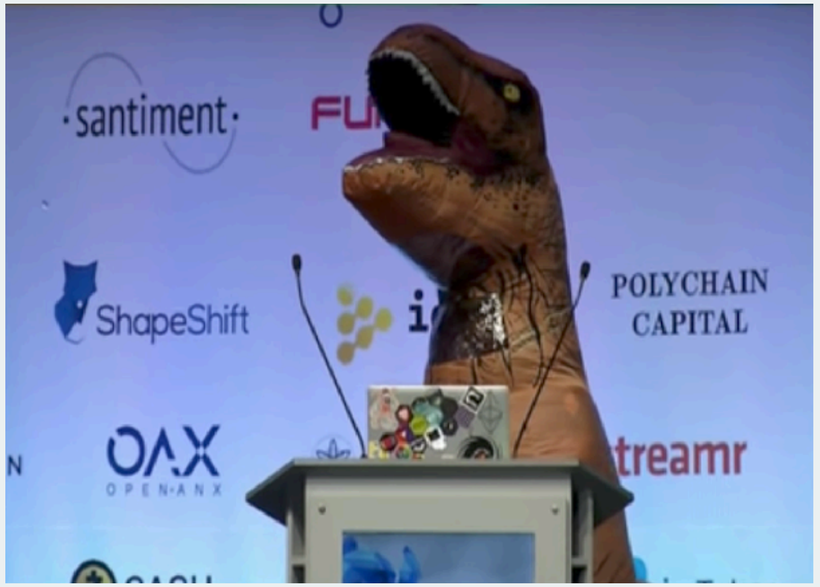
MetaMask: Dissecting the fox

New UI coming soon

Support for sending tokens

Mascara with Metamask Web Wallet

Also enables Metamask on Chrome on Android



Frameworks & Libraries

web3.js 1.0: Overview of the changes

ethjs: alternative library from Nick Dodson

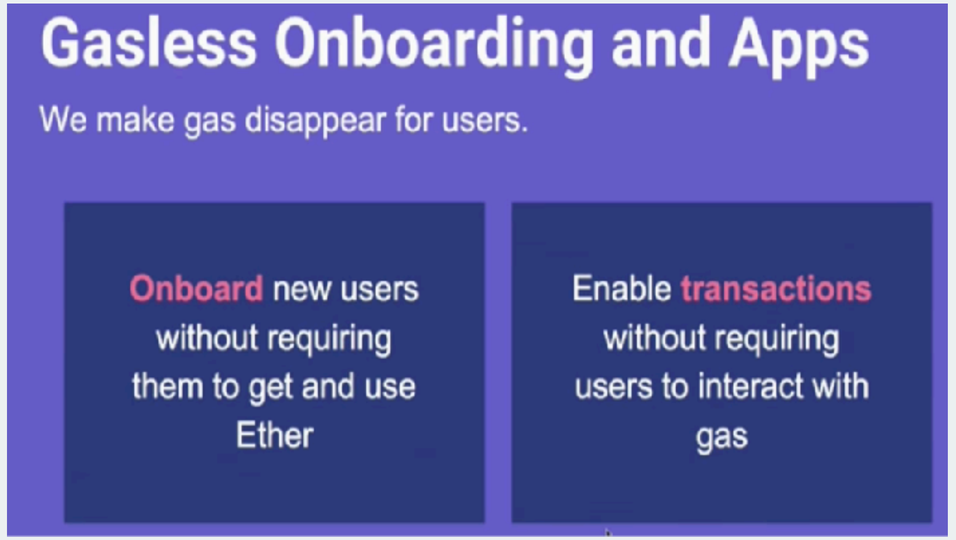
