



ethereum
vienna

General Introduction



Project

Decentralisation of the web

Removing the role of central points

Takes away control from service owners

Data cannot just disappear

Data can only be modified by certain rules*

Censorship resistant

Server cannot freeze funds

* most of the time



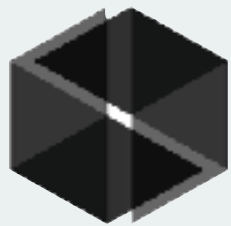
Web 3.0

Platform for decentralised applications (**DApps**)



Ethereum (Blockchain)

Consensus Layer



Whisper

Messaging and Broadcasting



Swarm / IPFS (Content System)

Data publication and distribution



DApps

Escrow Standard UI Wallet

Crowdfunding Weifund

Subscription Services (see workshop)

Prediction Markets Augur / Gnosis

Registries Namereg

Marketplace Safemarket

Decentralised Autonomous Organisations (DAO)

Stablecoins MakerDAO



ethereum

blockchain



Blockchain

Public record of all transactions

Stored and processed by all full nodes

Determines order of transactions

Necessary to determine current state of the system





Blockchain

Account based System

identified by a 160 bit address

has a balance of Ether / Wei

2 types of accounts

"Accounts" (external)

Contracts (internal)



Blockchain

Account (external)

user controlled account

controlled by a private key

can send and receiver ether

| | |
|--|--------|
| 0x1350cf34d093953ce0d2803648da8f3b6a84de77 | 100 |
| 0xd5f9d8d94886e70b06e474c3fb14fd43e2f23970 | 2500 |
| 0xd2963cd505c94dbf3bc663bdd2321bd3000204bb | 23290 |
| 0xd2963cd505c94dbf3bc663bdd2321bd3000204bb | 123809 |
| ... | ... |



Blockchain

Contract (internal)

Controlled by code (EVM byte-code)

Gets executed whenever it receives a message

Ether can only be sent out by the code

Persistent storage to preserve state across txs

Can send other messages during its execution

```
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
```



Blockchain

Code written in an ethereum specific language

- Solidity



high level

official language

- LLVM

lisp-like (low level)

- EVM Assembly

```
contract Coin {  
  
    event Transfer(address indexed from, address indexed to);  
  
    mapping (address => uint) public balances;  
  
    function() {  
        balances[msg.sender] = 10;  
    }  
  
    function Send(address to, uint amount) {  
        if(balances[msg.sender] >= amount) {  
            balances[msg.sender] -= amount;  
            balances[to] += amount;  
        }  
    }  
}
```



Blockchain

```
contract Coin {  
    event Transfer(address indexed from, address indexed to);  
    mapping (address => uint) public balances;  
  
    function() {  
        balances[msg.sender] = 10;  
    }  
  
    function Send(address to, uint amount) {  
        if(balances[msg.sender] >= amount) {  
            balances[msg.sender] -= amount;  
            balances[to] += amount;  
        }  
    }  
}
```

token contract

persistent storage
use to store balance



Blockchain

Message

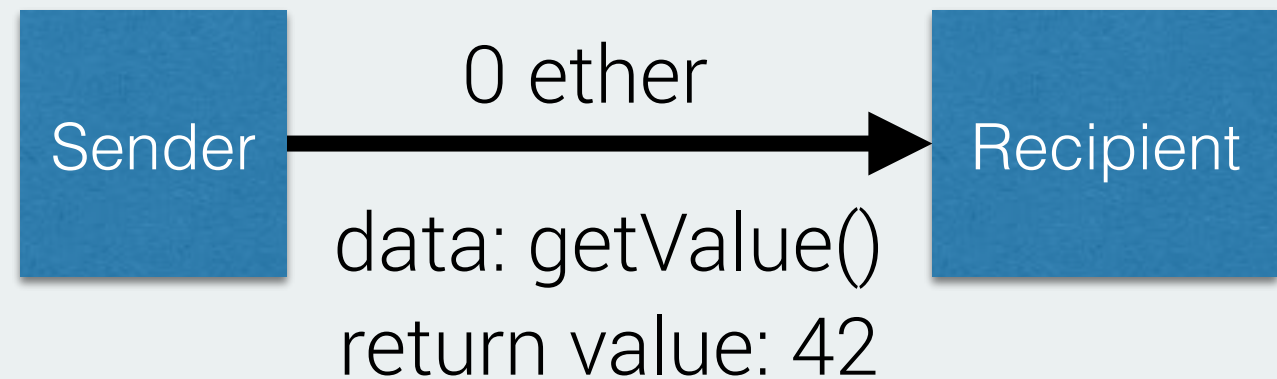
1 Sender

1 Recipient

Value in Ether / Wei (can be 0)

Can have additional data (for function calls)

