Real world use case for blockchain

Max Edwards
@maxwedwards

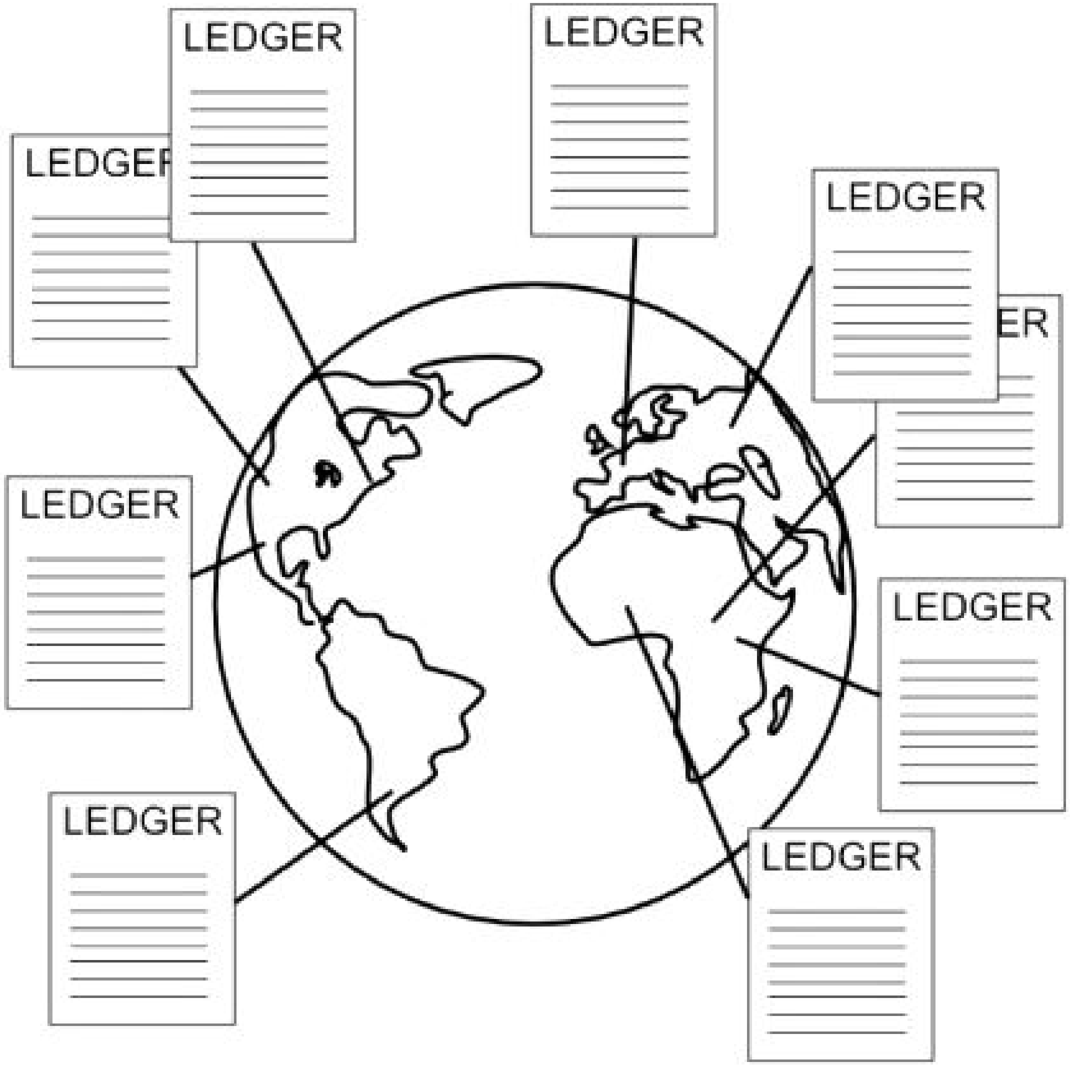
Agenda

Blockchain - what is it?