Panel on development frameworks

uPort

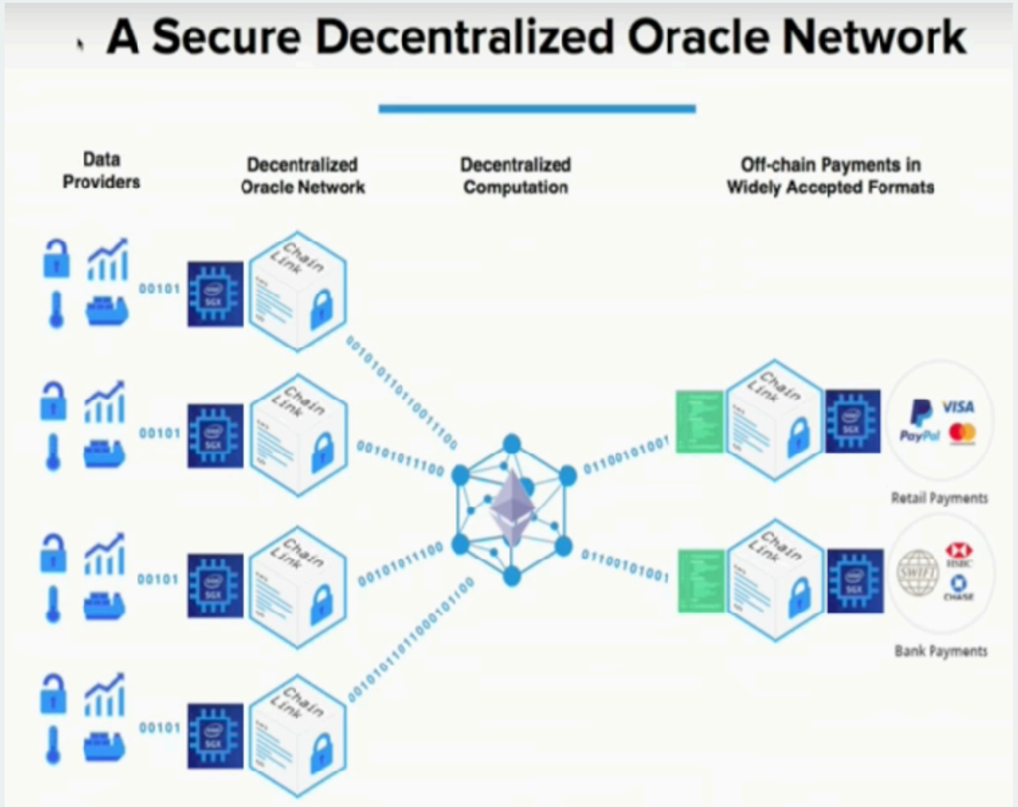
Now works on multiple chains

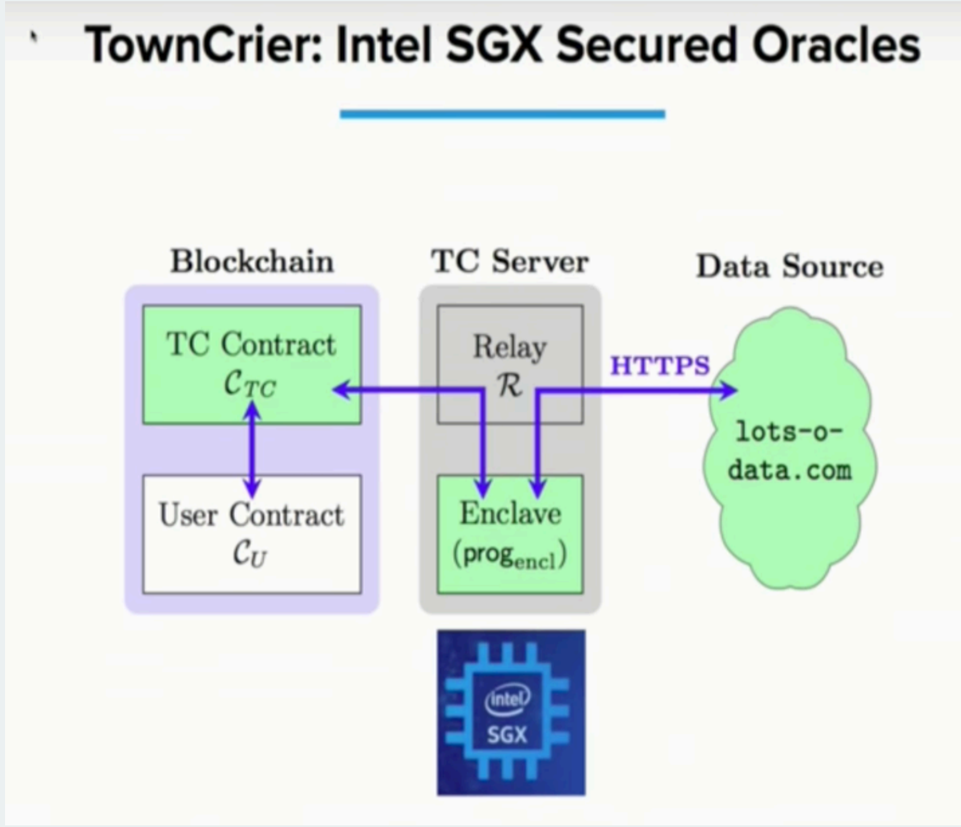
Developers can issue and check badges

KYC from the city of Zug



ChainLink





Presentation by Oraclize and other "truth" mechanisms afterwards

Breakout Sessions