Can have return value





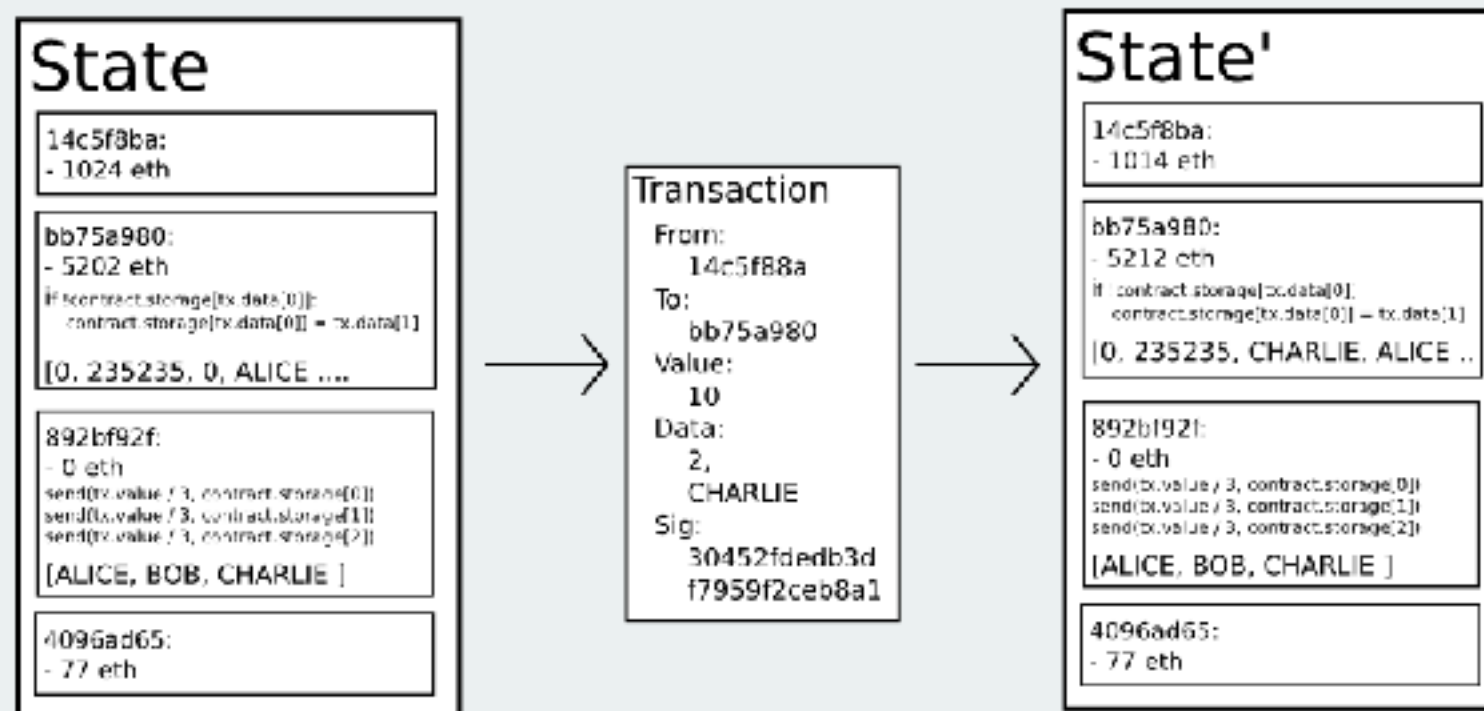
Blockchain

Transaction

Contains a message

Signed by a private key (external account)

Transitions from one state to the next





Blockchain

Gas

Used for transaction fees

Sender “buys” gas at a sender-specified **gasprice**

Every computational step has a fixed gas cost

Remaining gas sent back to sender

If gas runs out

- the state reverts

- but miner keeps ether



Blockchain

Gasprice

Associated gas cost for some action is constant

But the price of ether is not

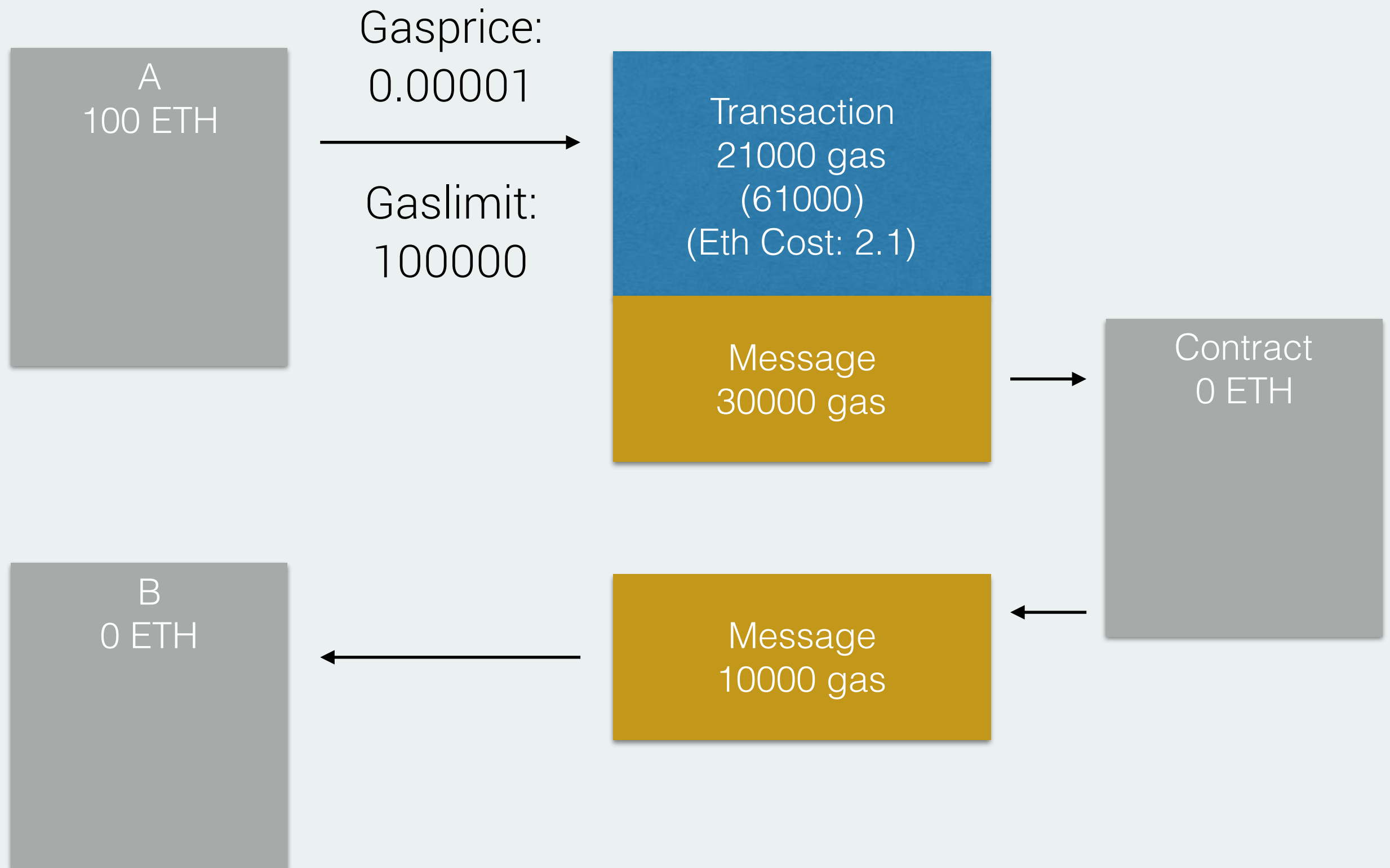
Gasprice is a scale factor against ether price

