Ethereum Vienna
General Introduction

Ethereum Project

- Decentralization of services
- Removing the role of centralized servers
- Control goes from server owner to users
  - Server can't disappear with your data
  - Server can't just randomly modify your data
  - Server can't just freeze your funds
  - Censorship-proof
  - DDOS-resistant

Web 3.0

- Ðapps (run in a Web 3.0 client)
  - **Ethereum** (Blockchain)
    - Agreements
    - Relationships
  - **Whisper**
    - Messaging
    - Bulletins
  - **Distributed Content System** (“Swarm”)
    - Data publication and distribution

Possible ĐApps

- Escrow (m-of-n transactions)
- Namecoin (decentralized dns)
- Subscription Service
- Crowdfunding
- Subcurrencies
- Decentralized Autonomous Organizations
- Marketplace

Ethereum Blockchain

- Maintains Accounts with balances denominated in ether/wei
  - **Externally owned** (account)
    - Controlled by a private key
    - Owner can send ether to other accounts
    - Similar in usage to normal bitcoin addresses

Ethereum Blockchain

- **Internally owned** (contract)
  - Controlled by code
  - Code is executed for each incoming transaction/message
  - No private key, ether can only be sent by the code
  - Has a 256 bit to 256 bit persistent storage
  - Can call other contracts
  - Code written in an ethereum-specific language:
    - **Solidity**: high-level, main language
    - **Serpent2**: python-like (no longer officially supported)
    - **lll**: low-level

Ethereum Blockchain

- Gas
  - Used for transaction fees
  - Sender “buys” necessary amount of gas at a specified **gasprice** (goes down as price goes up)
  - Every computational step has an associated gas cost
  - Remaining gas is returned to the sender
  - If the sender does not provide enough gas, the state reverts and the miner keeps the ether

Ethereum Blockchain

- Gives messages an order
- Messages are grouped together in blocks
- Blocks are chained together
- Longest chain is considered valid
- 12s Block Time (made possible with uncle blocks)
- Hybrid PoW (ASIC-resistant) / PoS (planned)
  - Genesis Release: dagger-hashimoto
- Constant Block Reward (dis-inflationary)

EtherStarter v0.1

- Keeps track of crowdfunding campaigns
- Automatic payout if goal is reached
- Automatic payback if campaign fails
- Functions
  - **create_campaign** *<id> <recipient> <goal> <timelimit> <shh_identity>*
  - **contribute** *<id>*
  - ***get_free_id*** *only for local usage*
  - Various getters

EtherStarter v0.1

```
contract crowdfund {

    struct contribution {
        address sender;
        uint256 value;
    }

    struct campaign {
        address recipient;
        uint256 goal;
        uint256 deadline;
        uint256 contrib_total;
        uint256 contrib_count;
        shh_identity identity;
        mapping (uint256 => contribution) contrib;
    }

    mapping (uint256 => campaign) campaigns;

    function create_campaign (uint256 id, address recipient, uint256 goal, uint256 deadline,
    uint256 identity_lsb, uint256 identity_msb) {
        campaign c = campaigns[id];

        if (c.recipient != 0) return;

        c.recipient = recipient;
        c.goal = goal;
        c.deadline = deadline;
        c.identity.lsb = identity_lsb;
        c.identity.msb = identity_msb;
    }
```

Who?

- Ethereum Stiftung
  - Allocates resources
- ethereum Switzerland GmbH
  - Responsible for genesis-block-related tasks
- ĐΞV
  - Nonprofit
  - Building and promoting Ethereum 1.0

Ether Sale

- Development funded via crowdfunding
- 31,529 BTC (~12.5m USD)
- Over 9000 transactions
- 2nd biggest crowdfunder

Who?