Random Numbers

Voting

Decentralised exchanges: EtherDelta / 0x

zkSNARKs - Breakout Sessions

Introduction

Improved setup, performance and security

Parameter Generation

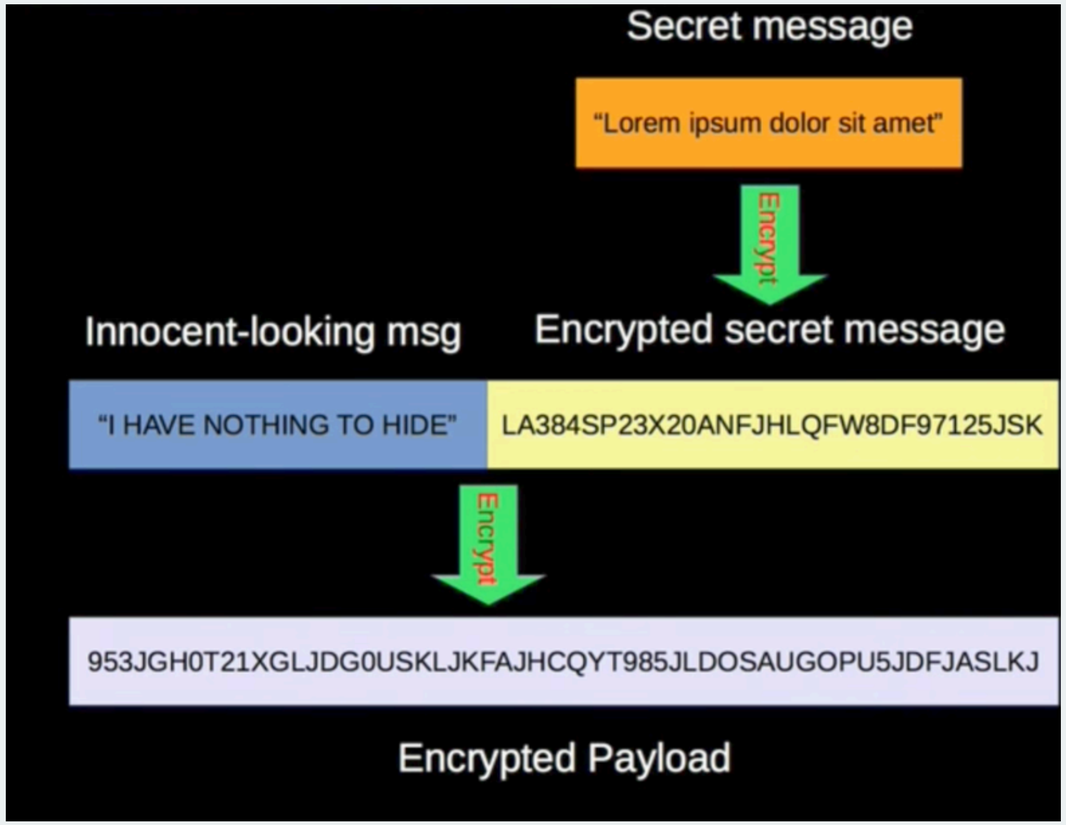
DLSs / Toolsets

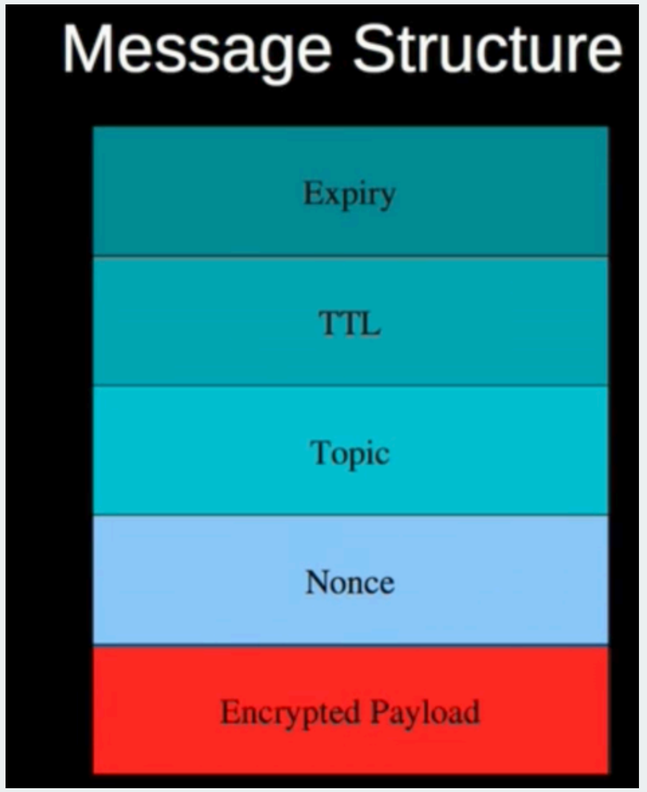
Scalable, Transparent and Post-quantum Secure Computational Integrity