Ether goes up -> Gasprice goes down

Ether goes down -> Gasprice goes up

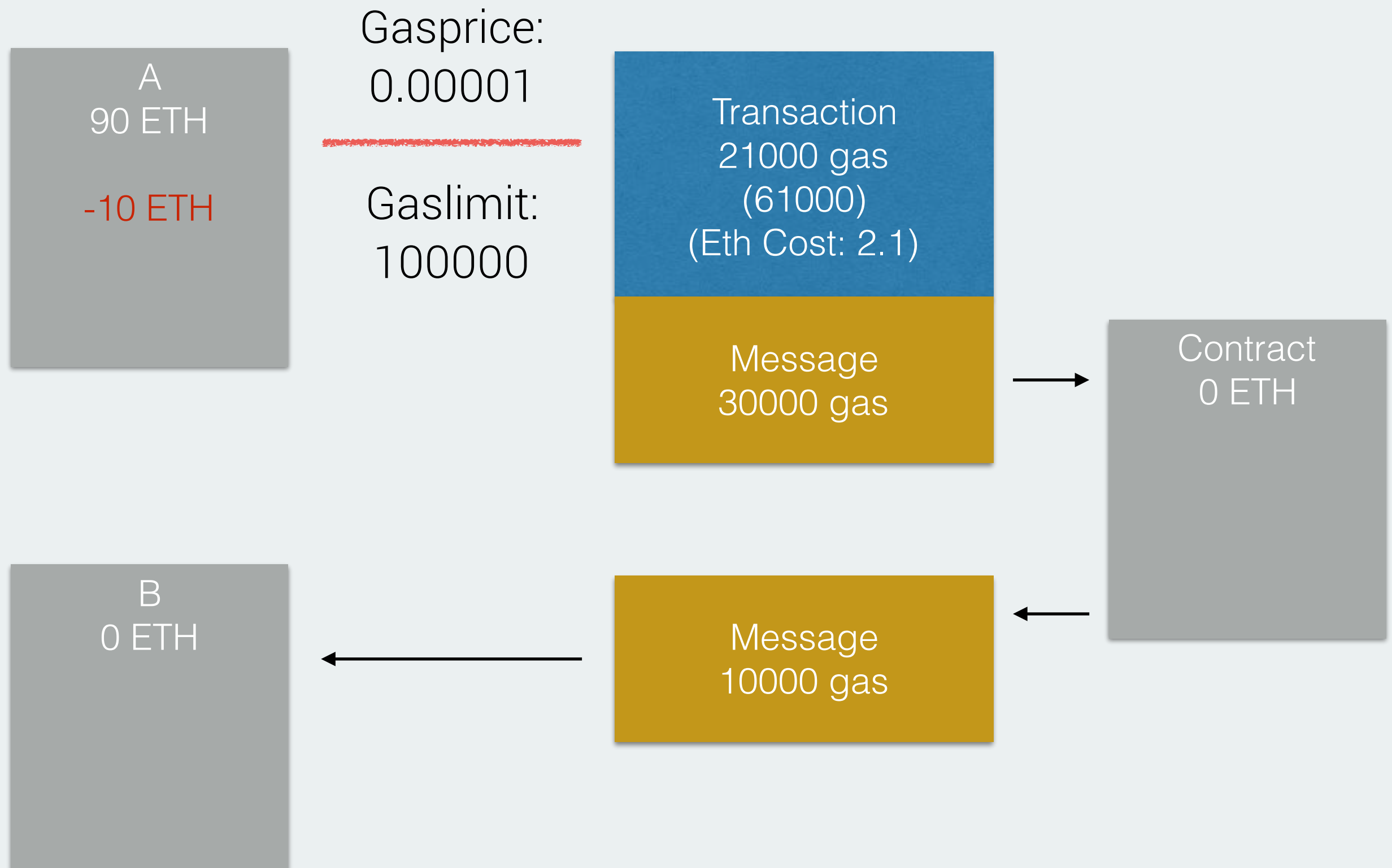


Blockchain



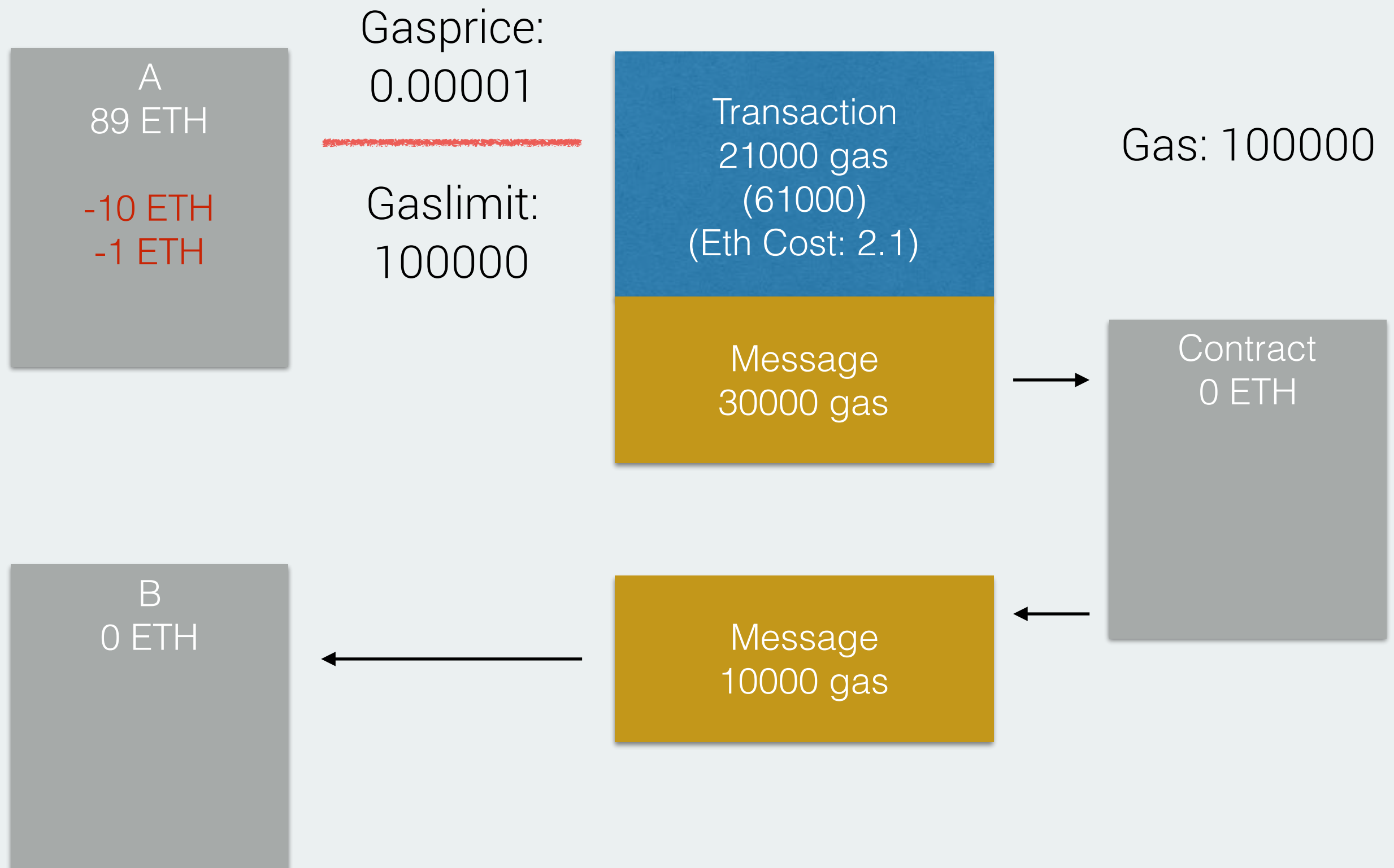


Blockchain



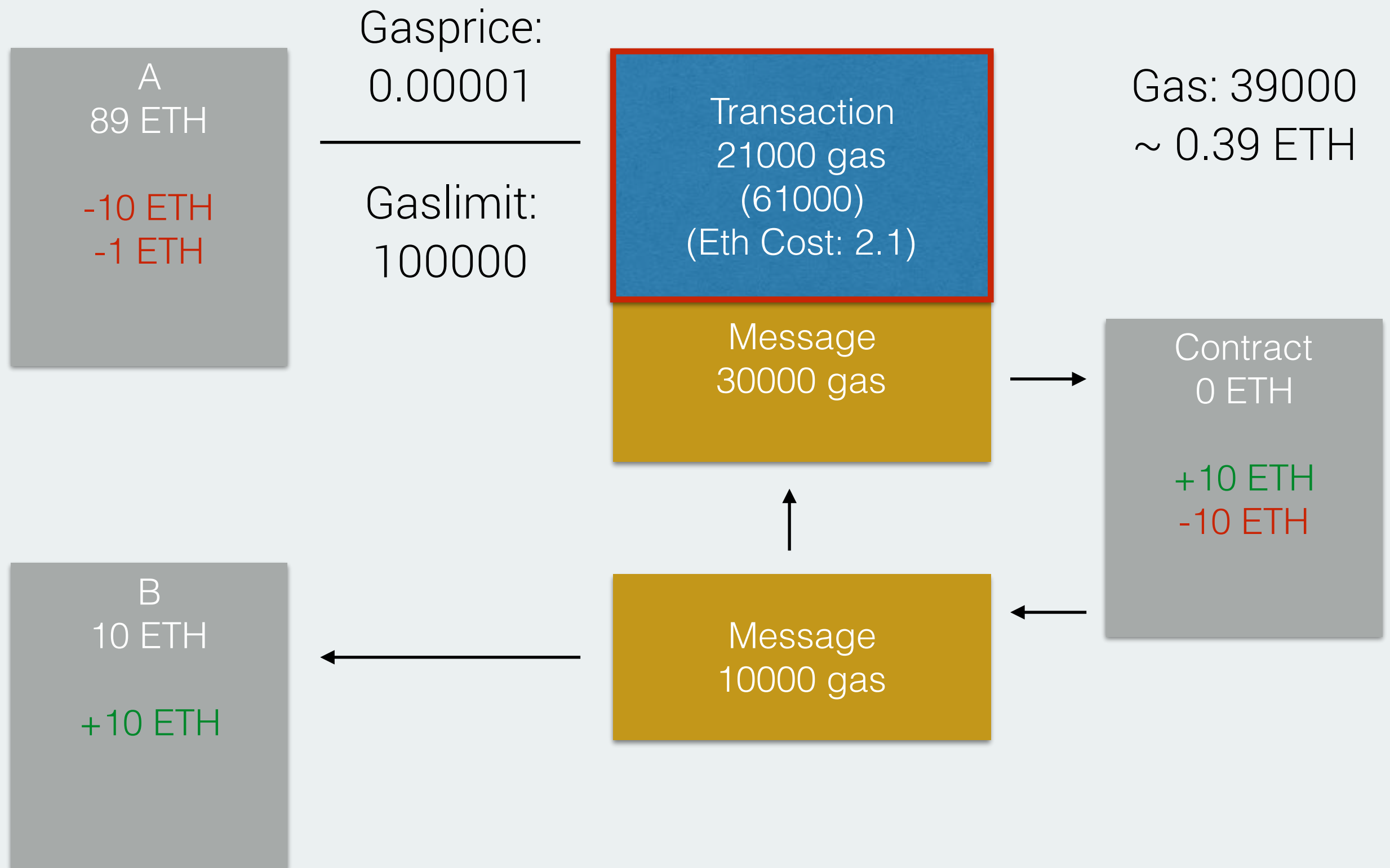


Blockchain



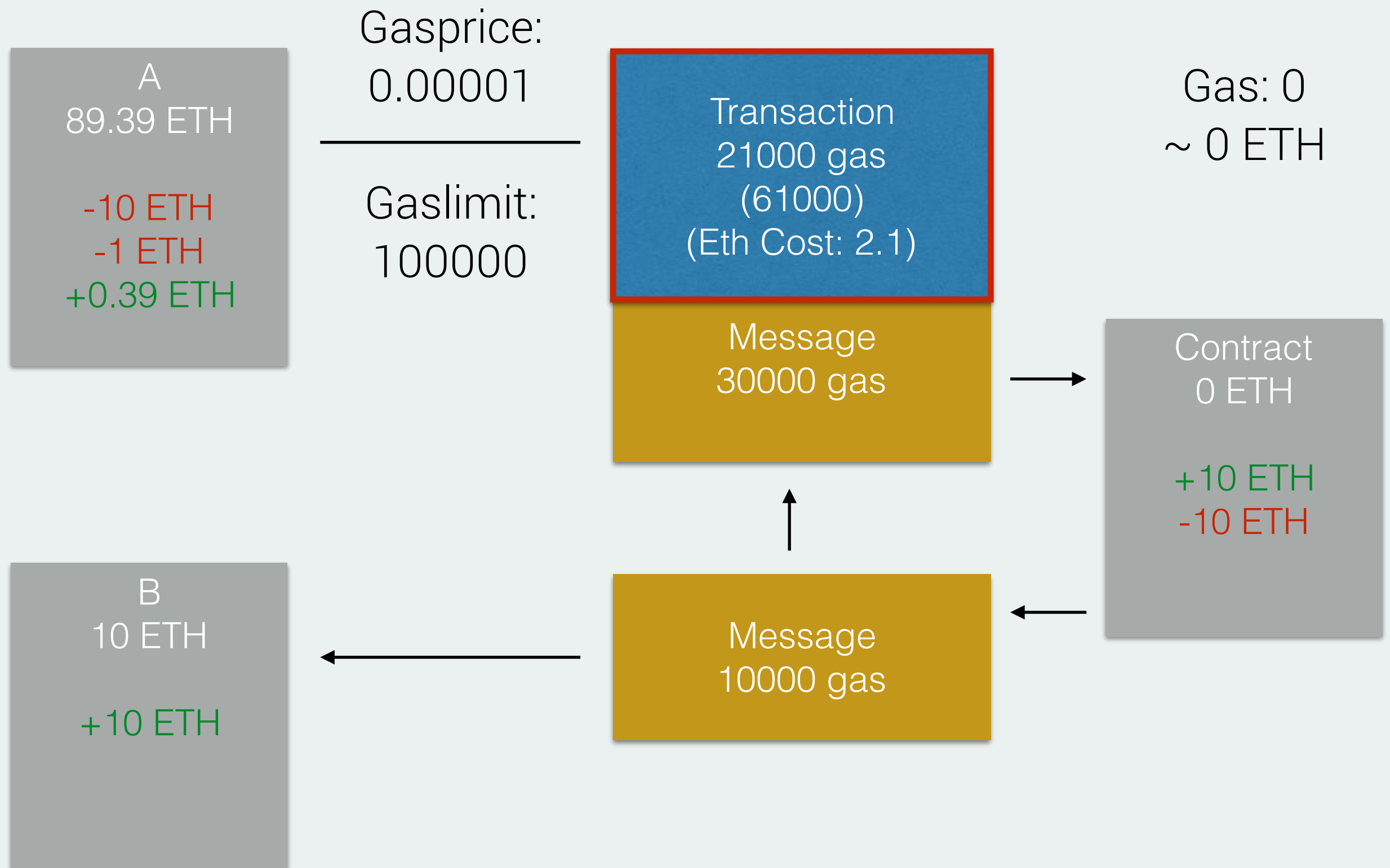


Blockchain





