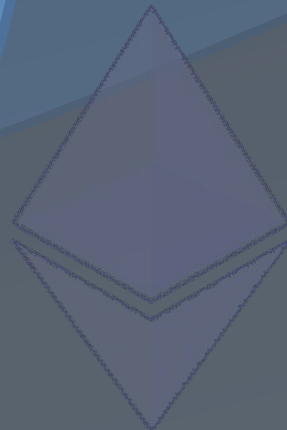
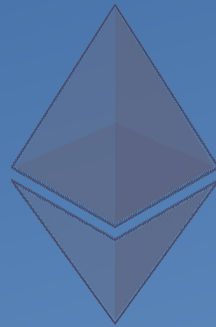


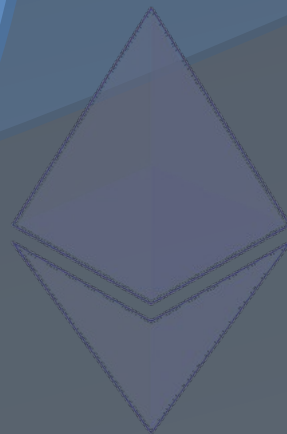
Ethereum Vienna

General Introduction



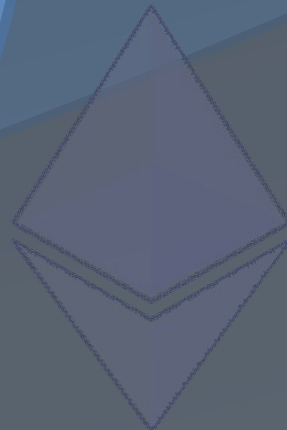
Ethereum Project

- Decentralization of services
- Trustless Contract Execution - “crypto-law”
- Lowering barriers for innovation
- Pseudonymity, but with reputation



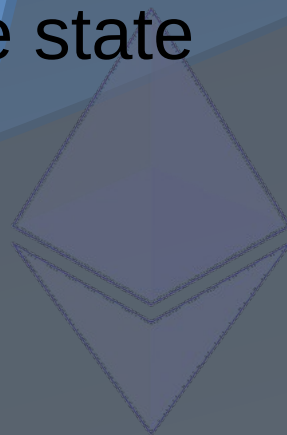
Ethereum Blockchain

- Maintains Accounts with balances denominated in ether/wei
 - Externally owned
 - Controlled by a private key
 - Owner can send ether to other accounts
 - Internally owned
 - 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 byte to 256 byte persistent storage



Ethereum Blockchain

- Gas
 - Used for transaction fees
 - Sender “buys” necessary amount of gas for a specified gasprice
 - 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
- Hybrid PoW / PoS to determine score of blockchain

<PLACEHODLER/>

- Keeps track of account balances
- Received ether added to balance of sender
- 3 commands
 - **send** <vol/> <recv>: transfer <vol/> wei from sender balance to balance of <recv>
 - **withdraw** <vol/> <recv>: subtract <vol/> from sender balance and send <vol/> wei from contract to <recv>
 - **deposit** (no command): don't attempt to send or withdraw

<PLACEHODLER/>

EtherScripter – Visual smart-contract builder for Ethereum – Mozilla Firefox

PoC 5 JS ... EtherScri... Paper.pdf

etherscripter.com/0-4-0/ Google F170%

EtherScripter View Toolbox Workspace Samples About

init body

in save slot contract caller

put data at save slot contract caller + tx amount

when tx input slot count == 3

then

@ cmd = data at input slot 0

@ vol = data at input slot 1

@ dest = data at input slot 2

if @ vol ≤ data at save slot contract caller

then

if @ cmd == "withdraw"

then spend @ vol to @ dest

else

if @ cmd == "send"

then

in save slot @ dest

put data at save slot @ dest + @ vol

else stop

in save slot contract caller

put data at save slot contract caller - @ vol

else stop

text

0 ether

tx amount

contract caller

block number

+

=

and

in save slot

put

data at save slot

@ =

@

store @@ =

@@

spend to

Show LLL

<PLACEHODLER/>

```
1 code:
2     contract.storage[msg.sender] += msg.value
3     if msg.datasize == 3:
4         cmd = msg.data[0]
5         vol = msg.data[1]
6         dest= msg.data[2]
7         if vol <= contract.storage[msg.sender]:
8             if cmd == "withdraw":
9                 send (tx.gas-100, dest, vol)
10            else:
11                if cmd == "send":
12                    contract.storage[dest] += vol
13                else:
14                    stop
15            contract.storage[msg.sender] -= vol
16        else:
17            stop|
```