- Bitcoin
- Ethereum

Use case:- Academic peer review

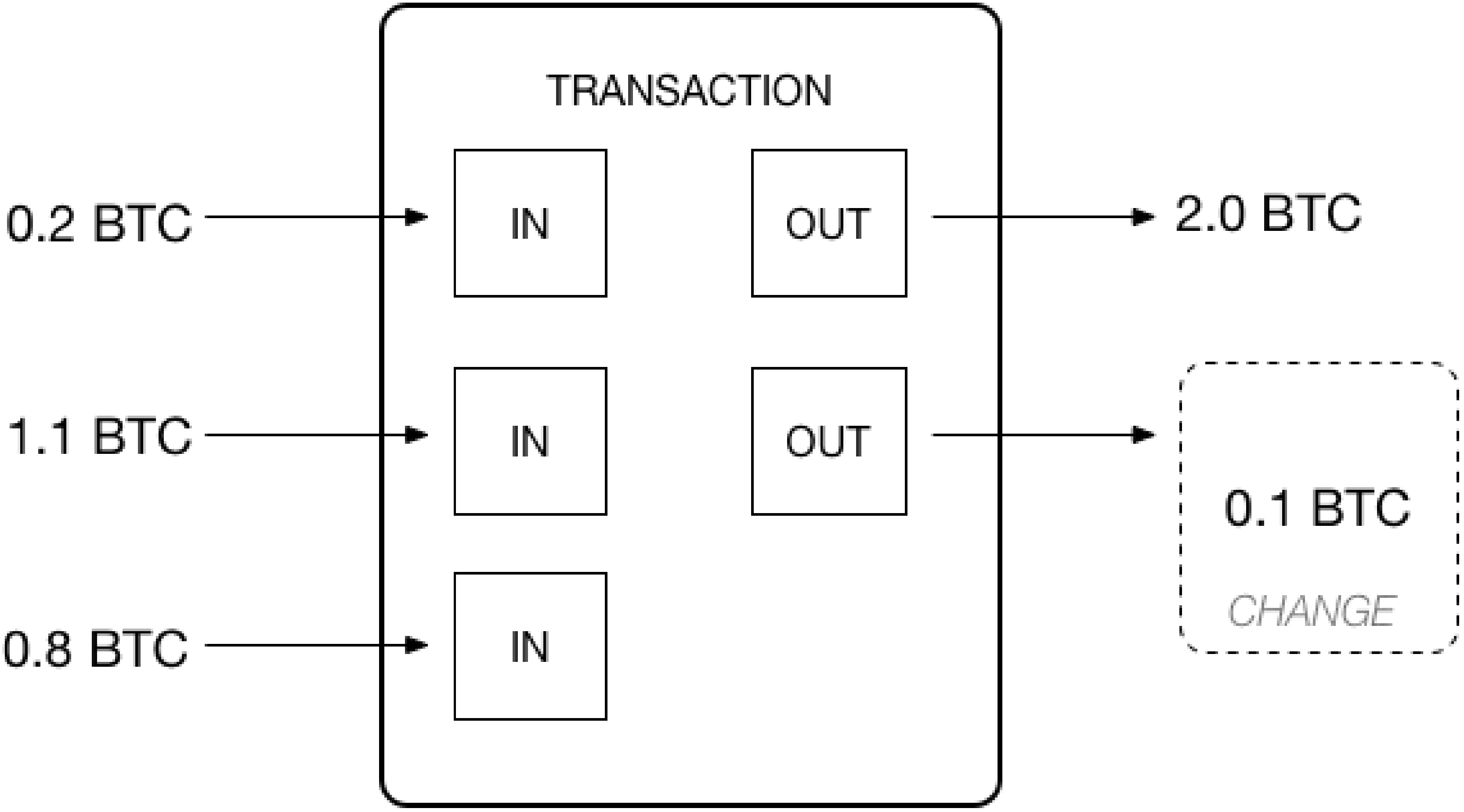
bitcoin


LEDGER
LEDGEF
LEDGER
LEDGER
ER
LEDGER
LEDGER
LEDGER
LEDGER

Typical Transaction

Alice wants to pay Bob 5BTC

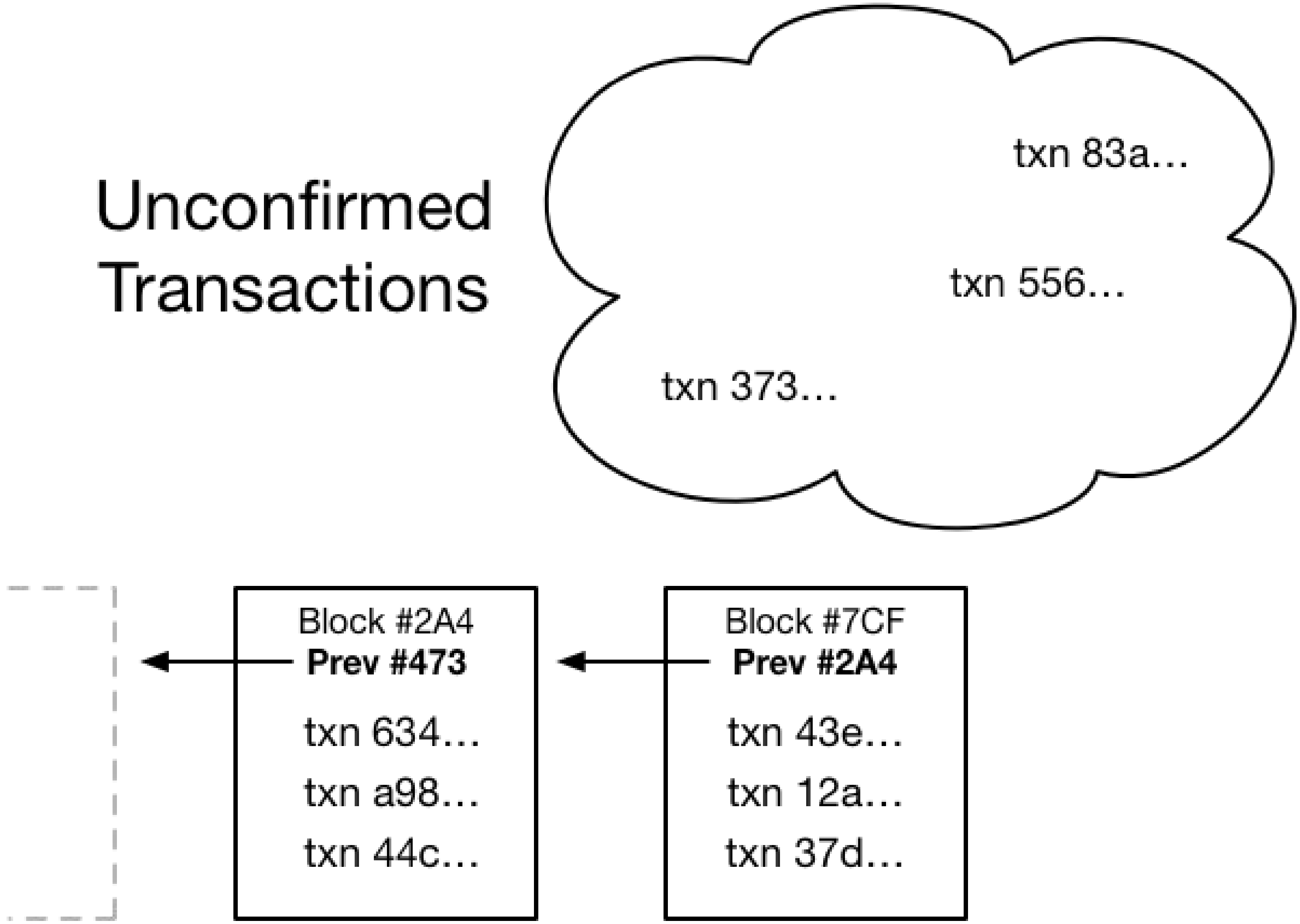
```
Input:
Previous transaction: f5d8ee39a430901c91…
Signature: 304502206e21798a42fae…

Output:
Value: 5 BTC
Public Key: 404371705fa9db…
```