Blockchain

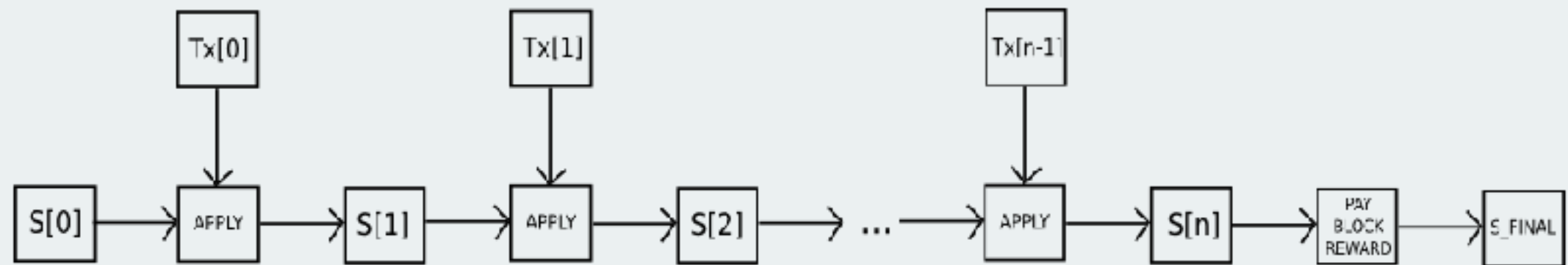




Blockchain

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 the same contract

Different order -> Potential different outcome

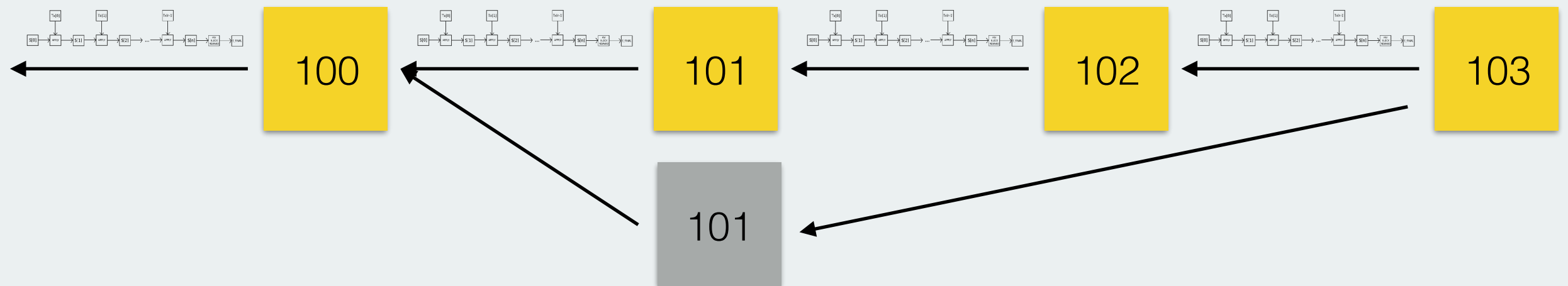


Blockchain

Blocks form a chain

~15 seconds apart

Some can uncle blocks



Longest chain is considered the consensus



Blockchain

Proof of Work (Ethereum 1.0)

EthHash

asic-resistant (high memory, io bandwidth)

targets gpu mining (2GB+ GRAM)

To be succeeded by Casper (PoS)

Constant Block Reward during PoW Phase



Blockchain

Yellow Paper (github: ethereum/latexpaper)

