ethereum

vienna

General Introduction

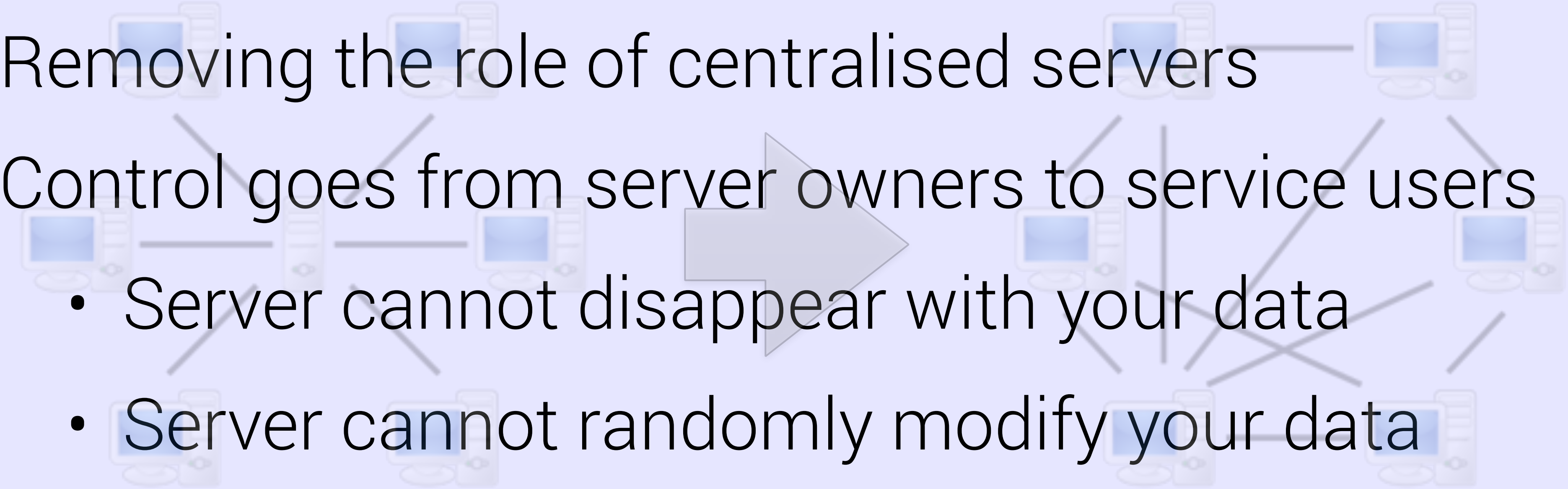
ethereum Project

Decentralisation of the web

Removing the role of centralised servers

Control goes from server owners to service users

- Server cannot disappear with your data
- Server cannot randomly modify your data
- Server cannot freeze your funds
- Censorship resistant



ethereum Web 3.0

ĐApps (decentralised applications)

- **Ethereum** (Blockchain)
    - Agreements
    - Relationships
- **Whisper** (Messaging)
    - Messaging
    - Broadcasting
- **Swarm** (Content System)
    - Data publication and distribution

ethereum ĐApps

Escrow Bitcoin Multisig

Crowdfunding Lighthouse

Subscription services

Prediction Markets

DNS Namecoin

Decentralised autonomous organisations

Marketplace OpenBazaar

Betting

Subcurrencies

ethereum Blockchain

Public Record that tracks state

Stored and processed by all participants (full nodes)

Maintains Accounts

- Ether / Wei Balance
- 160 bit address
- 2 types of Accounts
  - Externally owned (account)
  - Internally owned (contract)

ethereum Blockchain

Account (Externally owned)

User controlled account

Has a private key / public address

Can send and receive ether

0x1350cf34d093953ce0d2803648da8f3b6a84de77	100
0xd5f9d8d94886e70b06e474c3fb14fd43e2f23970	2500
0xd2963cd505c94dbf3bc663bdd2321bd3000204bb	2323000
0x75a4001939a7a990f786a74dade89dac1fcb3a51	2321453
...	...

ethereum Blockchain

Contract (Internally owned)

Has associated code (in evm byte-code)

Gets executed for every incoming transaction

No private key, ether can only be sent by code

Has a persistent 256-bit to 256-bit storage

Can send messages to other contracts

```
DUP2 SWAP1 SSTORE POP DUP5 DUP5 POP PUSH1 0x6 ADD
PUSH1 0x0 SWAP1 SLOAD SWAP1 PUSH2 0x1 0x0 EXP
SWAP1 DIV PUSH1 0xff AND PUSH2 0x6 0x88 JUMPI DUP5
DUP5 POP PUSH1 0x1 ADD PUSH1 0x0 POP SLOAD DUP4 LT
ISZERO PUSH2 0x5 0x8e JUMPI PUSH2 0x6 0x83 JUMP
JUMPDEST DUP5 DUP5 POP PUSH1 0x0 ADD PUSH1 0x0
```