TRANSACTION
0.2 BTC
IN
OUT
2.0 BTC
1.1 BTC
IN
OUT
0.1 BTC
CHANGE
0.8 BTC
IN

Ledger

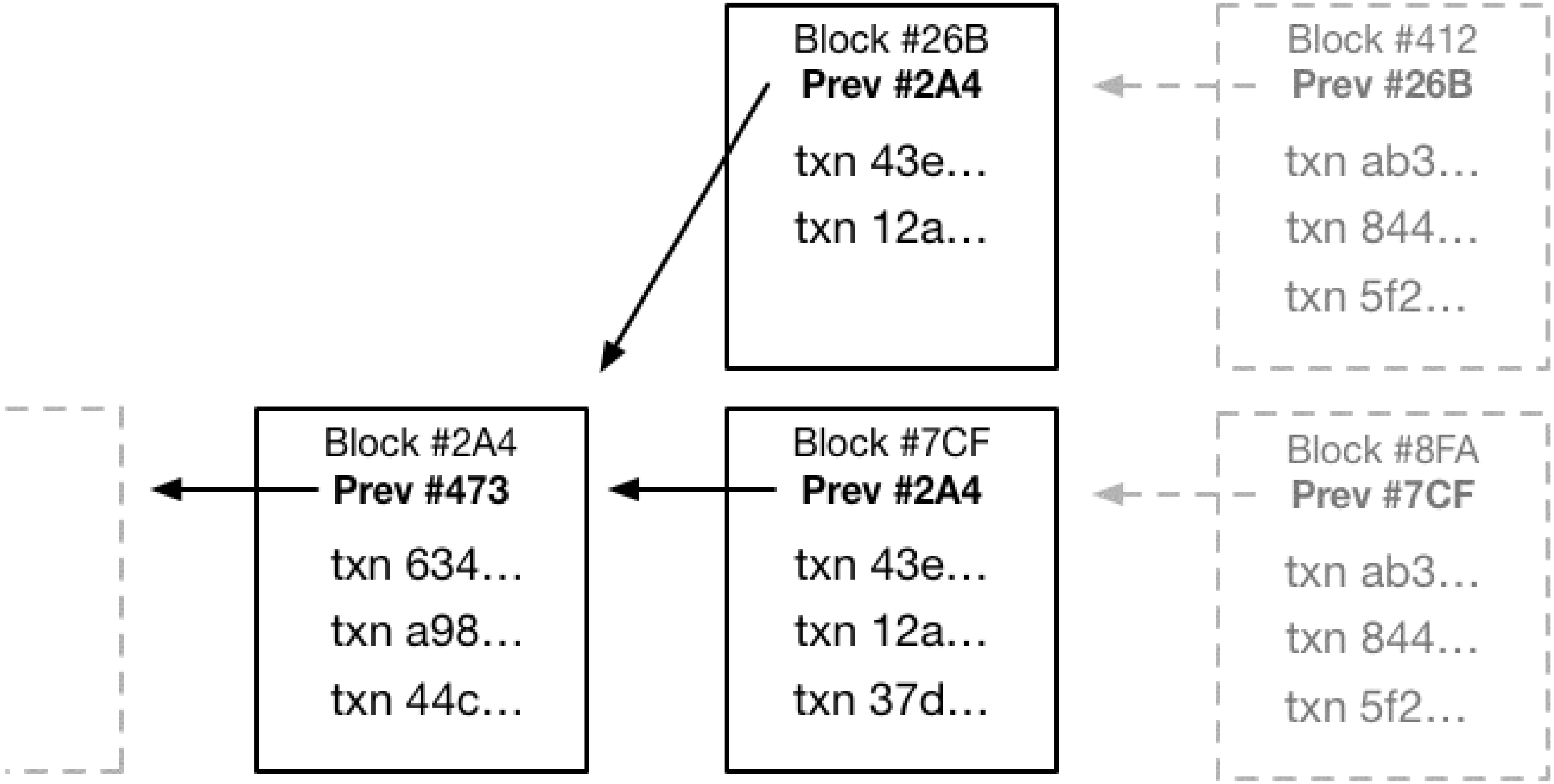
TX ID	Previous TX ID	To	Amount
...	...	...	...
~~300~~	~~184~~	~~Alice~~	~~1~~
~~301~~	~~254~~	~~Alice~~	~~1.5~~
302	300, 301	Bob	2.5