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER HOMESTEAD DRAFT

0xf1 CALL 7 1 Message-call into an account.
$$\mathbf{i} \equiv \mu_{\mathbf{m}}[\mu_{\mathbf{s}}[3] \dots (\mu_{\mathbf{s}}[3] + \mu_{\mathbf{s}}[4] - 1)]$$
$$(\sigma', g', A^+, \mathbf{o}) \equiv \begin{cases} \Theta(\sigma, I_a, I_o, t, t, & \text{if } \mu_{\mathbf{s}}[2] \leq \sigma[I_a]_b \wedge \\ C_{\text{CALLGAS}}(\mu), I_p, \mu_{\mathbf{s}}[2], \mu_{\mathbf{s}}[2], \mathbf{i}, I_e + 1) & I_e < 1024 \\ (\sigma, g, \emptyset, \mathbf{o}) & \text{otherwise} \end{cases}$$
$$n \equiv \min(\{\mu_{\mathbf{s}}[6], |\mathbf{o}|\})$$
$$\mu'_{\mathbf{m}}[\mu_{\mathbf{s}}[5] \dots (\mu_{\mathbf{s}}[5] + n - 1)] = \mathbf{o}[0 \dots (n - 1)]$$
$$\mu'_g \equiv \mu_g + g'$$
$$\mu'_{\mathbf{s}}[0] \equiv x$$
$$A' \equiv A \uplus A^+$$
$$t \equiv \mu_{\mathbf{s}}[1] \bmod 2^{160}$$

where $x = 0$ if the code execution for this operation failed due to an exceptional halting $Z(\sigma, \mu, I) = \top$ or if $\mu_{\mathbf{s}}[2] > \sigma[I_a]_b$ (not enough funds) or $I_e = 1024$ (call depth limit reached); $x = 1$ otherwise.

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

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



ethereum

Whisper / Swarm
Mist



Whisper

Decentralised Messaging

Messages can be filtered by topics

Very flexible

- Messages can be encrypted

- Messages can be signed

- Broadcast

PoW for spam protection and priority

Not designed for real time communication





Swarm

Swarm (or IPFS)

Reverse Hash-table

Originator of source unknown

Low-latency

Incentivation model for storage

merged into geth

Orange Papers





Mist

TEST-NET | 11 peers | 567,297 | 20s since last block

BROWSE

ETHEREUM WALLET
4.99 ETH

Wallets

Send

Etherbase 5 ETH


Main Wallet 0 ETH

WALLETS


SEND

CONTRACTS


4.99 ETH




Etherbase

 0x41219bb718473ad918462631f320b7abded54fbf


4.99 ETH




Deposit



Copy address



Show QR-Code





GoXcoin0.21000000 GOX


LATEST TRANSACTIONS

Filter transactions

Mar 15


Created contract

 Etherbase →  Created contract at

 0x176577fec9dea0b2984611f168b25bdabe5dfc1d

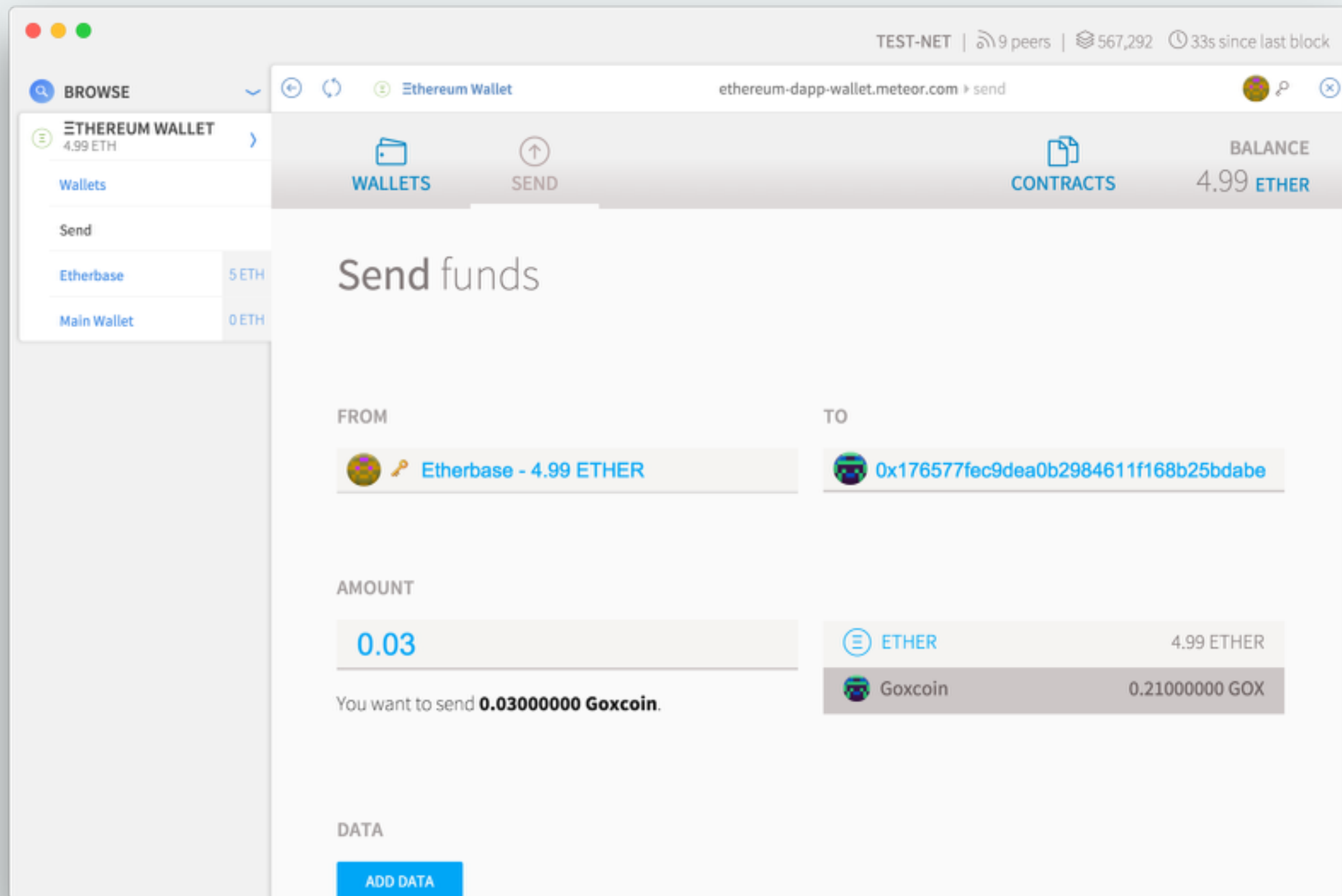
5 minutes ago

-0.00 ETH





Mist





ethereum

Mist

TEST-NET | 8 peers | 567,244 | 16s since last block

BROWSE

augur

augur

ETHereum WALLET
5.00 ETH

Markets

Portfolio

Reporting

My Markets

Cash: 9,998.20

Rep: 47.00

Ether: 4.99

Sign Out

Markets

New Market

Search

Volume

Open Markets

Showing 1 - 15 of 70

<

1

2

3

4

5

>

Which US Presidential candidate will win the US Presidency?