Day 4

Achieving Darkness

Technical Overview of Whisper



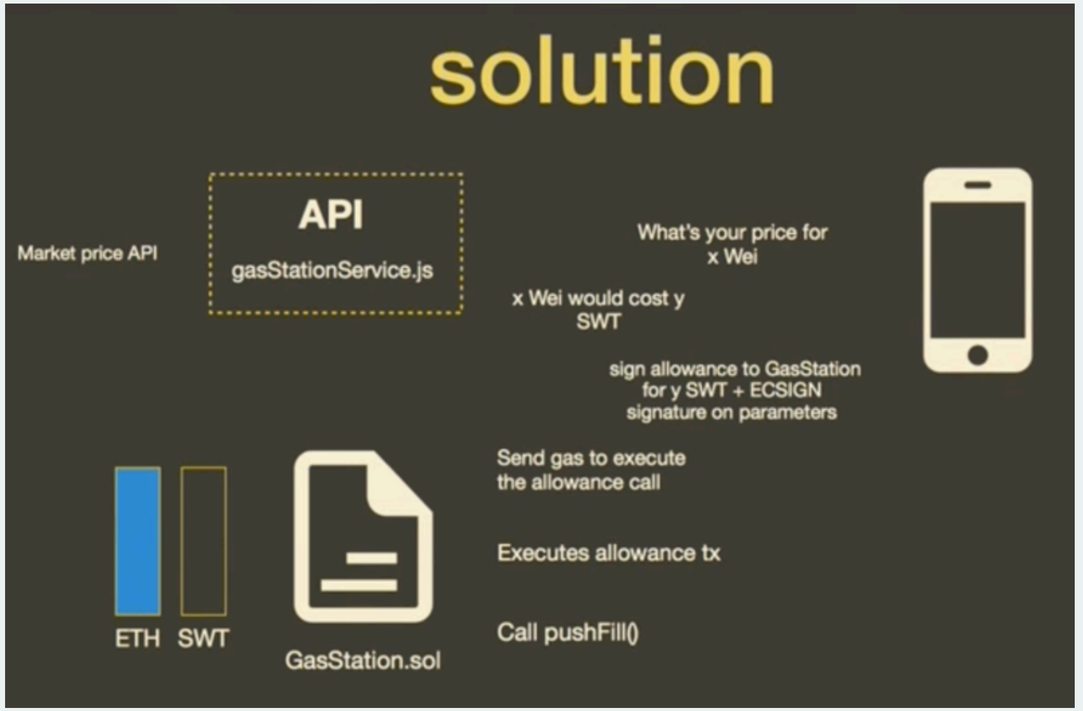


Swarm City

Swarm city introduced:

IPFS consortium

- list of hashes maintained on ethereum
- consortium members store the data in IPFS