Blockchain - It’s in the name

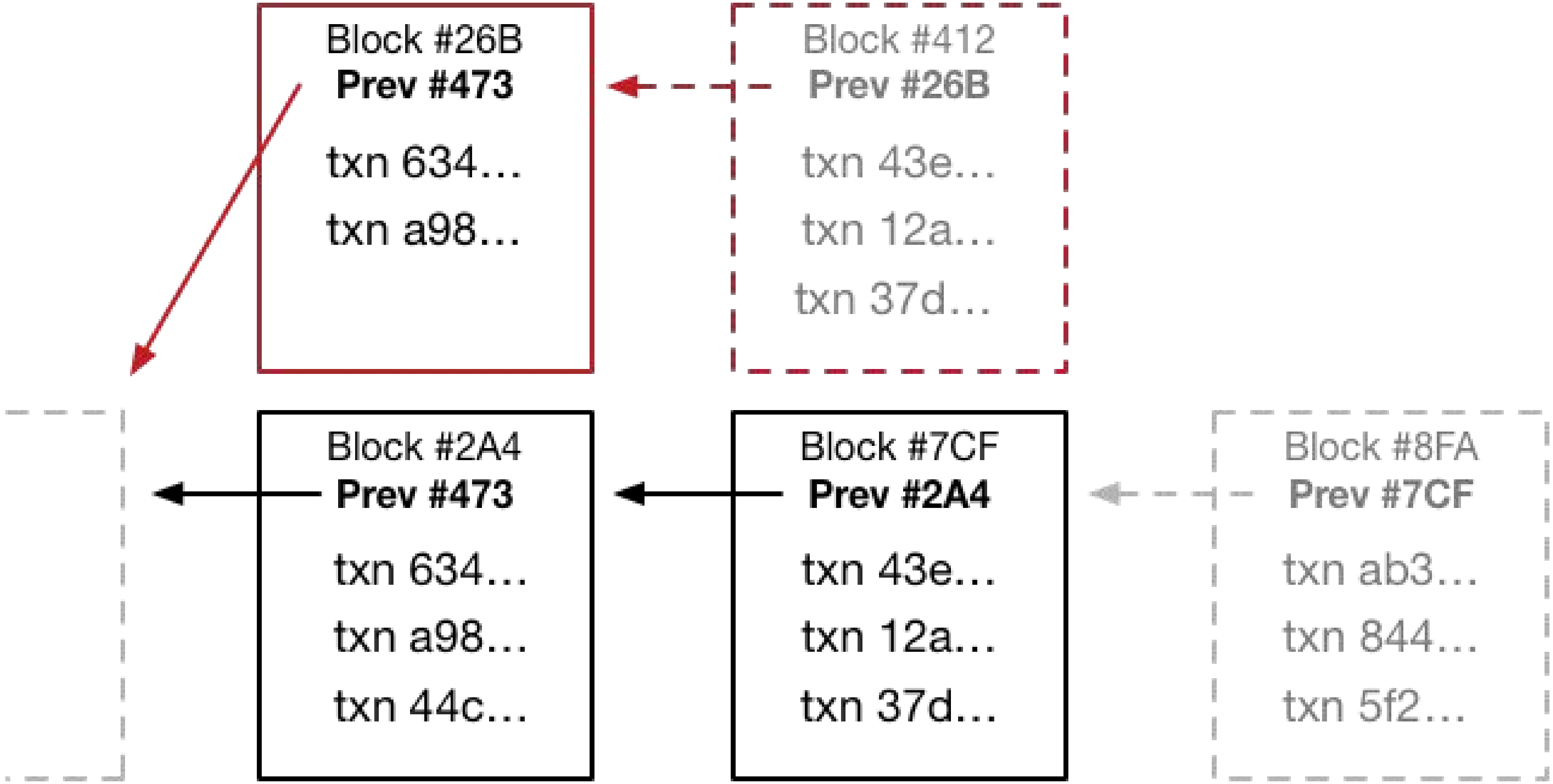


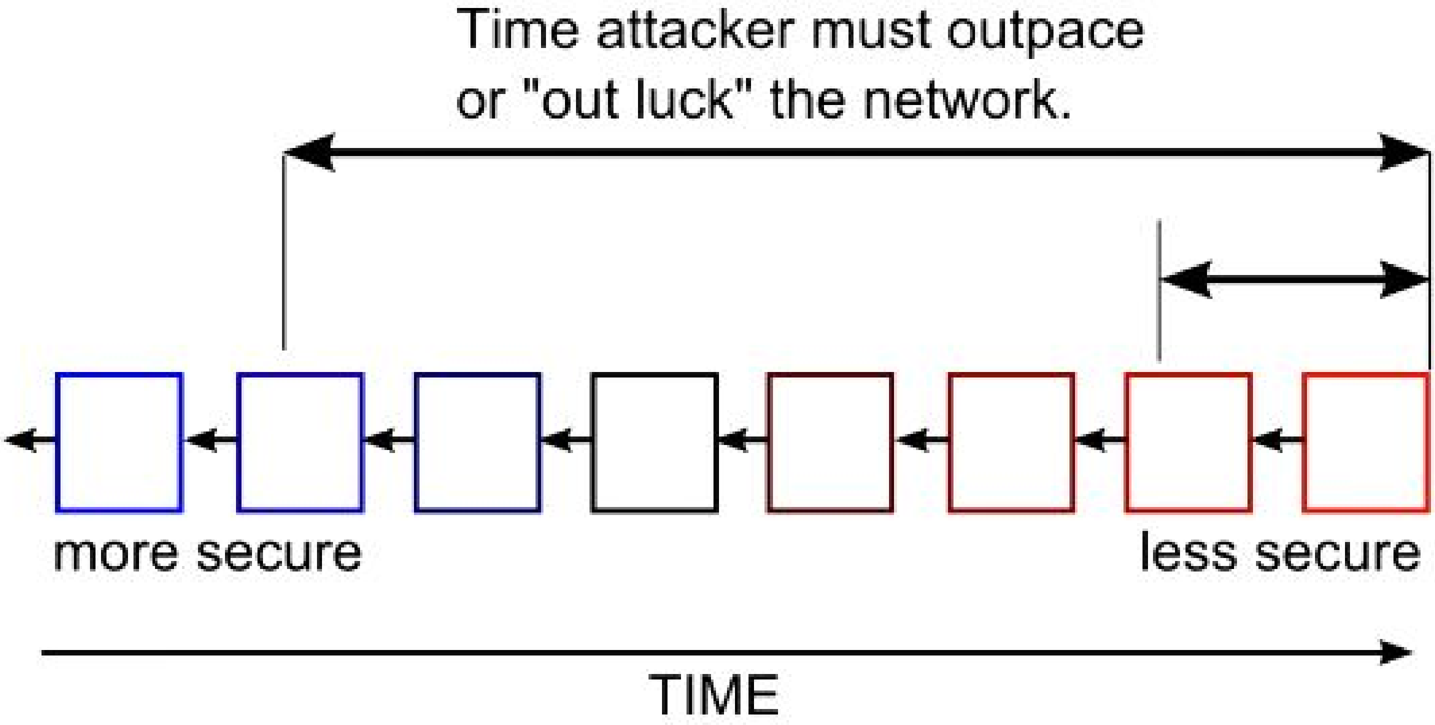
hash(Block data + random nonce)
= number with n leading 0s

Orphaned Blocks



51% Attacks


Block #26B
Prev #473
txn 634…
txn a98…
Block #412
Prev #26B
txn 43e…
txn 12a…
txn 37d…
Block #2A4
Prev #473
txn 634…
txn a98…
txn 44c…
Block #7CF
Prev #2A4
txn 43e…
txn 12a…
txn 37d…
Block #8FA
Prev #7CF
txn ab3…
txn 844…
txn 5f2…



Time attacker must outpace or "out luck" the network.

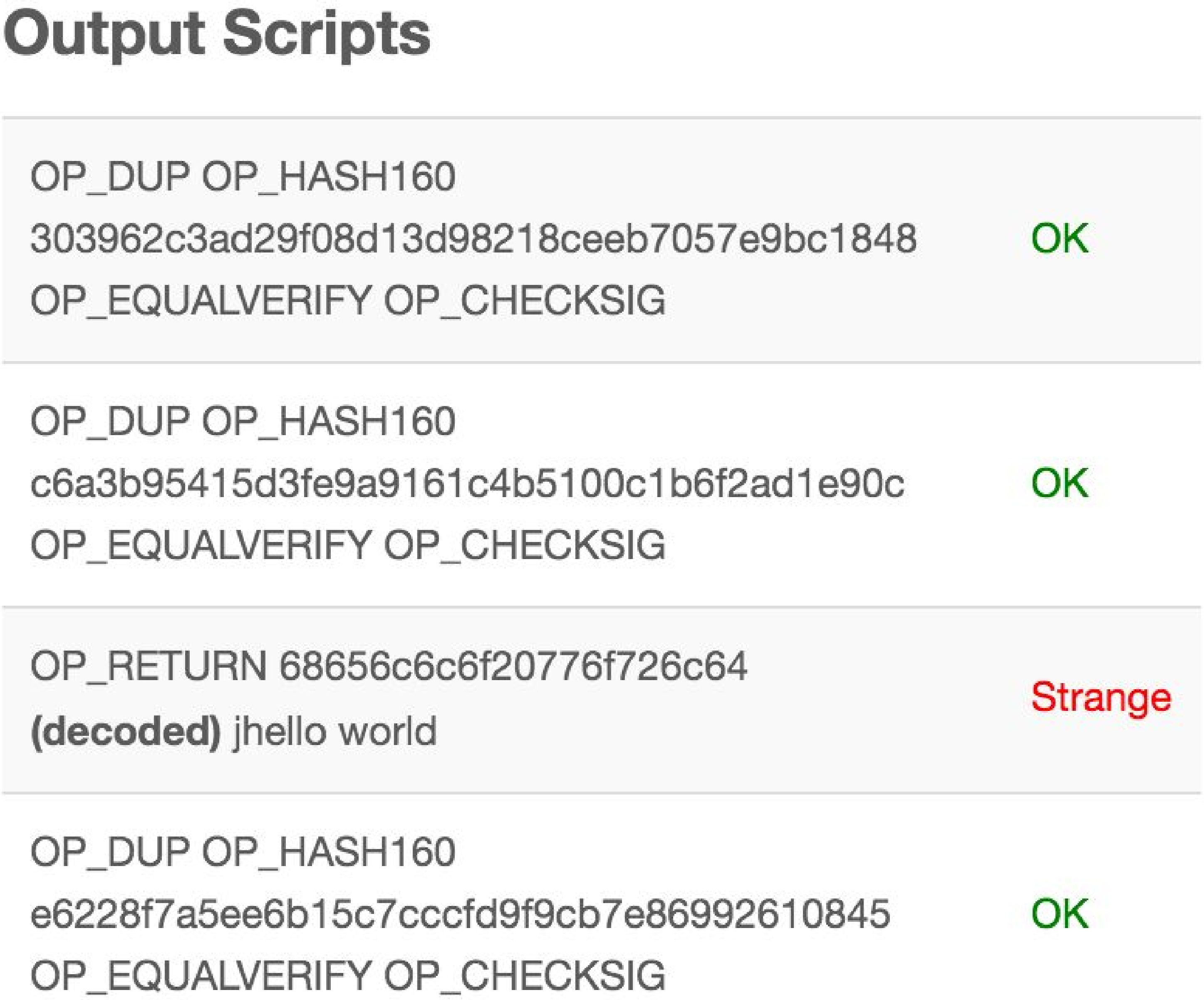
more secure

less secure

TIME

Distributed Ledger - capable of more?