View Market

Multiple-Choice Market (6 outcomes)

End Date: Nov 9, 2016

Trading Fee: 2.0%

Volume: 352317.80 shares

TOP PREDICTIONS

| | |
|-----------------|-----|
| Hillary Clinton | 42% |
| Donald Trump | 41% |
| Bernie Sanders | 12% |
| John Kasich | 3% |
| Mario Rubio | 1% |

YOUR TRADING

| | | | |
|---------------|------|----------------|------|
| Positions | 1 | Trades | 0 |
| Profit / Loss | 0.00 | Unrealized P/L | 0.00 |

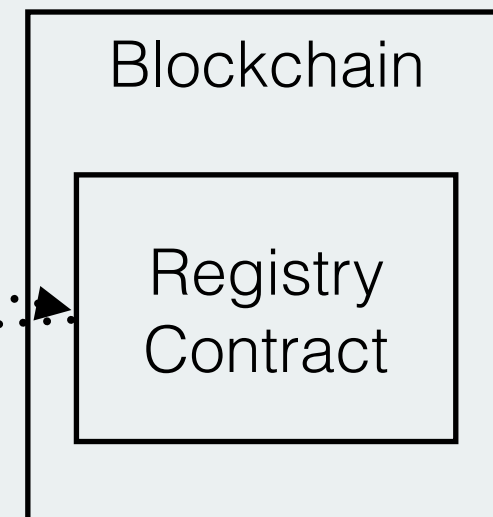
Marketplace DApp

Example



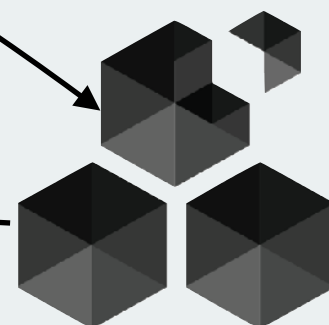
DApp

User enters URL



Registry translates URL to HASH

HTML
CSS
JSON



URL

HASH

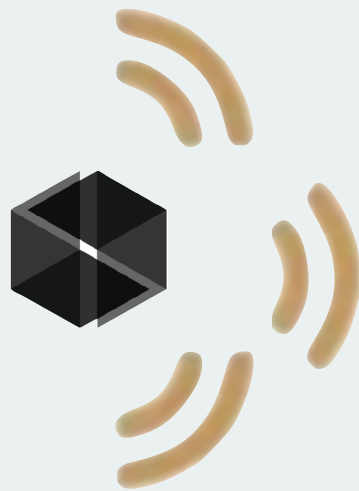
HASH



Marketplace

**Alice wants to sell a cup
for 10 ETH**

Whisper Broadcast
"I want to sell a cup for 10 ETH"



Broadcasts a Whisper message



ethereum

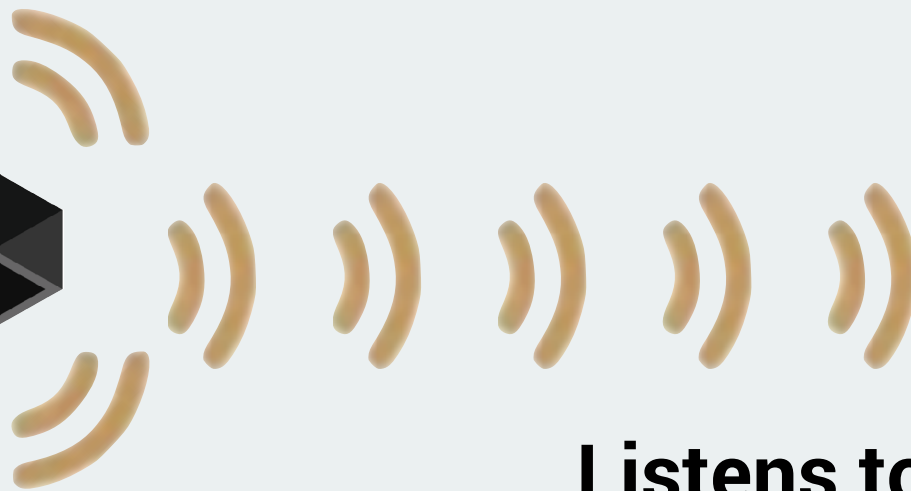
Marketplace

Bob wants to buy cups

10 ETH



Alice



Bob

Listens to the relevant messages



ethereum

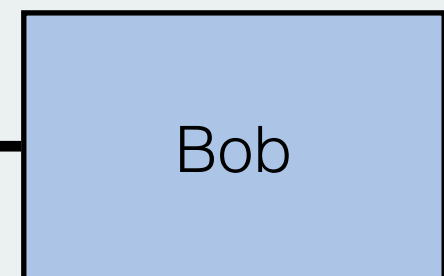
Marketplace

**Bob sees Alice's offer
and wants to buy**



Alice

Encrypted Whisper Message
"I want to buy the cup"



Bob

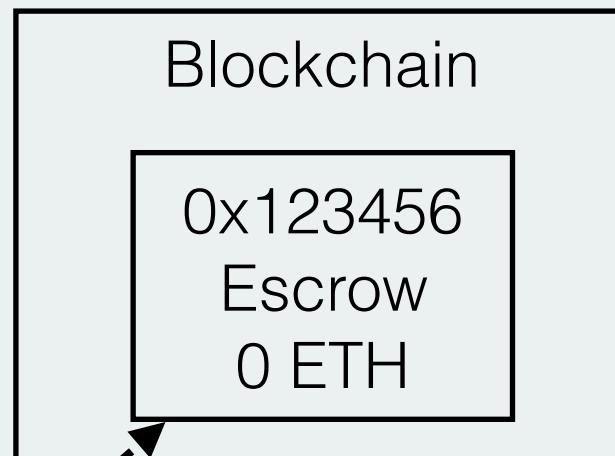
Sends a private message to Alice



ethereum

Marketplace

**Alice and Bob do not
trust each other**



Alice

Bob

Alice creates an escrow contract

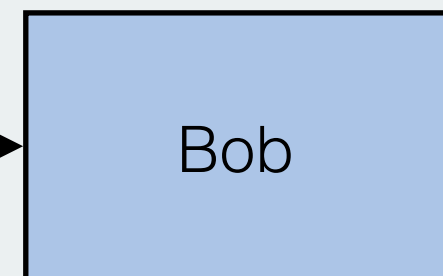


ethereum

Marketplace



Encrypted Whisper Message
"Escrow contract at 0x123456"