ethereum Blockchain

Code written in an ethereum specific language

- Solidity

  high level

  official language

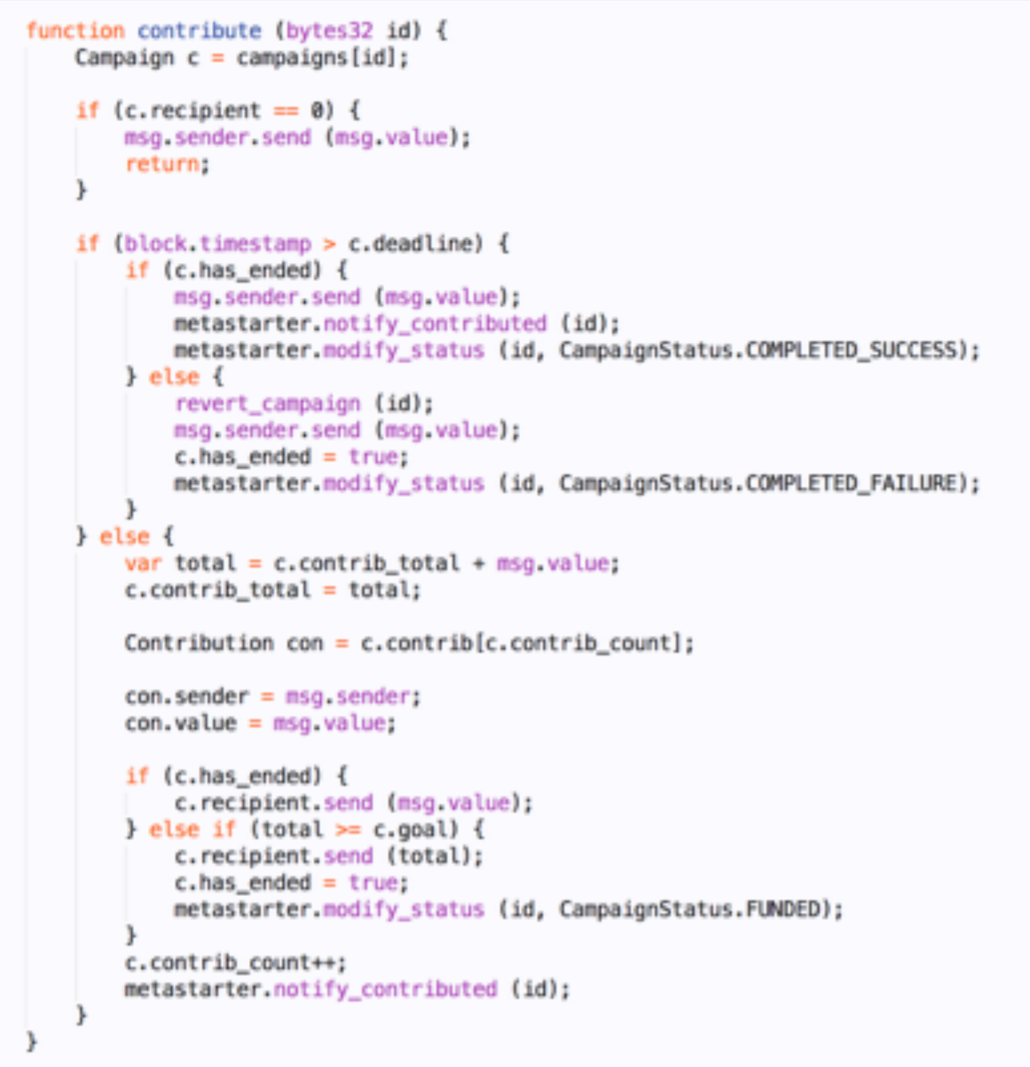
- Serpent2

  python-like

  no official support

- lll

  lisp-like (low-level)



```
function contribute (bytes32 id) {
    Campaign c = campaigns[id];

    if (c.recipient == 0) {
        msg.sender.send (msg.value);
        return;
    }

    if (block.timestamp > c.deadline) {
        if (c.has_ended) {
            msg.sender.send (msg.value);
            metastarter.notify_contributed (id);
            metastarter.modify_status (id, CampaignStatus.COMPLETED_SUCCESS);
        } else {
            revert_campaign (id);
            msg.sender.send (msg.value);
            c.has_ended = true;
            metastarter.modify_status (id, CampaignStatus.COMPLETED_FAILURE);
        }
    } else {
        var total = c.contrib_total + msg.value;
        c.contrib_total = total;

        Contribution con = c.contrib[c.contrib_count];

        con.sender = msg.sender;
        con.value = msg.value;

        if (c.has_ended) {
            c.recipient.send (msg.value);
        } else if (total >= c.goal) {
            c.recipient.send (total);
            c.has_ended = true;
            metastarter.modify_status (id, CampaignStatus.FUNDED);
        }
        c.contrib_count++;
        metastarter.notify_contributed (id);
    }
}
```

ethereum Blockchain

Message

1 sender, 1 recipient, 1 value

Contracts can spawn new messages

Can have additional data (contract parameters)

Can have return values

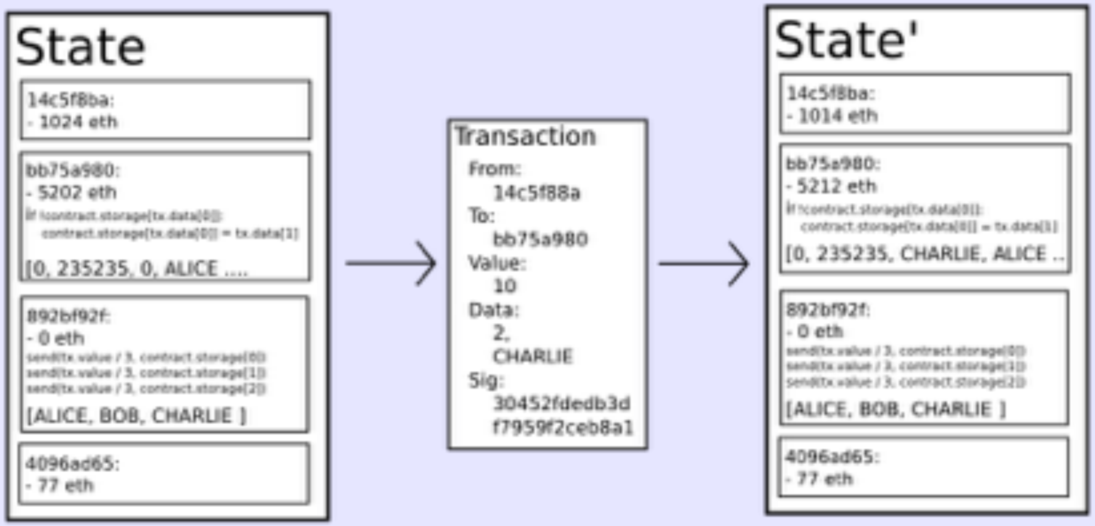
ethereum Blockchain

Transactions

Container for a message

Signed by private key (external account)

Transitions from one state to the next



State

14c5f8ba:
- 1024 eth

bb75a980:
- 5202 eth

```
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
```

[0, 235235, 0, ALICE ....

892bf92f:
- 0 eth

```
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
```

[ALICE, BOB, CHARLIE]

4096ad65:
- 77 eth

Transaction

From:
14c5f88a
To:
bb75a980
Value:
10
Data:
2,
CHARLIE
Sig:
30452fdedb3d
f7959f2ceb8a1

State'

14c5f8ba:
- 1014 eth

bb75a980:
- 5212 eth

```
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
```

[0, 235235, CHARLIE, ALICE ..

892bf92f:
- 0 eth

```
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
```

[ALICE, BOB, CHARLIE]

4096ad65:
- 77 eth

ethereum Blockchain

Gas

- Used for transaction fees
- Sender buys gas at a specified **gasprice**
- Every computational step has a certain gas cost
- Remaining gas sent back to sender (as ether)
- If gas runs out
  - the state reverts
  - miners keep the ether

ethereum Blockchain

Gasprice

Associated gas cost to some action is constant

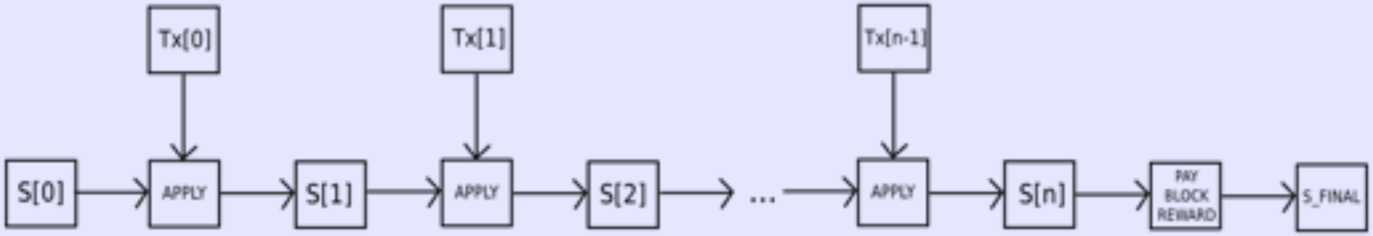
Gasprice is a scale factor against ether price