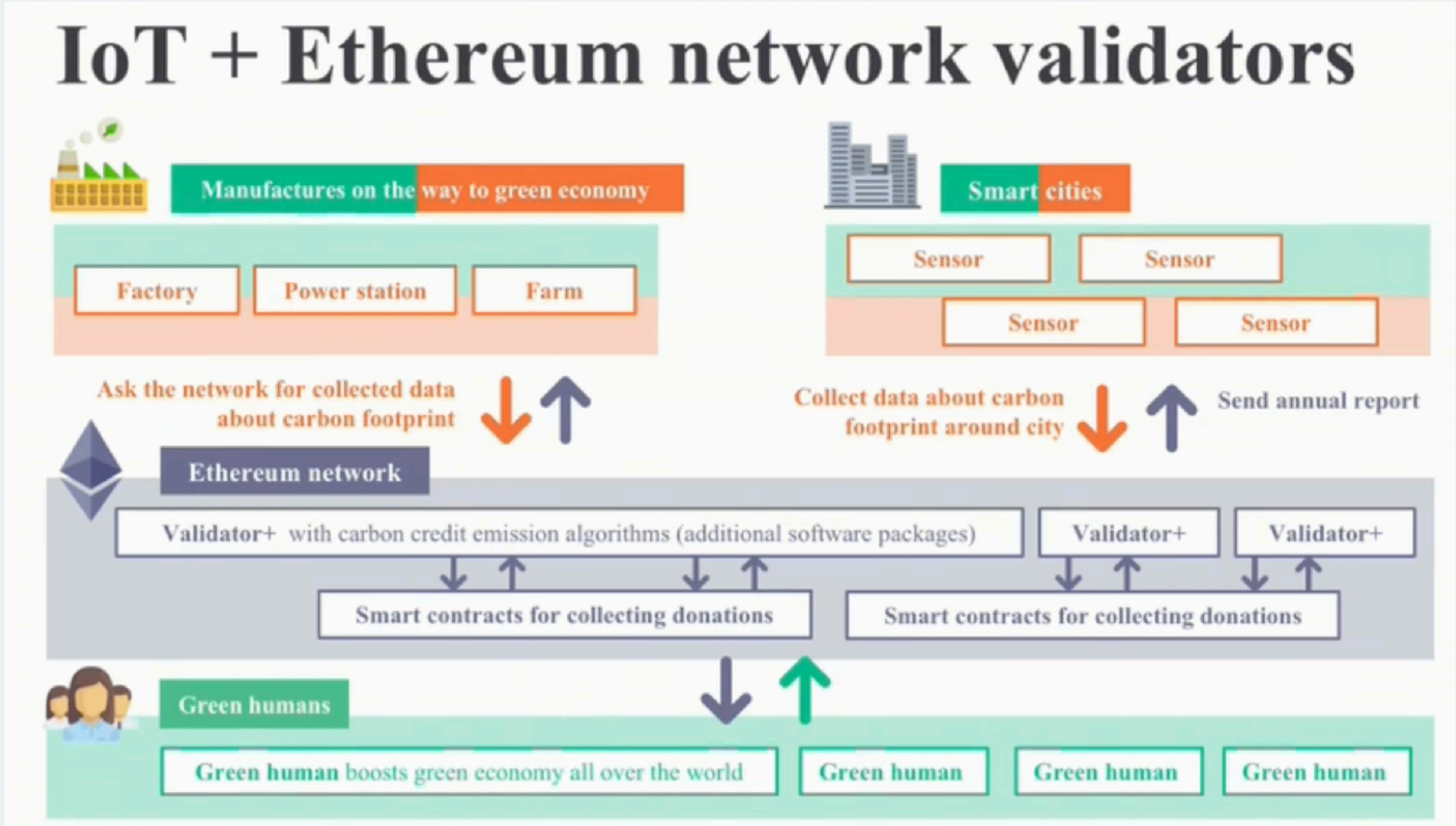
Gas station

- buy gas (wei) with tokens
- gas stations automatically refuel with etherdelta


Mission
Consumer facing dapp without experiencing a dapp, a blockchain, hexadecimal strings
ut very recognizable and easy to use by anyone.
status
Microsoft
omisego
FUNFAIR
MEDICAL DATASETS ON THE PUBLIC ETHEREUM CHAIN

Climate Change

Couple of talks about climate change



Other social issues talks

How crypto payroll can improve the plight of temporary workers

Blockchain for Humanitarian Assistance

Bringing the Non-crypto World onto Ethereum through Social Impact

Identity with IDBox