- Vitalik Buterin
  - Invented the concept of ethereum
  - Co-Founder / Writer of Bitcoin Magazine in 2011
  - 2014 World Technology Award (IT Software)
  - Thiel Award

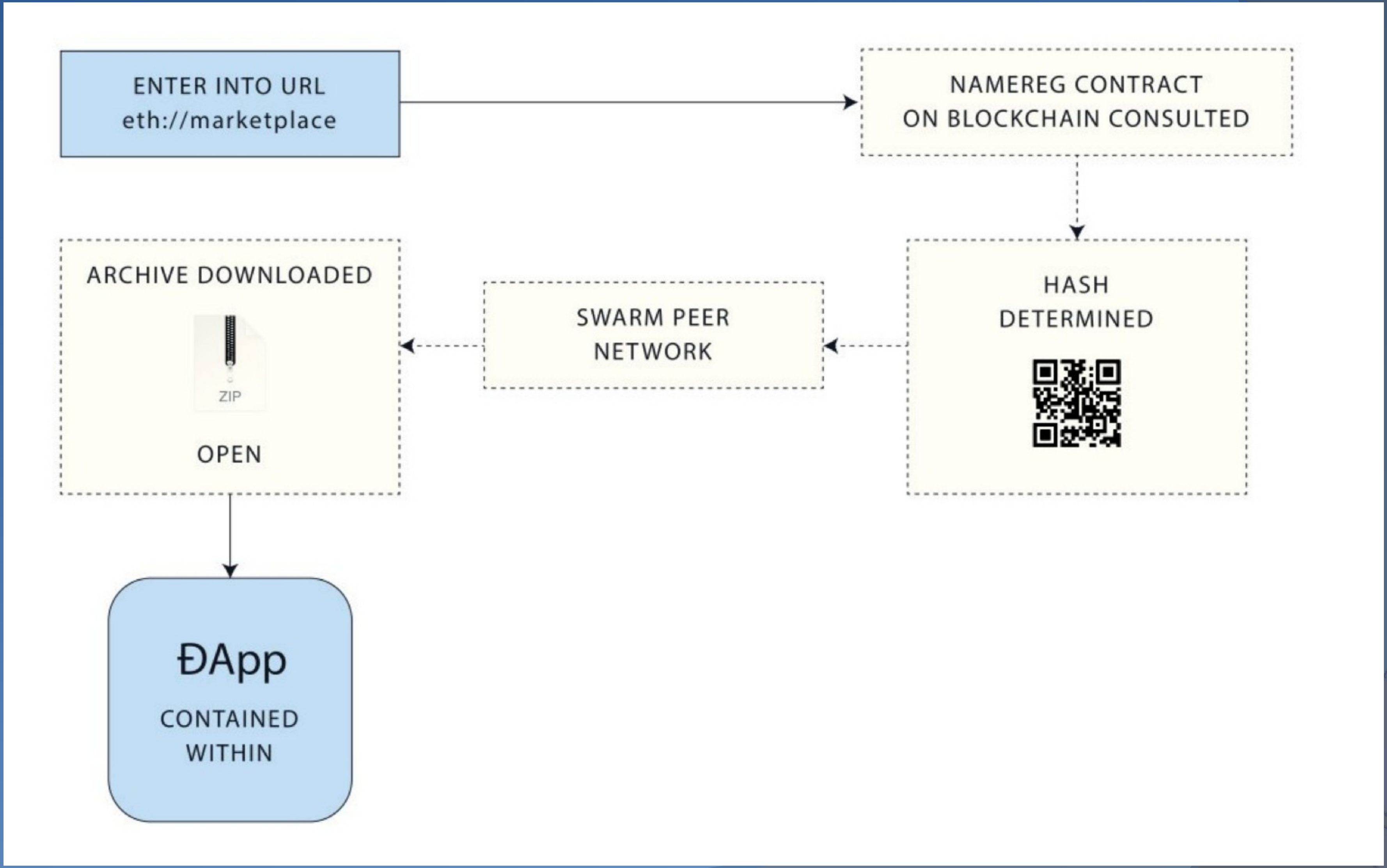
Whisper

- Decentralized Messaging
- Messages are assigned topics
- Private messages encrypted
- Public broadcasts
- Dark (no reliable tracing mechanism)
- Not designed for RTC