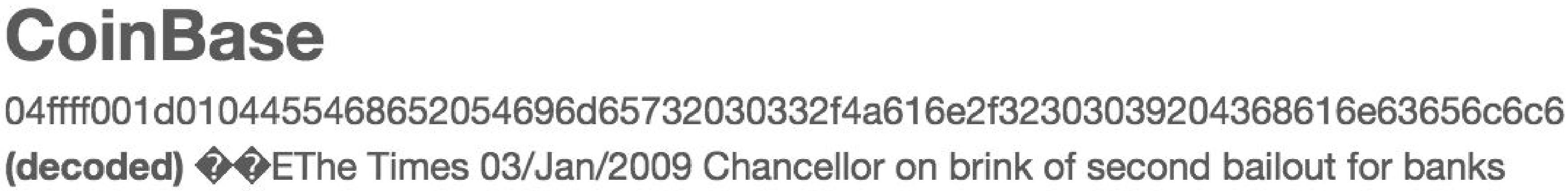
David Mondrus and Joyce Bayo - 2014 - Bitcoin Conference - Disney, Florida



Output Scripts

OP_DUP OP_HASH160 303962c3ad29f08d13d98218ceeb7057e9bc1848 OP_EQUALVERIFY OP_CHECKSIG	OK
OP_DUP OP_HASH160 c6a3b95415d3fe9a9161c4b5100c1b6f2ad1e90c OP_EQUALVERIFY OP_CHECKSIG	OK
OP_RETURN 68656c6c6f20776f726c64 **(decoded)** jhello world	Strange
OP_DUP OP_HASH160 e6228f7a5ee6b15c7cccfd9f9cb7e86992610845 OP_EQUALVERIFY OP_CHECKSIG	OK

tx/8881a937a437ff6ce83be
3a89d77ea88ee12315f37f7
ef0dd3742c30eef92dba



CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6

(decoded) ��EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks

block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Immutable Records

+

Distributed Consensus

What can Blockchain be used for?

Finance
Money
Micropayments
Escrow
Betting

Provenance
Diamonds
Food ingredients
Collectable Trainers
(Sneakers)

Digital Identity
Reviews and
Endorsements
Prediction Markets
Public sector and
governments

Asset Issuance
Gold
Land Title
Domain names

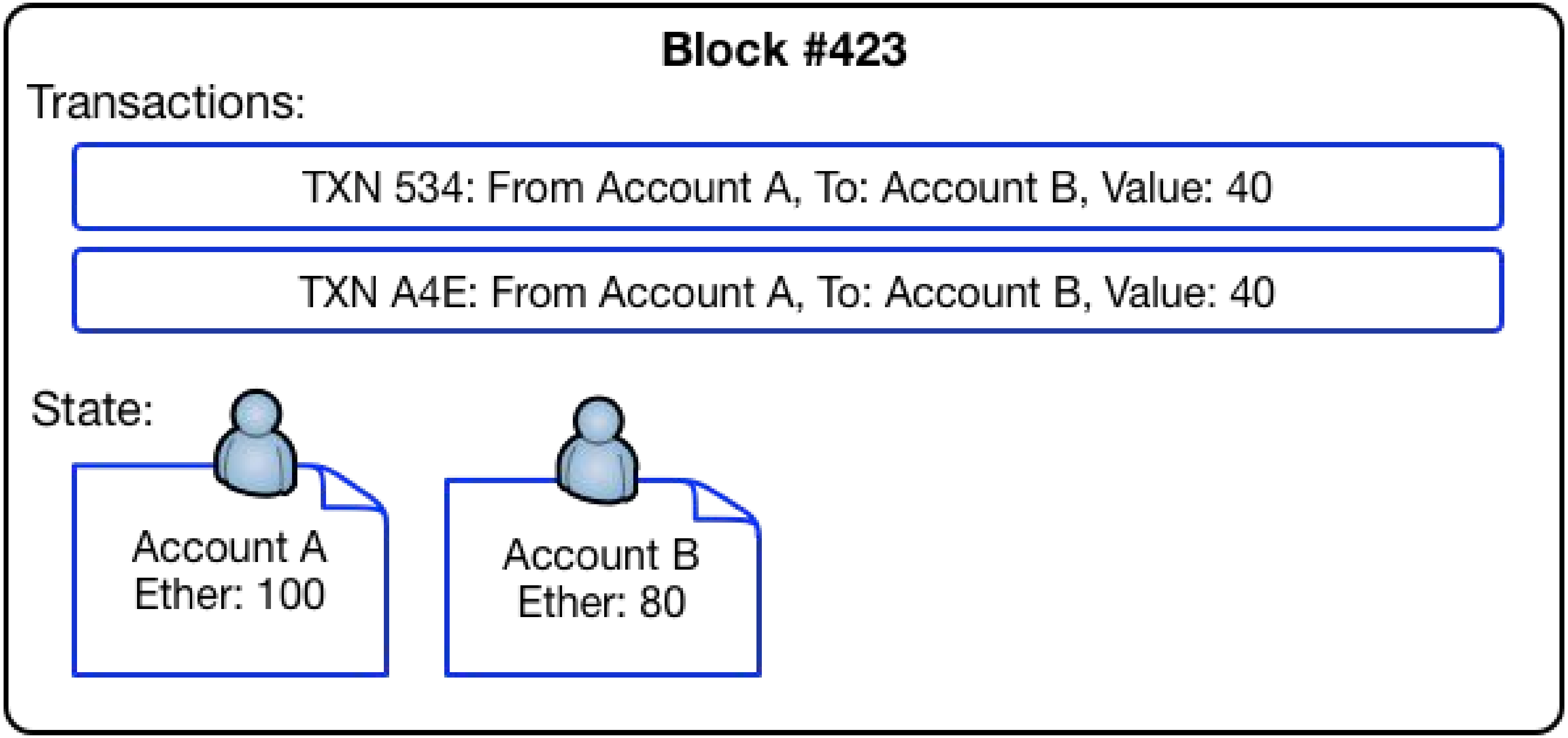
Namecoin

Coloured Coins

Metacoin

ethereum

Ethereum Block contains Transactions & State



Block #423

Transactions:

TXN 534: From Account A, To: Account B, Value: 40

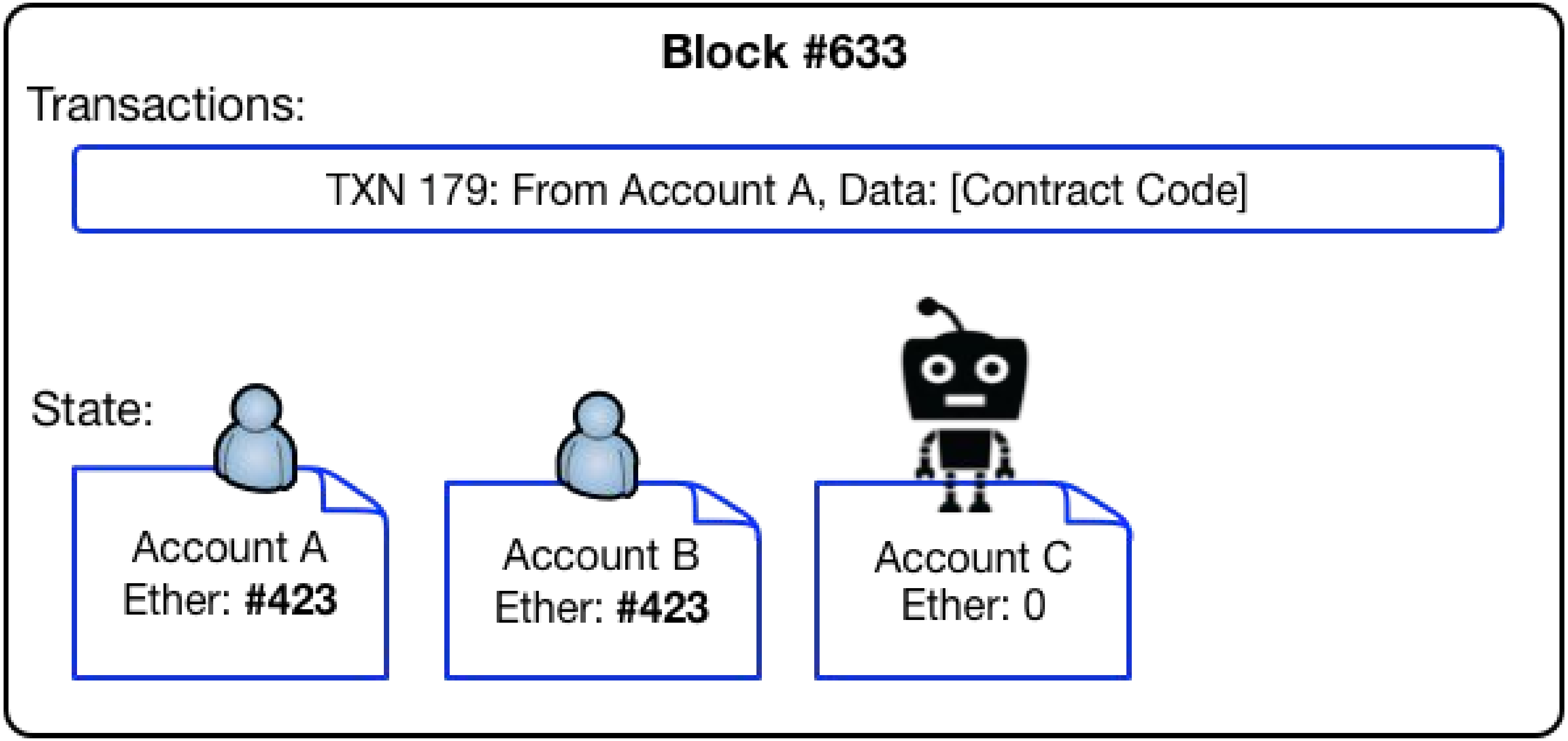
TXN A4E: From Account A, To: Account B, Value: 40

State:

Account A
Ether: 100

Account B
Ether: 80

Ethereum Accounts - Human / Code



Block #633

Transactions:

TXN 179: From Account A, Data: [Contract Code]

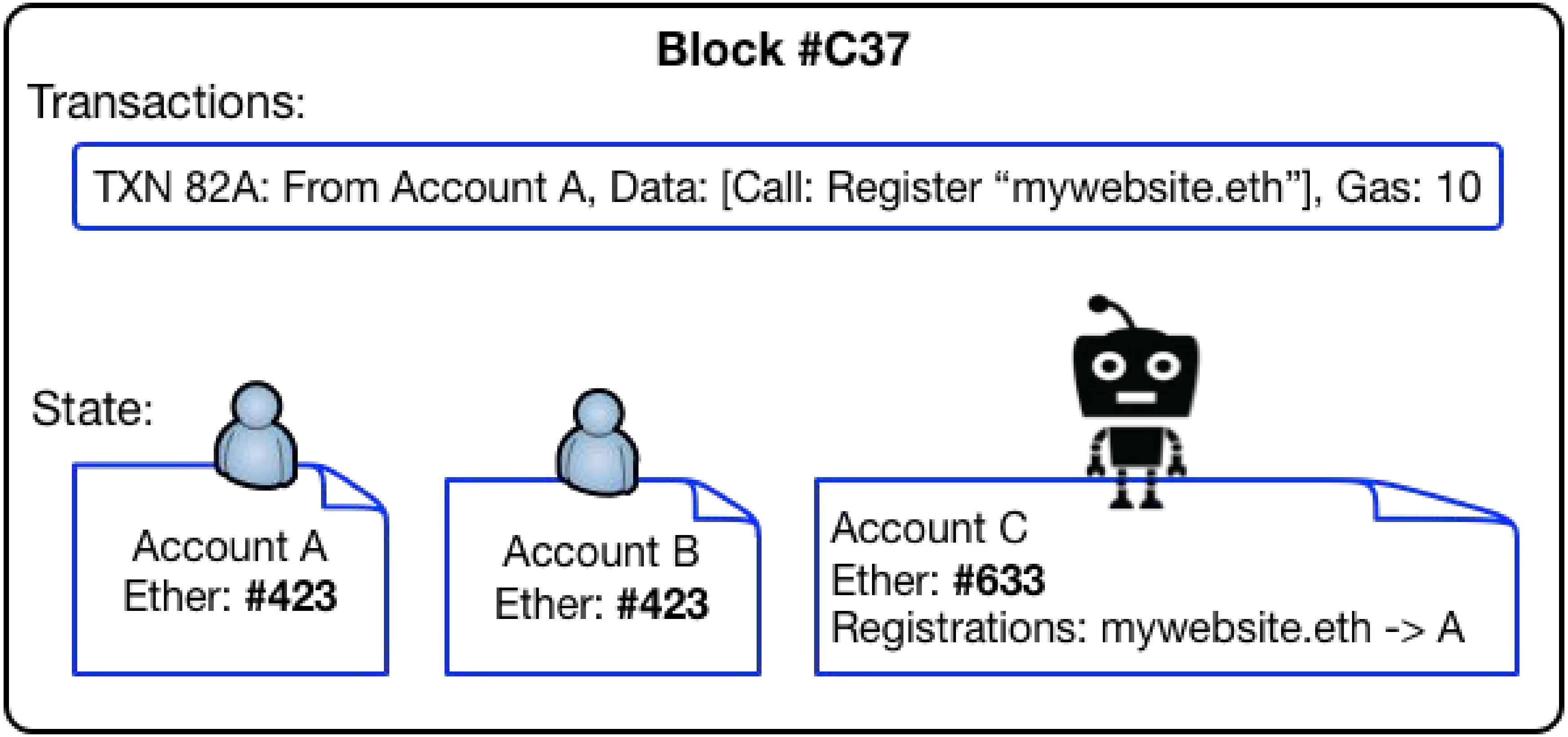
State:

Account A
Ether: **#423**

Account B
Ether: **#423**

Account C
Ether: 0

Smart contracts have state / storage



Block #C37

Transactions:

TXN 82A: From Account A, Data: [Call: Register “mywebsite.eth”], Gas: 10

State:

Account A
Ether: **#423**

Account B
Ether: **#423**

Account C
Ether: **#633**
Registrations: mywebsite.eth -> A

Domain Registration Smart Contract

Public Methods

Register (Name, IP_Address)

Lookup (Name)

Transfer (Name, Address To)

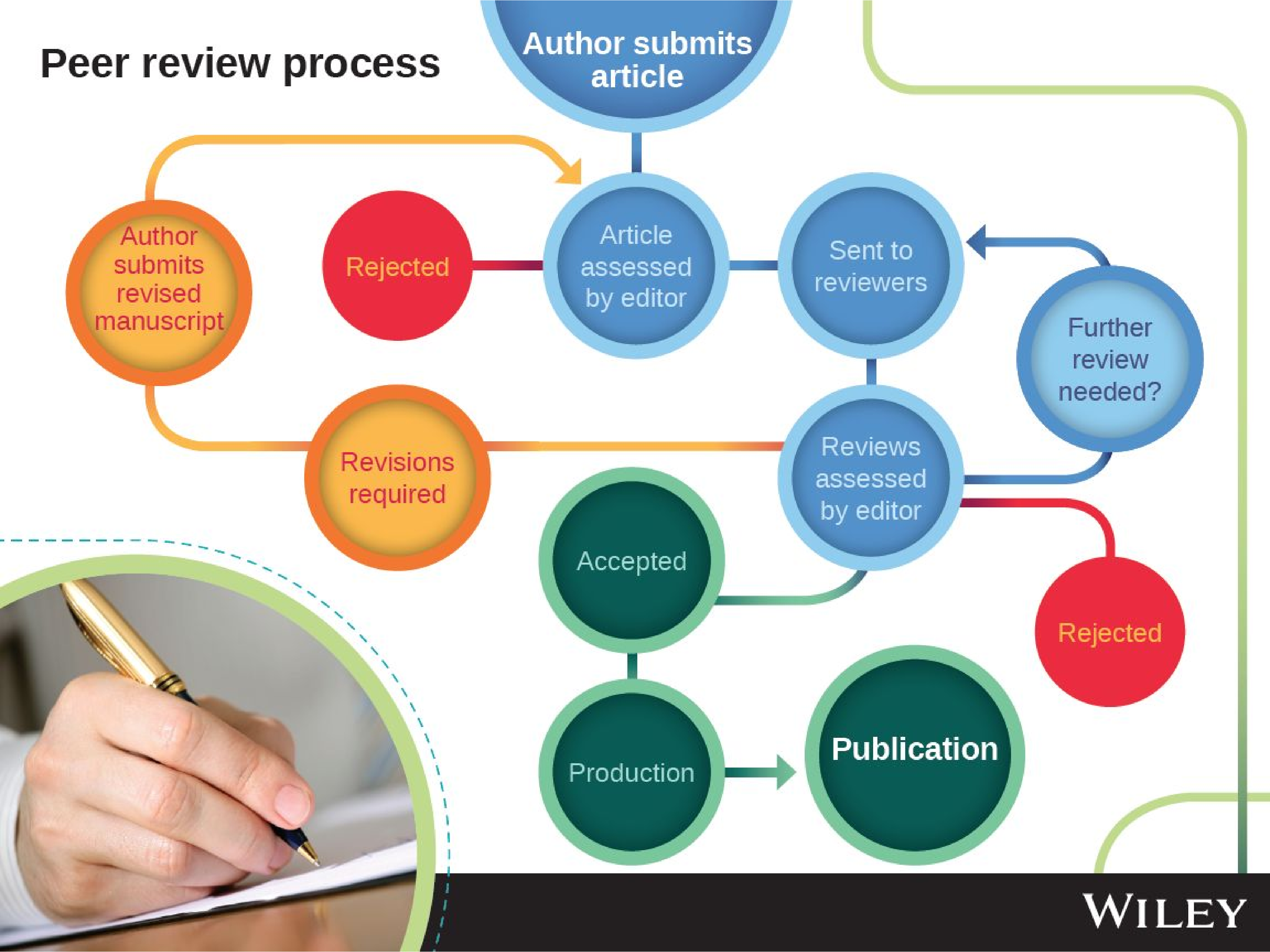
State

Mapping(Name, Address)

Mapping(Name, IP_Address)

Peer Review

Peer review process



Author submits article

Article assessed by editor

Rejected

Sent to reviewers

Reviews assessed by editor

Further review needed?