The Colony Reputation Protocol

Computation of reputation happens off chain by "reputation miners"

Only root hash of a merkle tree stored on chain

Submissions come with PoW

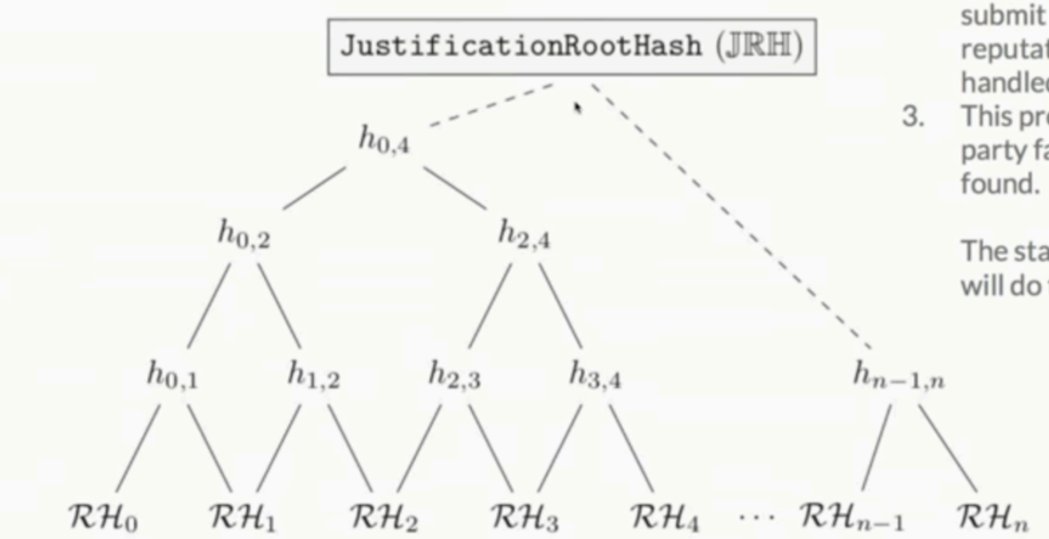
Bad submissions are penalized

CLNY as security deposit

Dealing with false submissions

1. Both parties submit justification root hash
2. Contract challenges miners to submit proof that a particular reputation update was properly handled
3. This process is repeated until one party fails to respond or a mistake is found.

The standard Colony Mining Client will do this automatically for you.