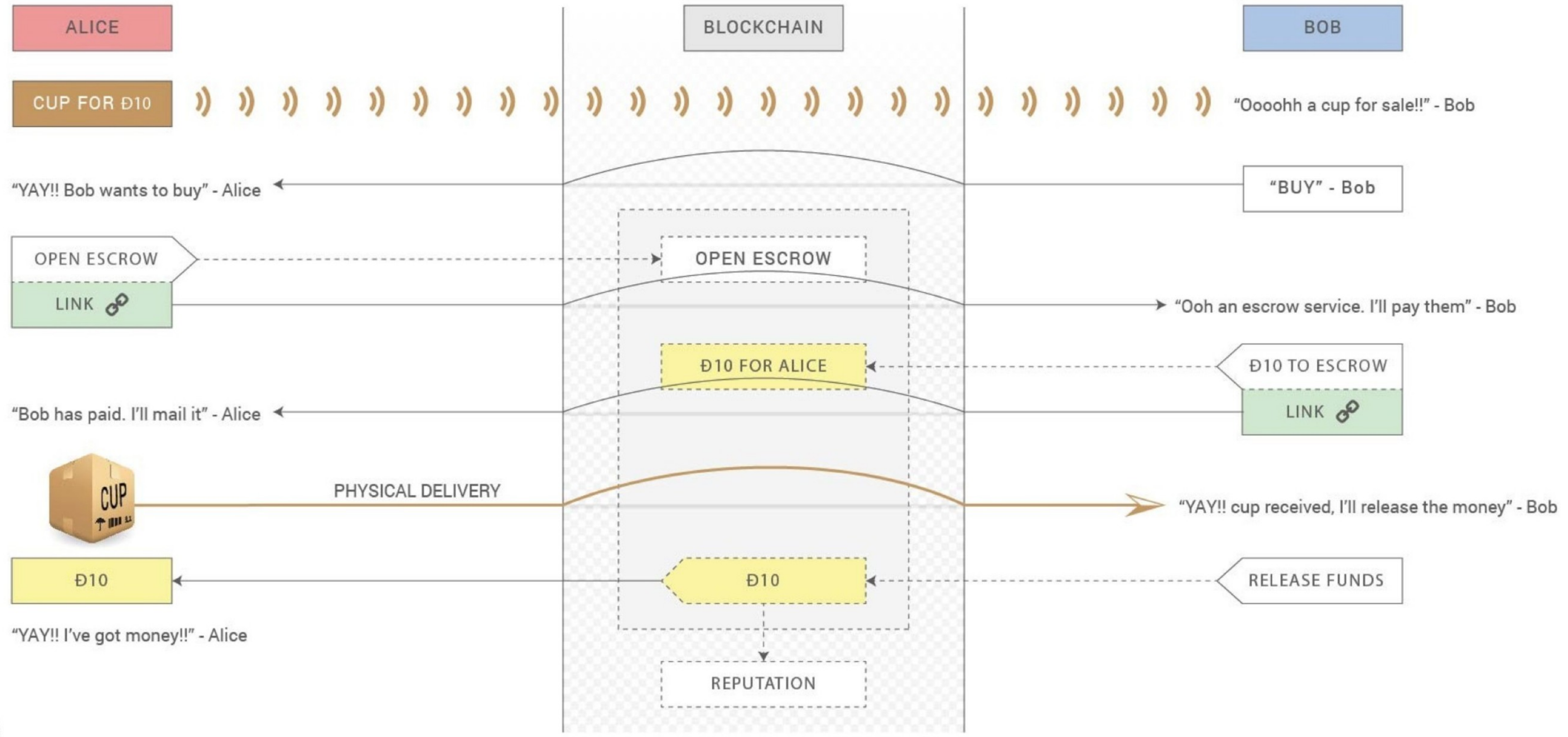
Distributed Content System

- Not yet chosen. Needs those properties:
  - Reverse Hash Table
  - Like bittorrent with magnet links
  - Private
  - Low-latency
  - Incentivised (content can get lost if no one pays maintenance)