Should go down as ether goes up and vice-versa

ethereum Blockchain

Blockchain gives transactions an order

Transactions are grouped together into blocks



Order is important

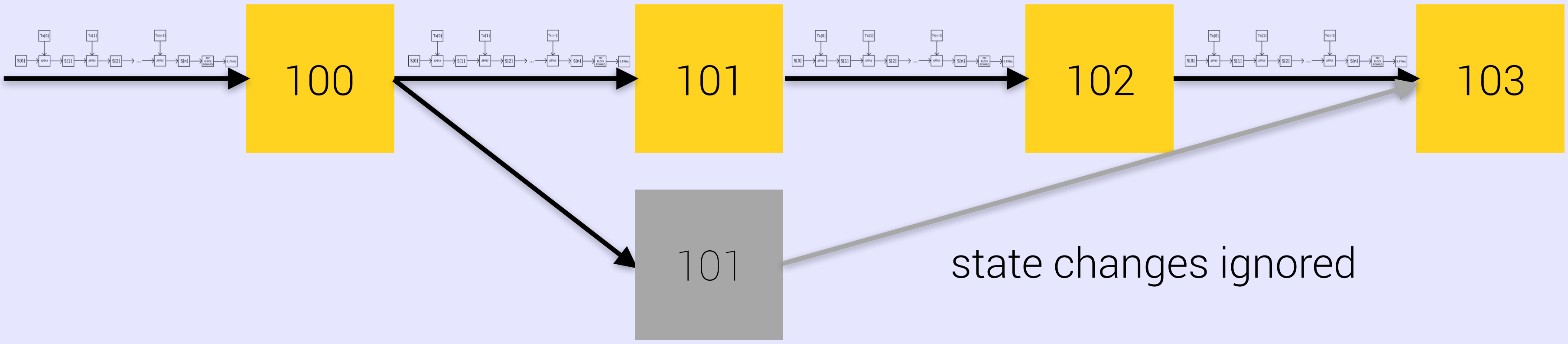
- Double spend (no unspent outputs, but balance might become 0)
- 2 transactions interacting with same contract
- Different order might mean different outcome
- Order from 1 account is guaranteed

ethereum Blockchain

Blocks form a chain

~15s apart (reorganisation very common)

Some can have uncle blocks



state changes ignored

Longest chain is considered to be the consensus

Ethereum 1.0: Length = Accumulated difficulty

ethereum Blockchain

Proof of Work (Ethereum 1.0)

EthHash

asic-resistant (high memory, io bandwidth)

targets gpu mining (2GB+ GRAM)

To be succeeded by PoW / PoS Hybrid

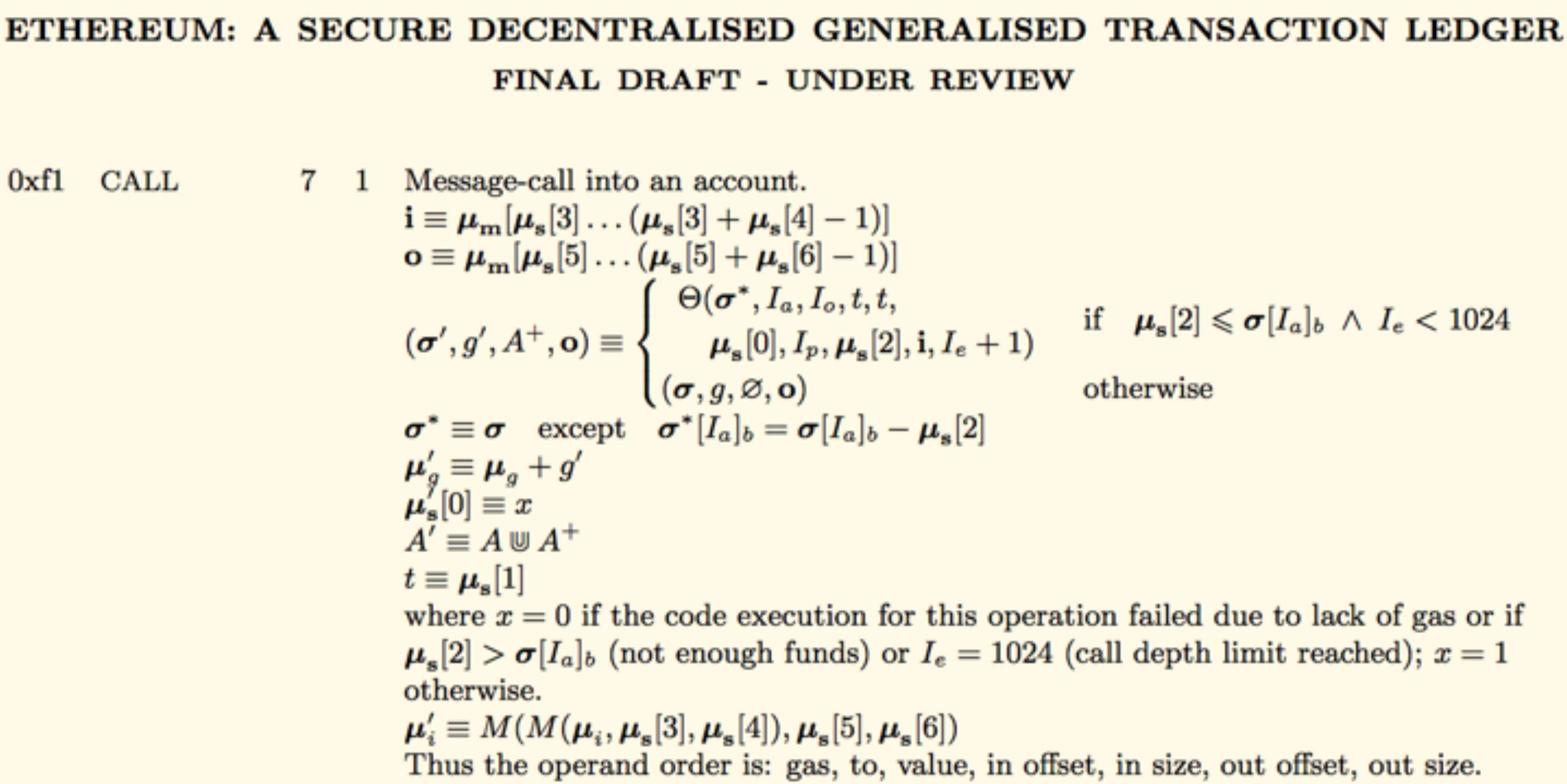
Additional exponential increase in difficulty over time

Constant Block Reward (dis-inflationary)

At least during PoW Phase

ethereum Specification

Yellow Paper (github: ethereum/latexpaper)



ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

FINAL DRAFT - UNDER REVIEW

0xf1 CALL 7 1 Message-call into an account.

$$\mathbf{i} \equiv \boldsymbol{\mu}_\mathbf{m}[\boldsymbol{\mu}_\mathbf{s}[3] \dots (\boldsymbol{\mu}_\mathbf{s}[3] + \boldsymbol{\mu}_\mathbf{s}[4] - 1)]$$

$$\mathbf{o} \equiv \boldsymbol{\mu}_\mathbf{m}[\boldsymbol{\mu}_\mathbf{s}[5] \dots (\boldsymbol{\mu}_\mathbf{s}[5] + \boldsymbol{\mu}_\mathbf{s}[6] - 1)]$$

$$(\boldsymbol{\sigma}', g', A^+, \mathbf{o}) \equiv \begin{cases} \Theta(\boldsymbol{\sigma}^*, I_a, I_o, t, t, \\ \quad \boldsymbol{\mu}_\mathbf{s}[0], I_p, \boldsymbol{\mu}_\mathbf{s}[2], \mathbf{i}, I_e + 1) & \text{if} \quad \boldsymbol{\mu}_\mathbf{s}[2] \leqslant \boldsymbol{\sigma}[I_a]_b \ \wedge \ I_e < 1024 \\ (\boldsymbol{\sigma}, g, \varnothing, \mathbf{o}) & \text{otherwise} \end{cases}$$