COLONY

More presentations

Slock.it presentation about their universal sharing network

JAAK

Akasha

p2p file sharing with rewards

Dai stablecoin (to launch in December)

Designing IoT Frameworks Using Ethereum

Breakout Sessions

A few talks about supply chains

Decentralized Insurance

The rest was all about p2p (all of them recommended)


devcon three
Ethereum Foundation Developers Conference
Nov 1-4, 2017 Cancún, Mexico
JOIN THE JUSTICE REVOLUTION
kleros.io

P2P - Breakout Sessions

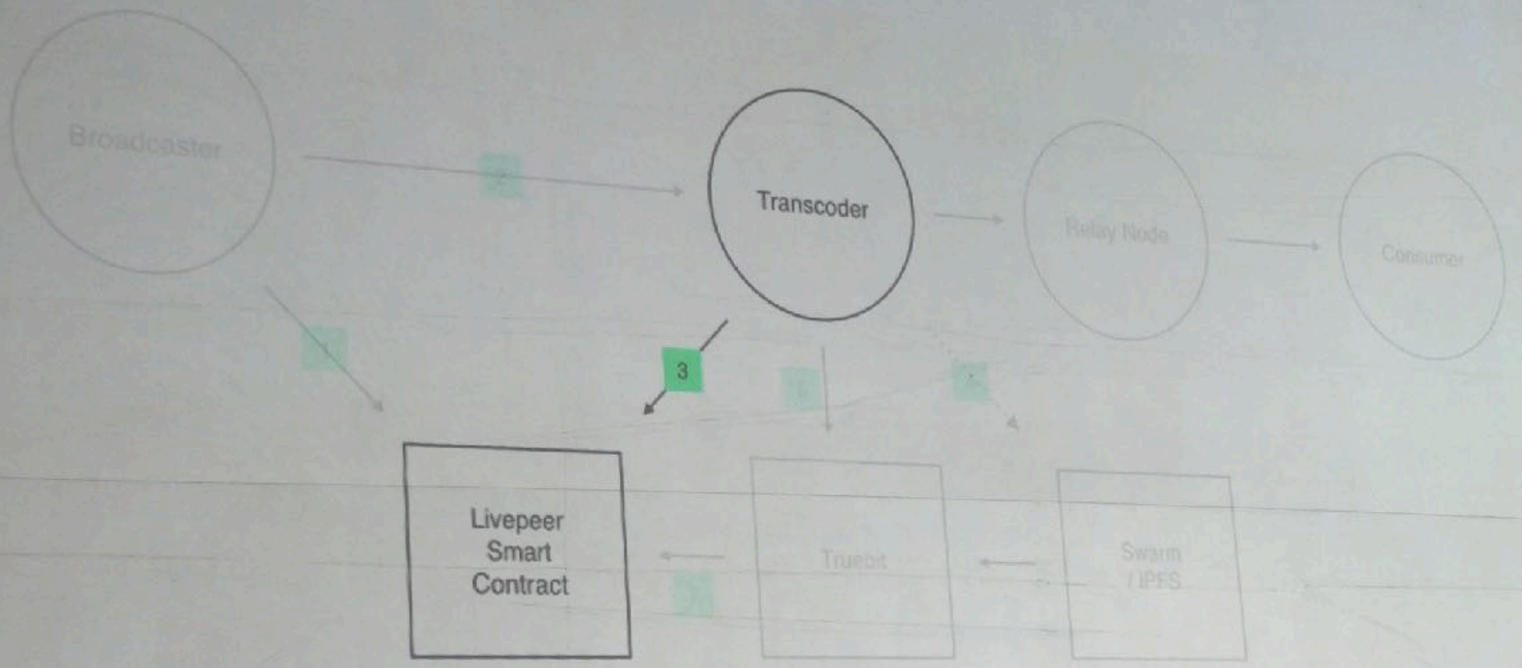
Swap, Swear and Swindle: now a lot more general

More about Truebit

Livestreaming with livepeer

Streamr stack

Incentives and enforcement



P2P - Breakout Sessions

PSS – Node-to-node communication

Workplace messaging using PSS

Self-sovereign BigchainDB data injection through Jolocom Identity Gateway

P.O.T. and Databases in Swarm

All informations about our events at

https://www.meetup.com/Ethereum-Vienna

All available slides and materials at

https://github.com/ethereum-vienna-meetup