Marketplace



Marketplace



ALICE

BLOCKCHAIN

BOB

CUP FOR Đ10

“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

Đ10 FOR ALICE

Đ10 TO ESCROW

LINK

“Bob has paid. I’ll mail it” - Alice

PHYSICAL DELIVERY

“YAY!! cup received, I’ll release the money” - Bob

Đ10

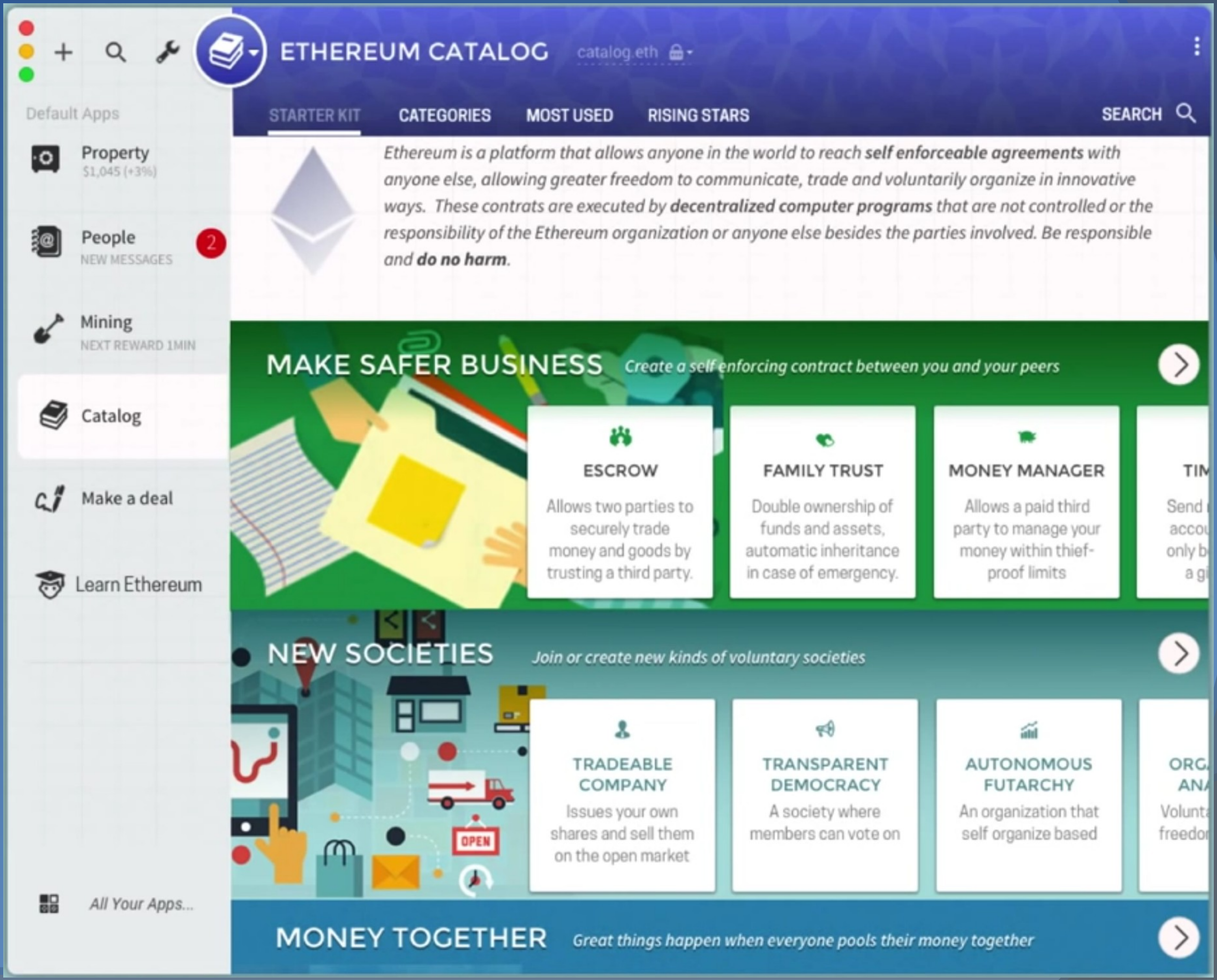
Đ10

RELEASE FUNDS

“YAY!! I’ve got money!!” - Alice

REPUTATION

Mist (Web 3.0 Client)