$$\boldsymbol{\sigma}^* \equiv \boldsymbol{\sigma} \quad \text{except} \quad \boldsymbol{\sigma}^*[I_a]_b = \boldsymbol{\sigma}[I_a]_b - \boldsymbol{\mu}_\mathbf{s}[2]$$

$$\boldsymbol{\mu}'_g \equiv \boldsymbol{\mu}_g + g'$$

$$\boldsymbol{\mu}'_\mathbf{s}[0] \equiv x$$

$$A' \equiv A \Cup A^+$$

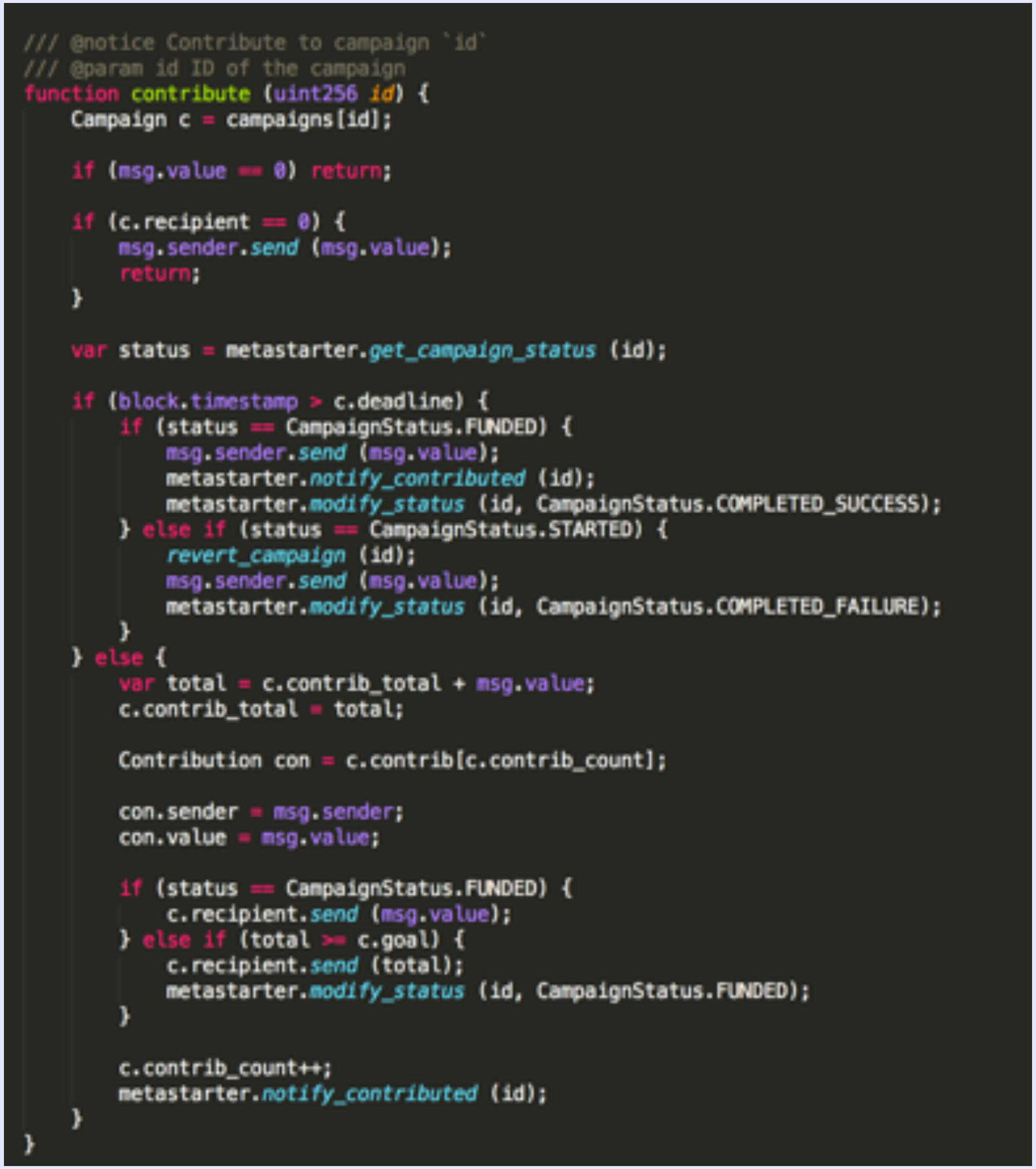
$$t \equiv \boldsymbol{\mu}_\mathbf{s}[1]$$

where $x = 0$ if the code execution for this operation failed due to lack of gas or if $\boldsymbol{\mu}_\mathbf{s}[2] > \boldsymbol{\sigma}[I_a]_b$ (not enough funds) or $I_e = 1024$ (call depth limit reached); $x = 1$ otherwise.

$$\boldsymbol{\mu}'_i \equiv M(M(\boldsymbol{\mu}_i, \boldsymbol{\mu}_\mathbf{s}[3], \boldsymbol{\mu}_\mathbf{s}[4]), \boldsymbol{\mu}_\mathbf{s}[5], \boldsymbol{\mu}_\mathbf{s}[6])$$

Thus the operand order is: gas, to, value, in offset, in size, out offset, out size.

etherSTARTER



```
/// @notice Contribute to campaign `id`
/// @param id ID of the campaign
function contribute (uint256 id) {
    Campaign c = campaigns[id];

    if (msg.value == 0) return;

    if (c.recipient == 0) {
        msg.sender.send (msg.value);
        return;
    }

    var status = metastarter.get_campaign_status (id);

    if (block.timestamp > c.deadline) {
        if (status == CampaignStatus.FUNDED) {
            msg.sender.send (msg.value);
            metastarter.notify_contributed (id);
            metastarter.modify_status (id, CampaignStatus.COMPLETED_SUCCESS);
        } else if (status == CampaignStatus.STARTED) {
            revert_campaign (id);
            msg.sender.send (msg.value);
            metastarter.modify_status (id, CampaignStatus.COMPLETED_FAILURE);
        }
    } else {
        var total = c.contrib_total + msg.value;
        c.contrib_total = total;

        Contribution con = c.contrib[c.contrib_count];

        con.sender = msg.sender;
        con.value = msg.value;

        if (status == CampaignStatus.FUNDED) {
            c.recipient.send (msg.value);
        } else if (total >= c.goal) {
            c.recipient.send (total);
            metastarter.modify_status (id, CampaignStatus.FUNDED);
        }

        c.contrib_count++;
        metastarter.notify_contributed (id);
    }
}
```