<PLACEHODLER/>

FileNetworkToolsDebugHelp

Enable NetworkConnect to PeerPreviewMineMining Paranoia

To

(Create Contract)

Create Contract

Amount

0

ether

Gas

10000 gas

@ 10

szabo

Data

(gas sub-total: 100 finney)

Serpent or LLL
Code goes here

Code

Total: 100 finney

Debug

Execute

0c0854ba...: 0 wei [0]

4d767cb7...: 0 wei [0]

872daf76...: 0 wei [0]

44843d19...: 0 wei [0]

dca8f2d7...: 1500 finney [0]

file:///home/ethbuild/ethereum-vienna/Meetup 4/ui.html

0c0854baac4c83e5a5a9c50b102a7078842c1b79 0 0x
4d767cb7d2eb46e6c030caa044a1f1ffc3a5b7f 0 0x
872daf760df9695c92214ef2d61fe64cbadf481c 0 0x
44843d1913d8ced9ef0cbfb720a1f2a40d205e1e 0 0x
dca8f2d7faa2ce12769c2c6a8056649e0198450f 0 0x

Deposit

0

wei

Address

0c0854baac4c83e5a5a9c50b102a7078842c1b79

Volume

0

wei

Destination Address

Deposit

Send

Withdraw

Accounts

1a26338f...: 1606938 Uether [0]

2ef47100...: 1606938 Uether [0]

51ba5931...: 1606938 Uether [0]

6c386a4b...: 1606938 Uether [0]

b9c01591...: 1606938 Uether [0]

cd2a3d9f...: 1606938 Uether [0]

Network

Ideal Peers

5

Listen on

30303

Client Name

Anony...

Pending

Contracts

Block Chain

Filter...

#1 5e1e7fe5..

7c9bba74cb4b
dbe3055b47be
114470b9f30
cb14b5

Log

*** [09:49:11 PM | main] Opened blockchain DB. Latest: 5e1e7fe5bc0c2336b7a6f28c63ea249afc077c67fe2ea10bdbf065dcd8e7c6c5

*** [09:49:11 PM | main] Opened state DB.

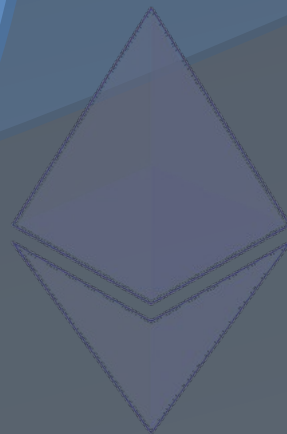
0 GAV | 1500 finney | 0 peer(s) | Not mining #1 @21 T22

Other Examples

- Escrow
- Namecoin
- Subscription Service
- Crowdfunding
- Prediction Markets
- Subcurrencies
- Decentralized Autonomous Organizations

Who?

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



Who?

- Vitalik Buterin
 - Invented the concept of ethereum
 - Co-Founder / Writer of Bitcoin Magazine in 2011
 - Thiel Award

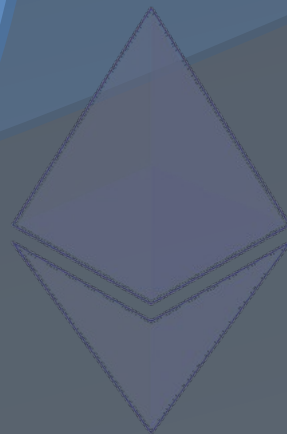


Whisper

- Decentralized Messaging
- Same keypairs like ethereum
- Private messages encrypted
- Public broadcasts
- Dark (no reliable tracing mechanism)
- Not designed for RTC

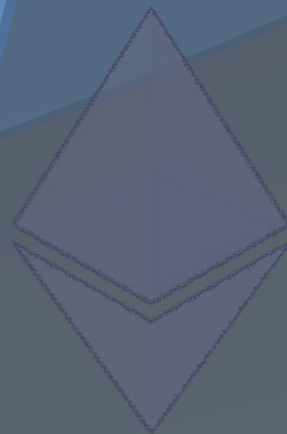
Distributed Content System

- Reverse Hash Table
- Like bittorrent with magnet links
- Lossy
- Private
- Low-latency
- Incentivised
- Swarm or existing solution?