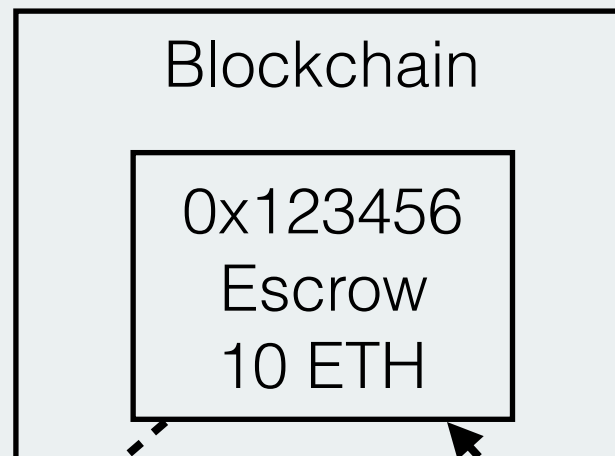
Alice informs Bob about the escrow



ethereum

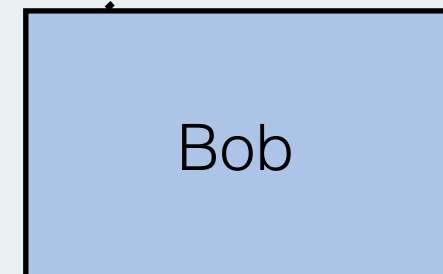
Marketplace

Funds now held by escrow



Bob pays

Event notification
"Bob payed"



10 ETH

Alice watches the blockchain

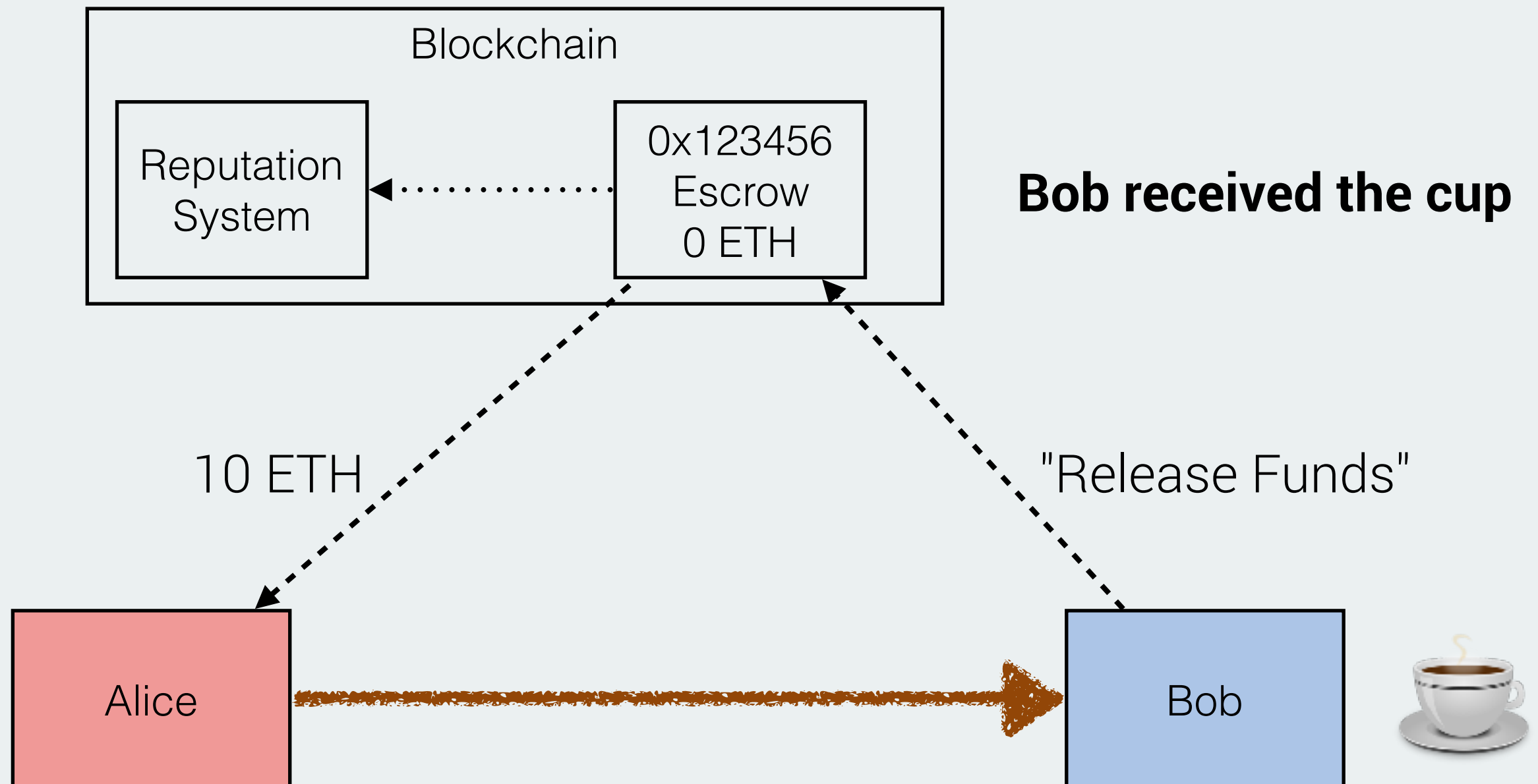
ethereum Marketplace





ethereum

Marketplace





Funding

Funded by crowdfunding

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

Over 9000 Transactions

half of that value lost due to bitcoin price decline

but rise in ether price secured funding for 4 years



2.0

Abstraction

- Contract pays fee

- Other signing mechanisms

Casper

- Proof of Stake with weak subjectivity

- Prediction market for blocks

Scalability

- Sharding



ethereum

Release Process

OLYMPIC

FRONTIER

Homestead
Hardfork

Retrieved ether
from DAO attacker

Removes bloat from
DDos Attacks

Release of **Mist**
DApp Store
Full Light Client
Abstractions (Part I)

HOMESTEAD

DAO
HF

EIP
150

EIP
161

HF
2017

METROPOLIS

HF
???

Ethereum 1.0 chain
UI Wallet

Stops
DDos Attacks

Casper
Abstractions

SERENITY

More
HFs



ethereum

Release Process