ethereum

Whisper

Decentralised Messaging

Messages filtered by topics

Very flexible

- Messages can be encrypted
- Messages can be signed
- Public broadcast

Proof of Work for spam protection and priority

TTL

Not designed for real-time communication

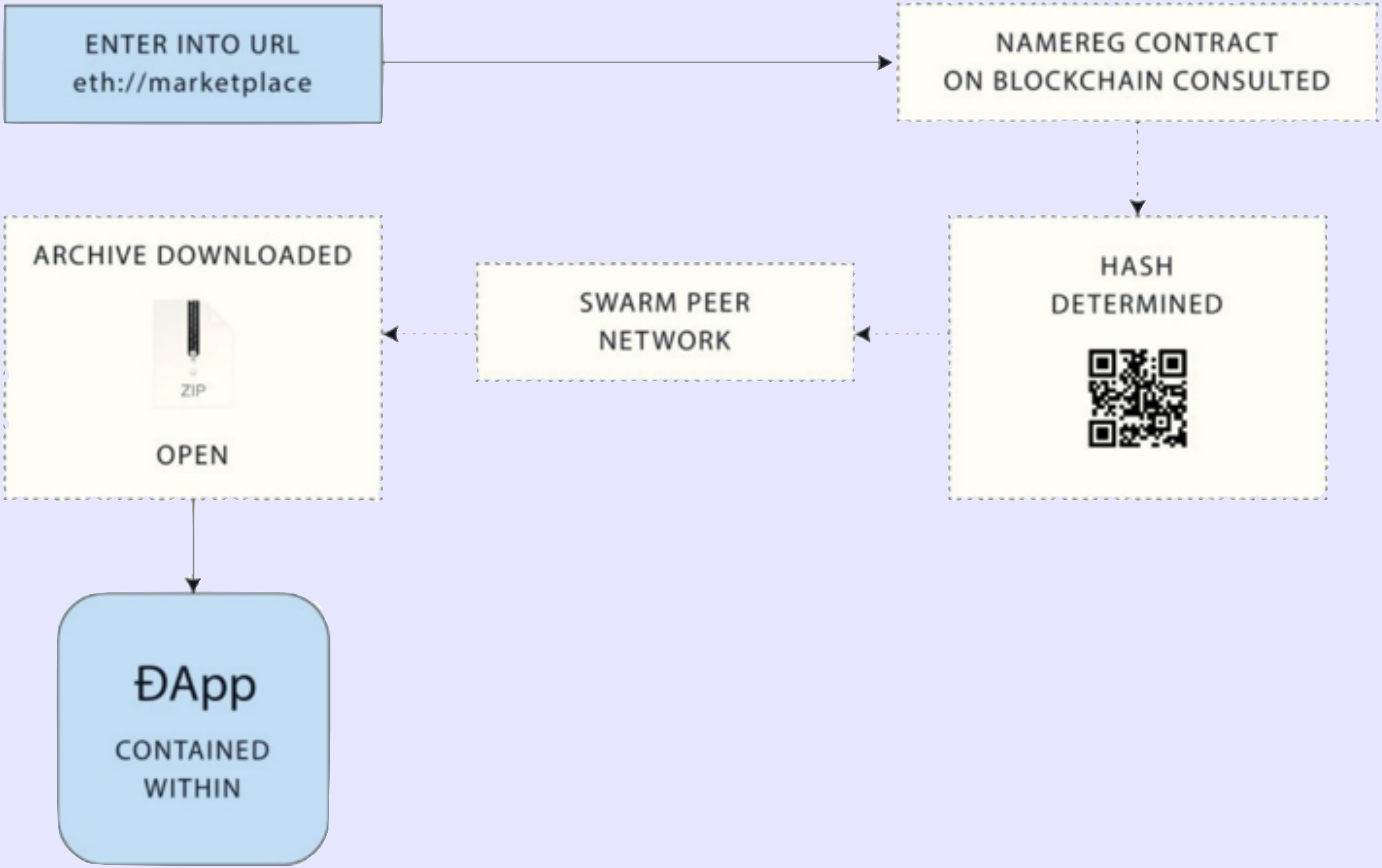
ethereum Swarm

Still not available. Needs those properties:

- Reverse Hash-Table
- Like bittorrent with magnet links (or ipfs)
- Originator of source unknown
- Low-Latency
- Incentivisation Model