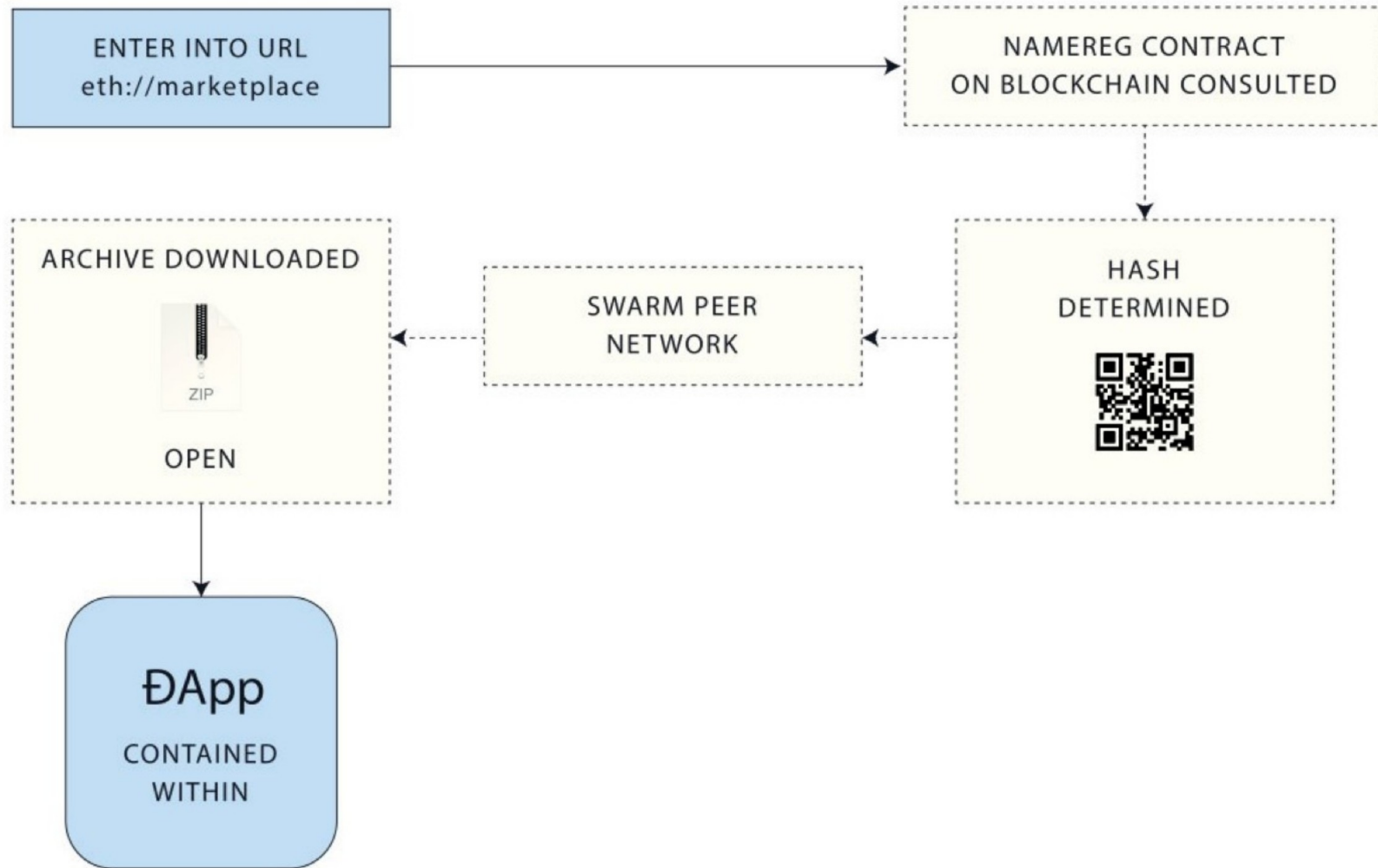


Web 3.0

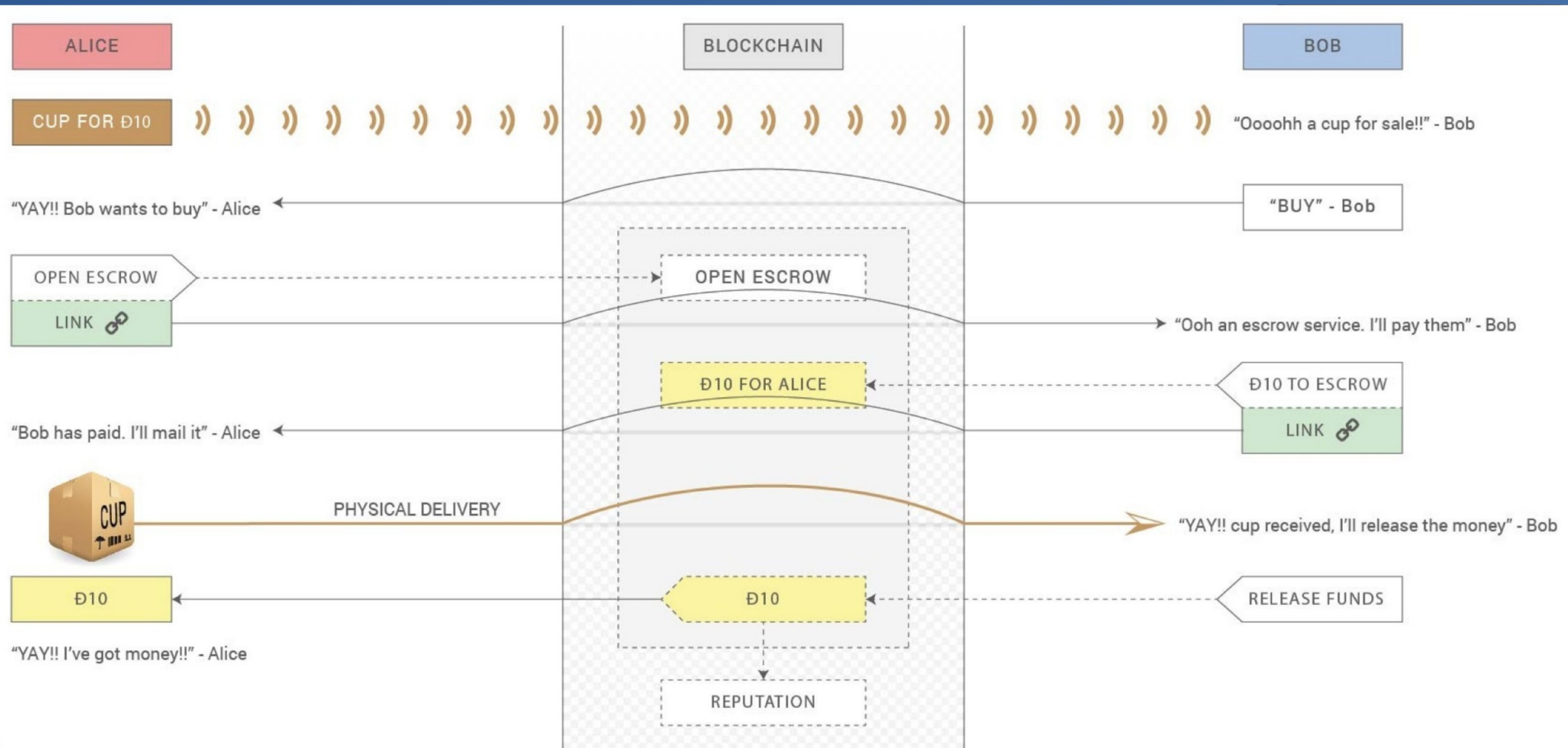
- DApps
 - Ethereum
 - Agreements
 - Relationships
 - Whisper
 - Messaging
 - Bulletins
 - “Swarm”
 - Data publication and distribution



Marketplace



Marketplace




Etherbrowser

×


−

+


ETHEREUM


 Identity

John_doe

 Wallet


2103eth


 Contacts

 Network


4.3TF

APPS


 App Catalog

 Congress


in session

 Dice


3:1

 Freebird


2 unread

 BitBeer


\$5.4 ↑

 Shapeshifter


12gen

 Fire Protection


!

 Chess

RD9

 Weather

\$1021.03 ↓


 Mixr

23h 34min

...

All apps


Type a contract name or hash


 Rumor Mill


Dropbox buys sunrise43.2%↓

Gruber resigns21.5%↑

Runkeeper IPO13.4%↓

 Stability Index MKT




 Air Miles


Your miles98MILES


Buy Price2,130.01USD↑

Sell Price2,130.45USD↑

 Bacon Futures

Bacon Price




 Currency Market

USD-ETH2.4ETHER↓


BRL-ETH1.1ETHER↑

EUR-ETH4.1ETHER↓

 Distributed Research

Total Research13.4TFLOPS


Donated CPU2.1KFLOPS

 Private Chat

Sarah Sushi tonight? There's this..

Work Group Since everyone was so..


Mr. Anderson I need you for a job..

 Snowball Effect

You donated1200ETHER

You got back122ETHER

Total Donations3.4METHER

 Chess

Last moveRook H3

Grand Prize2,130.01USD↑

Current Position981NTH