*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

TIM

Send
accou
only b
a gi

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

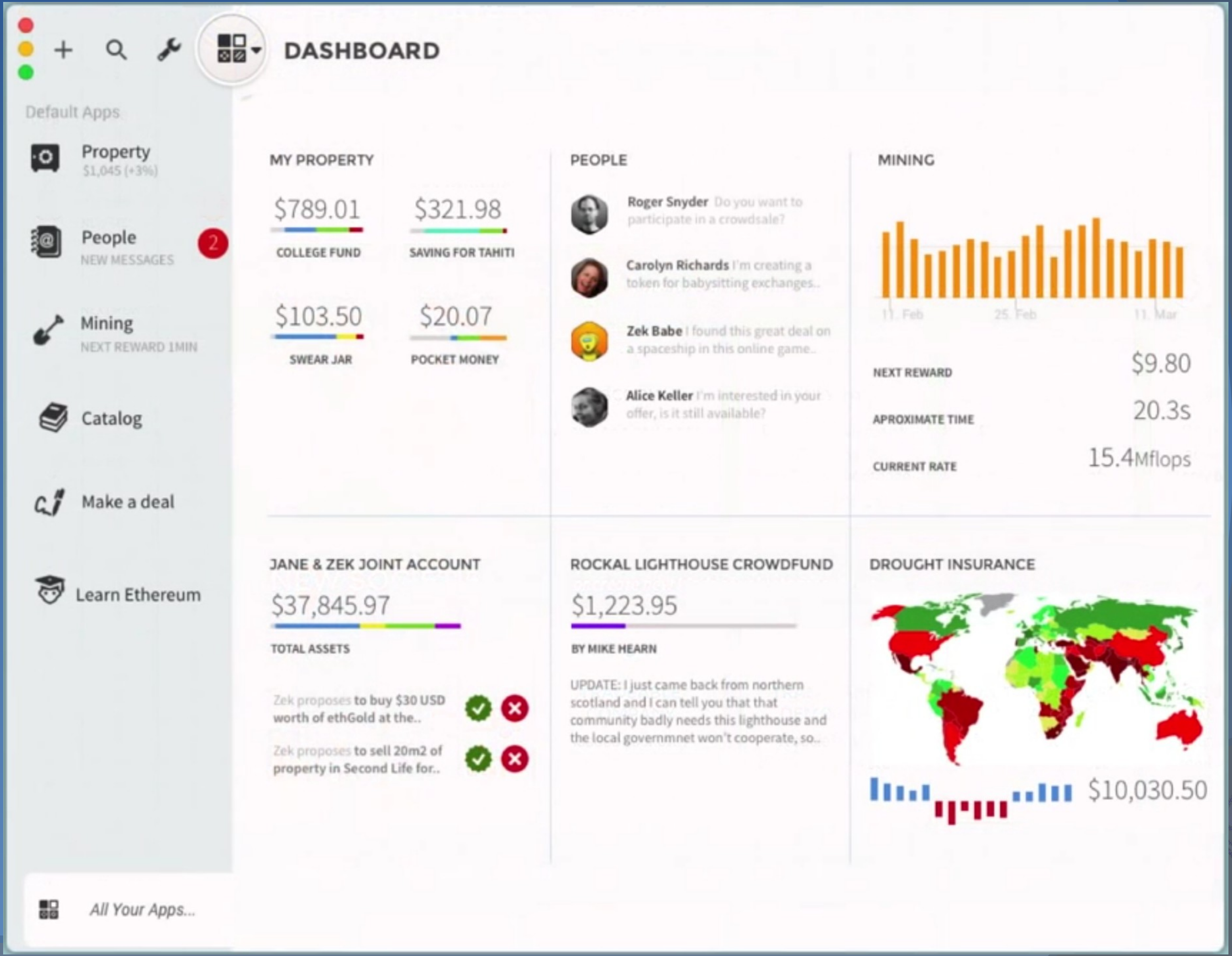
An organization that self organize based

ORG
ANA

Volunta
freedo

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

Mist (Web 3.0 Client)



DASHBOARD

Default Apps

Property
$1,045 (+3%)

People
NEW MESSAGES
2

Mining
NEXT REWARD 1MIN

Catalog

Make a deal

Learn Ethereum

All Your Apps...