But: “bzz” branch made it into the main repository

ethereum Marketplace



ENTER INTO URL eth://marketplace

NAMEREG CONTRACT ON BLOCKCHAIN CONSULTED

HASH DETERMINED

SWARM PEER NETWORK

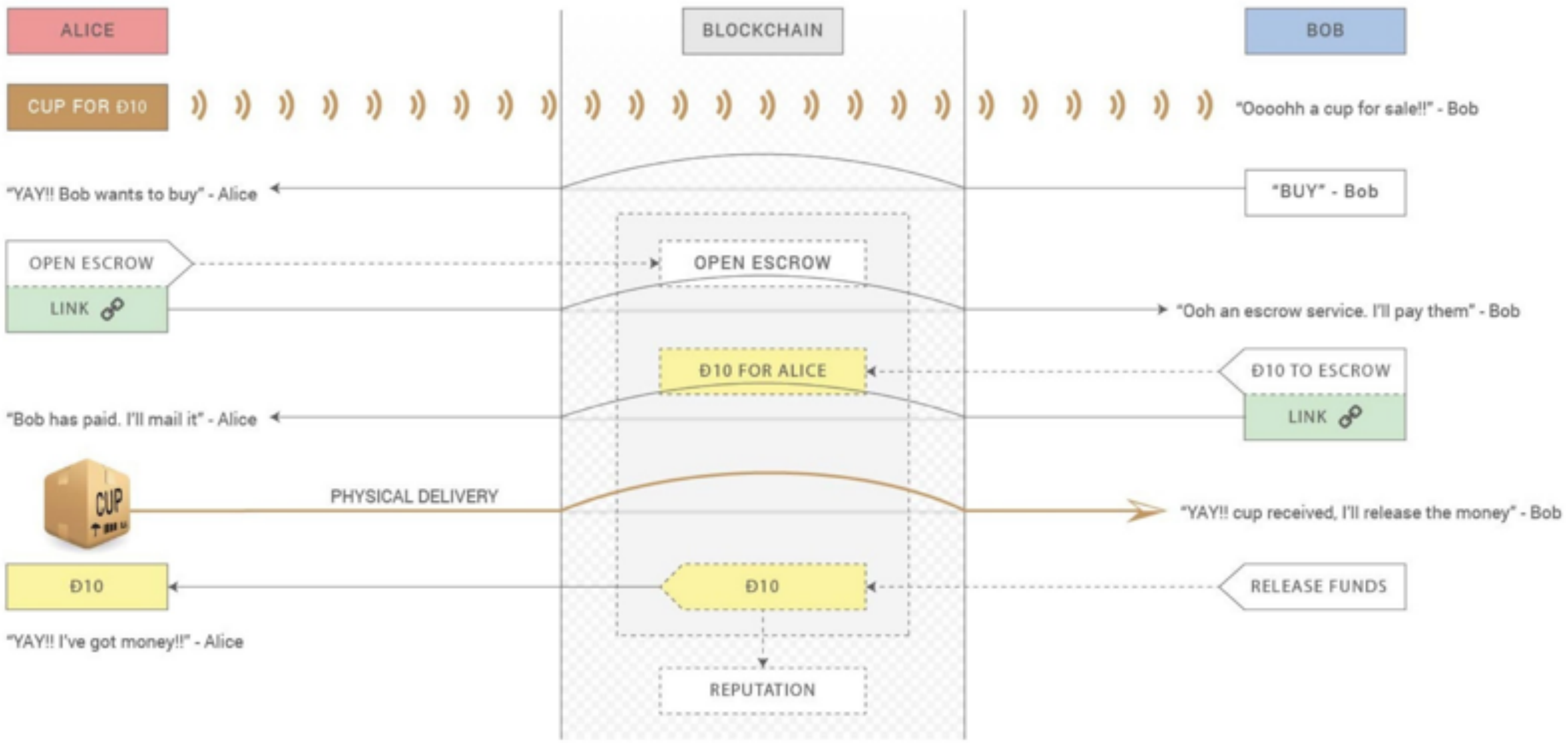
ARCHIVE DOWNLOADED

OPEN

ĐApp

CONTAINED WITHIN

ethereum Marketplace



ALICE

BLOCKCHAIN

BOB

CUP FOR Ð10

"Oooohh a cup for sale!!" - Bob

"YAY!! Bob wants to buy" - Alice

"BUY" - Bob

OPEN ESCROW

LINK

OPEN ESCROW

"Ooh an escrow service. I'll pay them" - Bob

Ð10 FOR ALICE

Ð10 TO ESCROW

LINK

"Bob has paid. I'll mail it" - Alice

CUP

PHYSICAL DELIVERY

"YAY!! cup received, I'll release the money" - Bob

Ð10

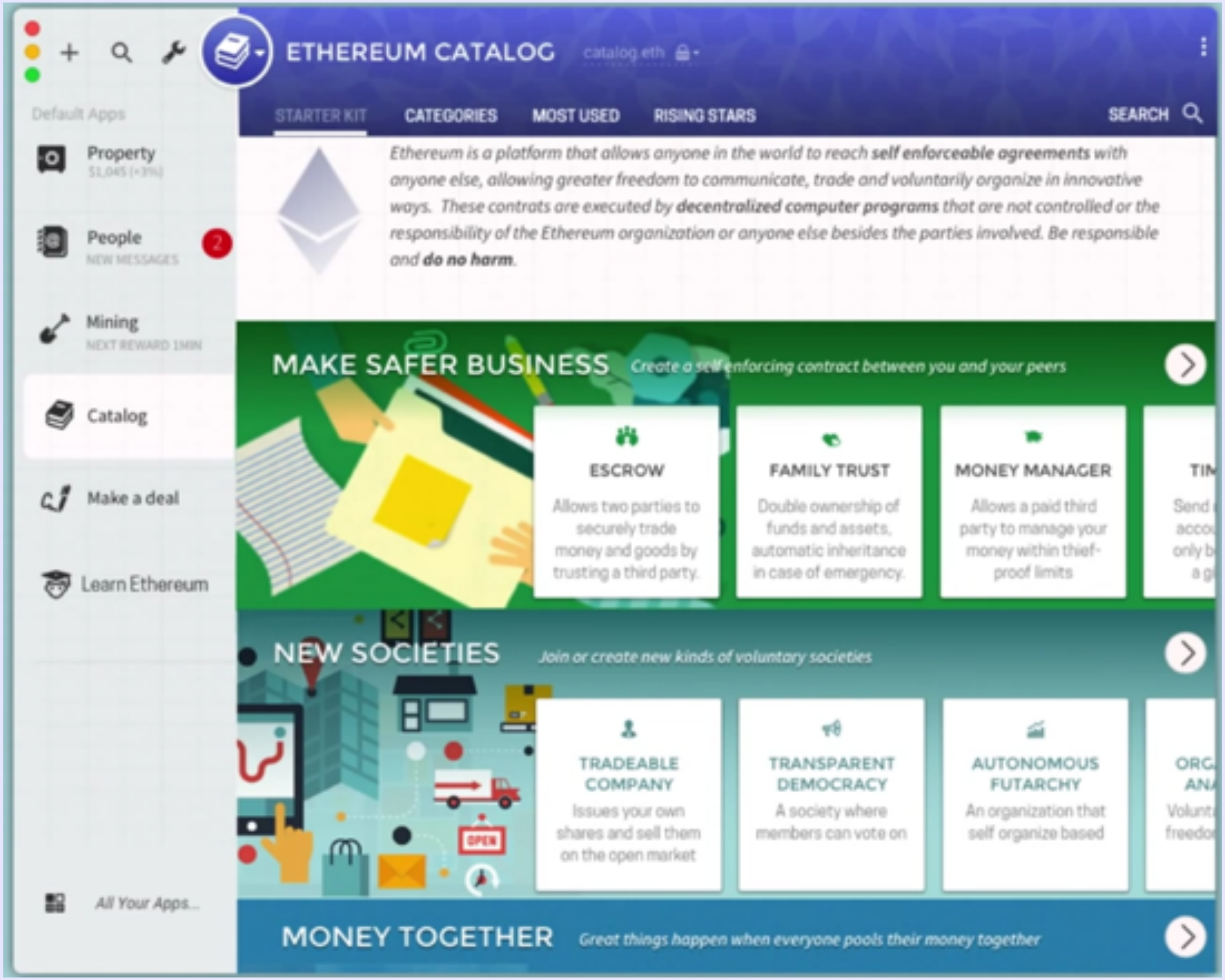
Ð10

RELEASE FUNDS

"YAY!! I've got money!!" - Alice

REPUTATION

ethereum Mist



Ethereum is a platform that allows anyone in the world to reach **self enforceable agreements** with anyone else, allowing greater freedom to communicate, trade and voluntarily organize in innovative ways. These contrats are executed by **decentralized computer programs** that are not controlled or the responsibility of the Ethereum organization or anyone else besides the parties involved. Be responsible and **do no harm**.

MAKE SAFER BUSINESS *Create a self enforcing contract between you and your peers*

ESCROW: Allows two parties to securely trade money and goods by trusting a third party.

FAMILY TRUST: Double ownership of funds and assets, automatic inheritance in case of emergency.

MONEY MANAGER: Allows a paid third party to manage your money within thief-proof limits

NEW SOCIETIES *Join or create new kinds of voluntary societies*

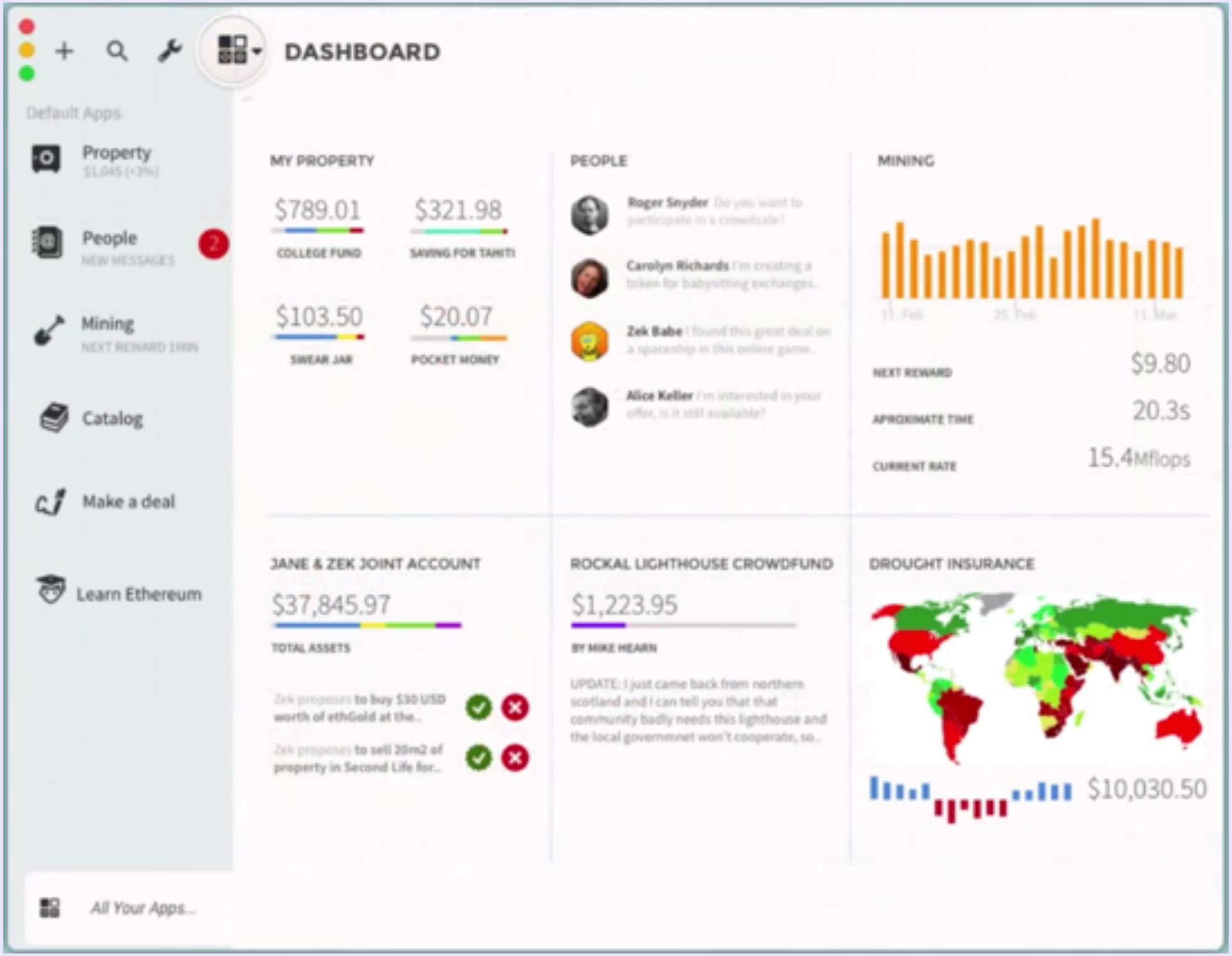
TRADEABLE COMPANY: Issues your own shares and sell them on the open market

TRANSPARENT DEMOCRACY: A society where members can vote on

AUTONOMOUS FUTARCHY: An organization that self organize based

MONEY TOGETHER *Great things happen when everyone pools their money together*

ethereum Mist



MY PROPERTY

$789.01 COLLEGE FUND	$321.98 SAVING FOR TAHITI
$103.50 SWEAR JAR	$20.07 POCKET MONEY

PEOPLE

Roger Snyder Do you want to participate in a crowdsale?

Carolyn Richards I'm creating a token for babysitting exchanges...

Zek Babe I found this great deal on a spaceship in this online game...

Alice Keller I'm interested in your offer, is it still available?

MINING

NEXT REWARD	$9.80
APROXIMATE TIME	20.3s
CURRENT RATE	15.4Mflops

JANE & ZEK JOINT ACCOUNT

$37,845.97

TOTAL ASSETS

Zek proposes **to buy $30 USD worth of ethGold at the...** ✓ ✗

Zek proposes **to sell 20m2 of property in Second Life for...** ✓ ✗

ROCKAL LIGHTHOUSE CROWDFUND

$1,223.95

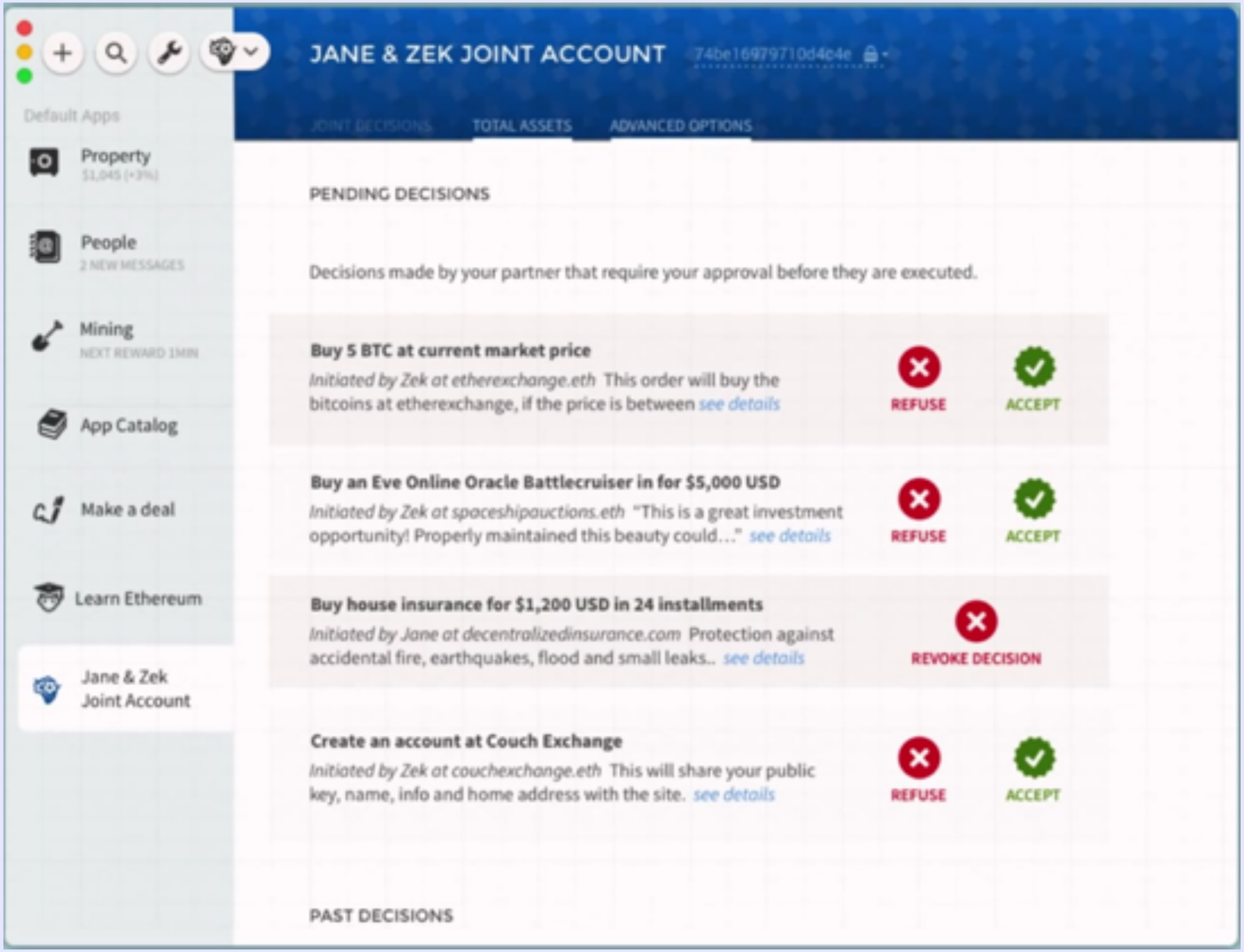
BY MIKE HEARN

UPDATE: I just came back from northern scotland and I can tell you that that community badly needs this lighthouse and the local governmnet won't cooperate, so...

DROUGHT INSURANCE

$10,030.50

ethereum Mist



JANE & ZEK JOINT ACCOUNT

PENDING DECISIONS

Decisions made by your partner that require your approval before they are executed.