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

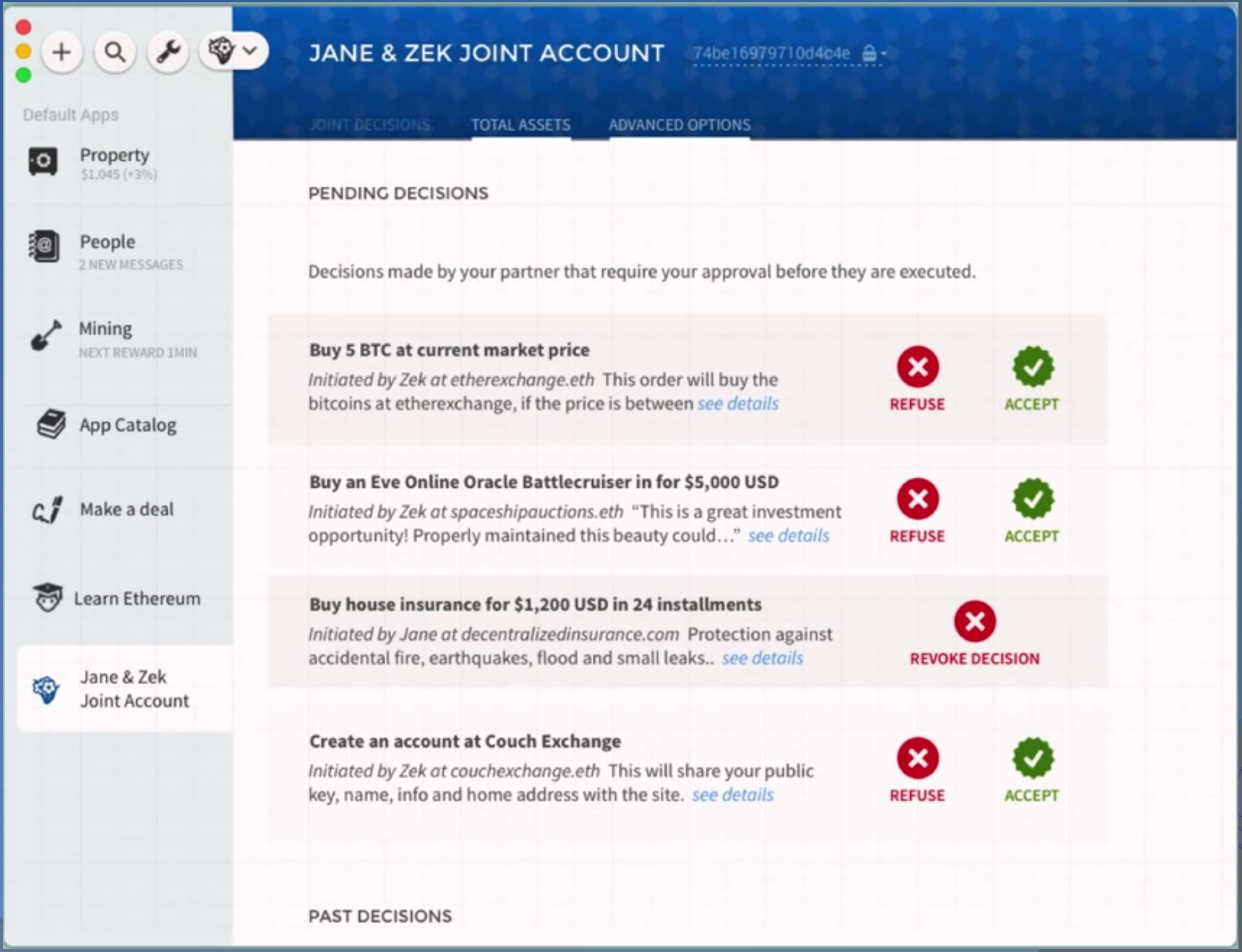
$1,223.95
BY MIKE HEARN

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

Mist (Web 3.0 Client)



JANE & ZEK JOINT ACCOUNT 74be16979710d4c4e

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*

REFUSE ACCEPT

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*

REFUSE ACCEPT

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*

REVOKE DECISION

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*

REFUSE ACCEPT

PAST DECISIONS