Buy 5 BTC at current market price
Initiated by Zek at etherexchange.eth This order will buy the bitcoins at etherexchange, if the price is between *see details*

Buy an Eve Online Oracle Battlecruiser in for $5,000 USD
Initiated by Zek at spaceshipauctions.eth "This is a great investment opportunity! Properly maintained this beauty could..." *see details*

Buy house insurance for $1,200 USD in 24 installments
Initiated by Jane at decentralizedinsurance.com Protection against accidental fire, earthquakes, flood and small leaks.. *see details*

Create an account at Couch Exchange
Initiated by Zek at couchexchange.eth This will share your public key, name, info and home address with the site. *see details*

PAST DECISIONS

ethereum Funding

Funded entirely by crowdfunding

31.529 BTC raised (~18.5m USD at the time)

Over 9000 transactions

2nd (now 3rd) biggest crowdfunding campaign

but half of the value lost due to decline in bitcoin price

ethereum Who?

- Ethereum Stiftung
    - Allocates resources
- ethereum Switzerland GmbH
    - Responsible for genesis-block related tasks
    - Afterwards ÐΞVOLUTION
- ÐΞV
    - Non Profit
    - Building and promoting Ethereum 1.0

ethereum Where?

Companies wherever there are employees

Berlin, Germany (Development Hub)

Amsterdam, Netherlands (Development Hub)

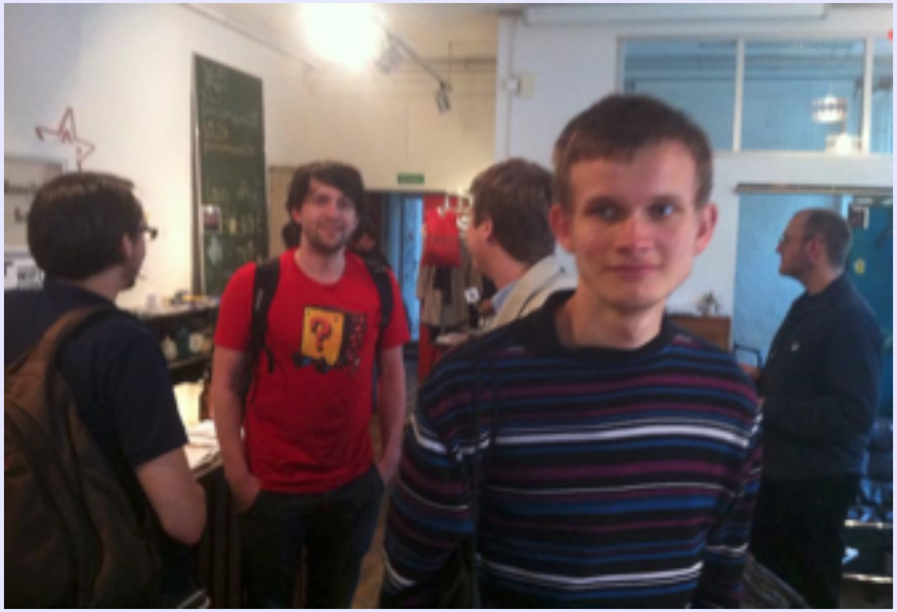
London, UK (Community Hub)

Zug, Switzerland (Legal / Development Hub)

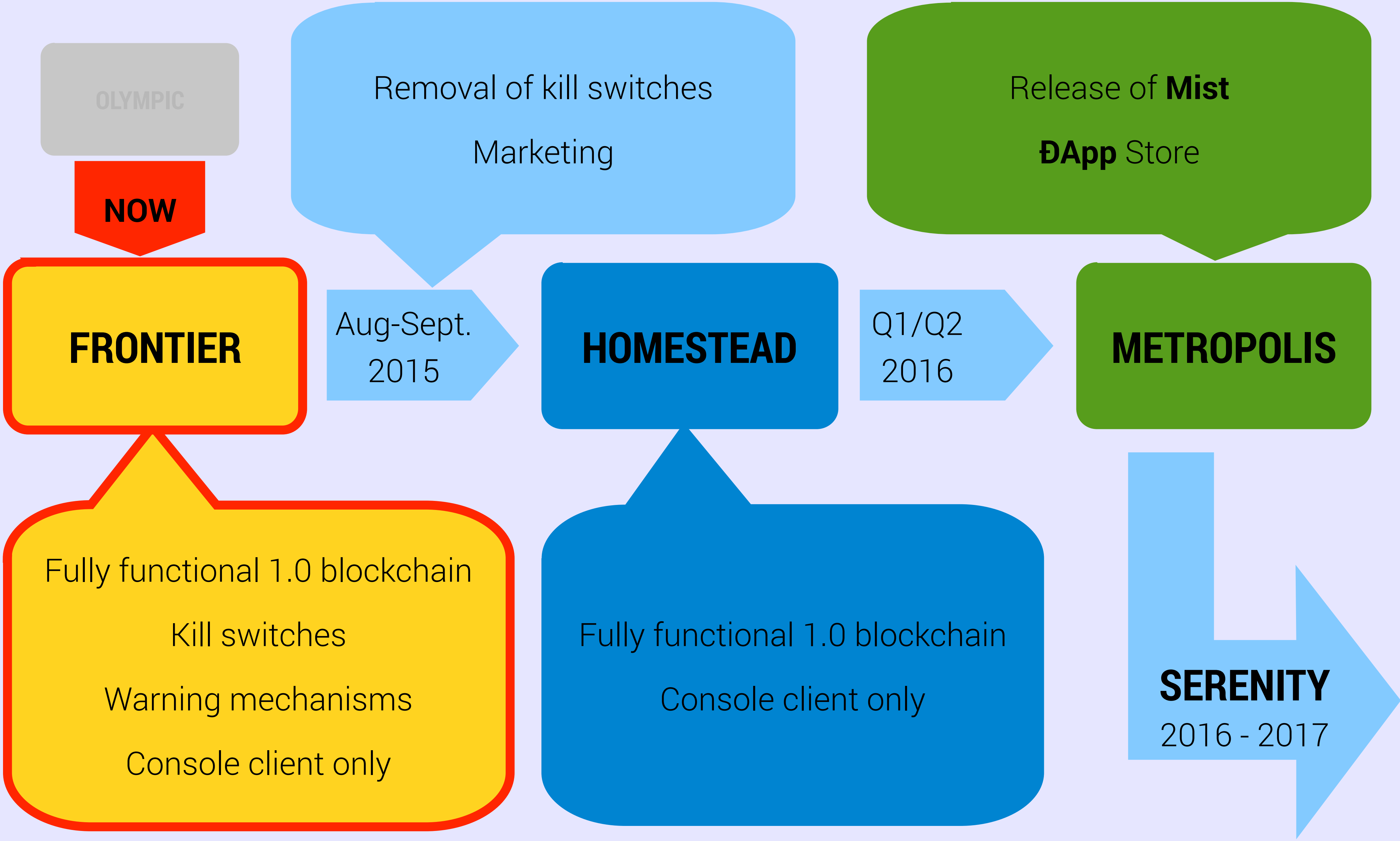
ethereum Who?

Vitalik Buterin

- Invented the concept
- Co-Founder / Writer, Bitcoin Magazine 2011
- Has won several IT related awards



ethereum Release Process



OLYMPIC

NOW

FRONTIER

Fully functional 1.0 blockchain

Kill switches

Warning mechanisms

Console client only

Aug-Sept. 2015

Removal of kill switches

Marketing

HOMESTEAD

Fully functional 1.0 blockchain

Console client only

Q1/Q2 2016

Release of **Mist**

ĐApp Store

METROPOLIS

SERENITY

2016 - 2017