Rejected

Revisions required

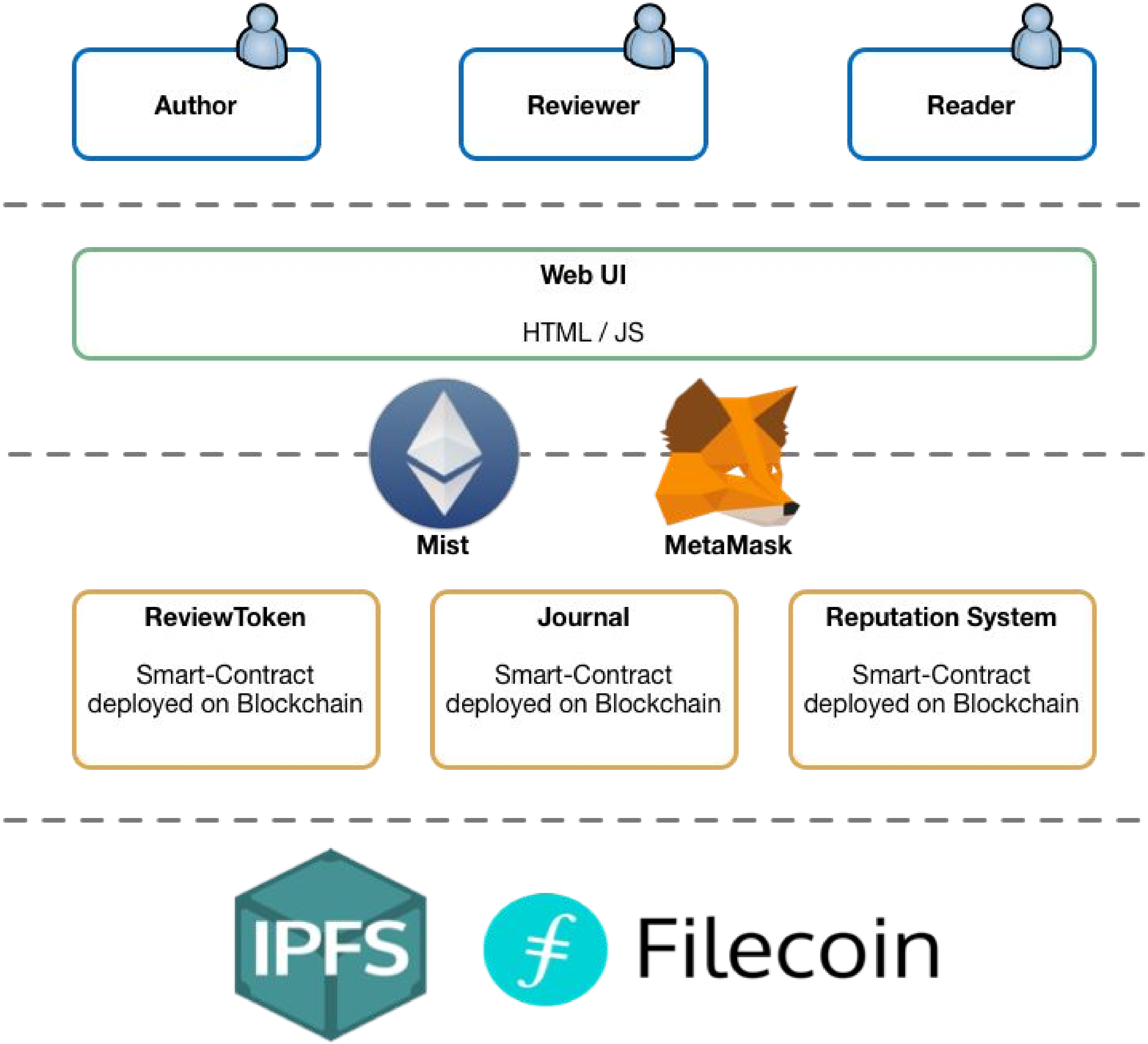
Author submits revised manuscript

Accepted

Production

Publication

On-chain peer reviewed journal



Author

Reviewer

Reader

Web UI

HTML / JS

Mist

MetaMask

ReviewToken

Smart-Contract deployed on Blockchain

Journal

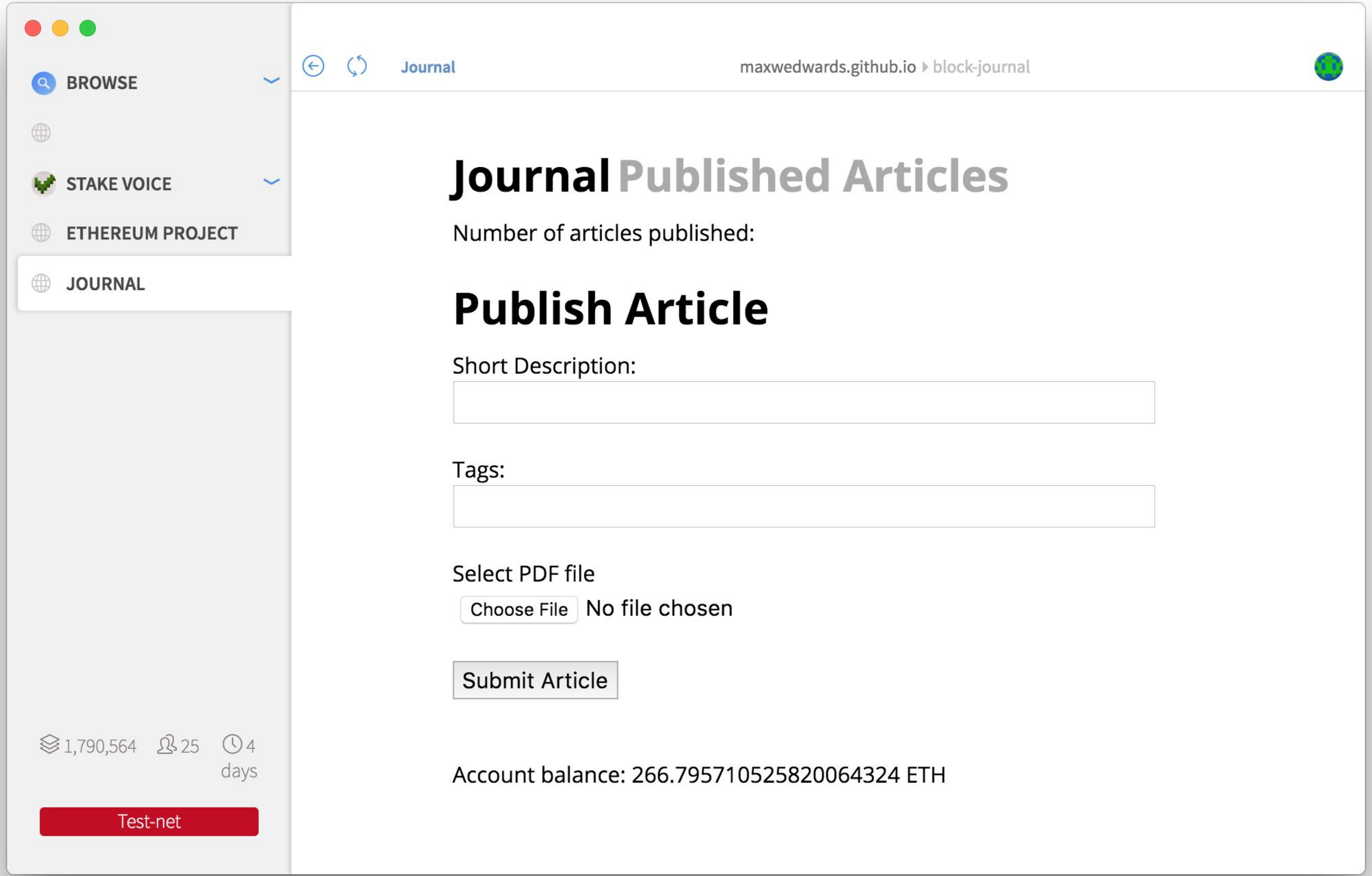
Smart-Contract deployed on Blockchain

Reputation System

Smart-Contract deployed on Blockchain

IPFS

Filecoin



Journal Published Articles

Number of articles published:

Publish Article

Short Description:

Tags:

Select PDF file

No file chosen

Account balance: 266.795710525820064324 ETH

Benefits of on chain

Complete transparency

Can alter the way “science is done” via a pull request!

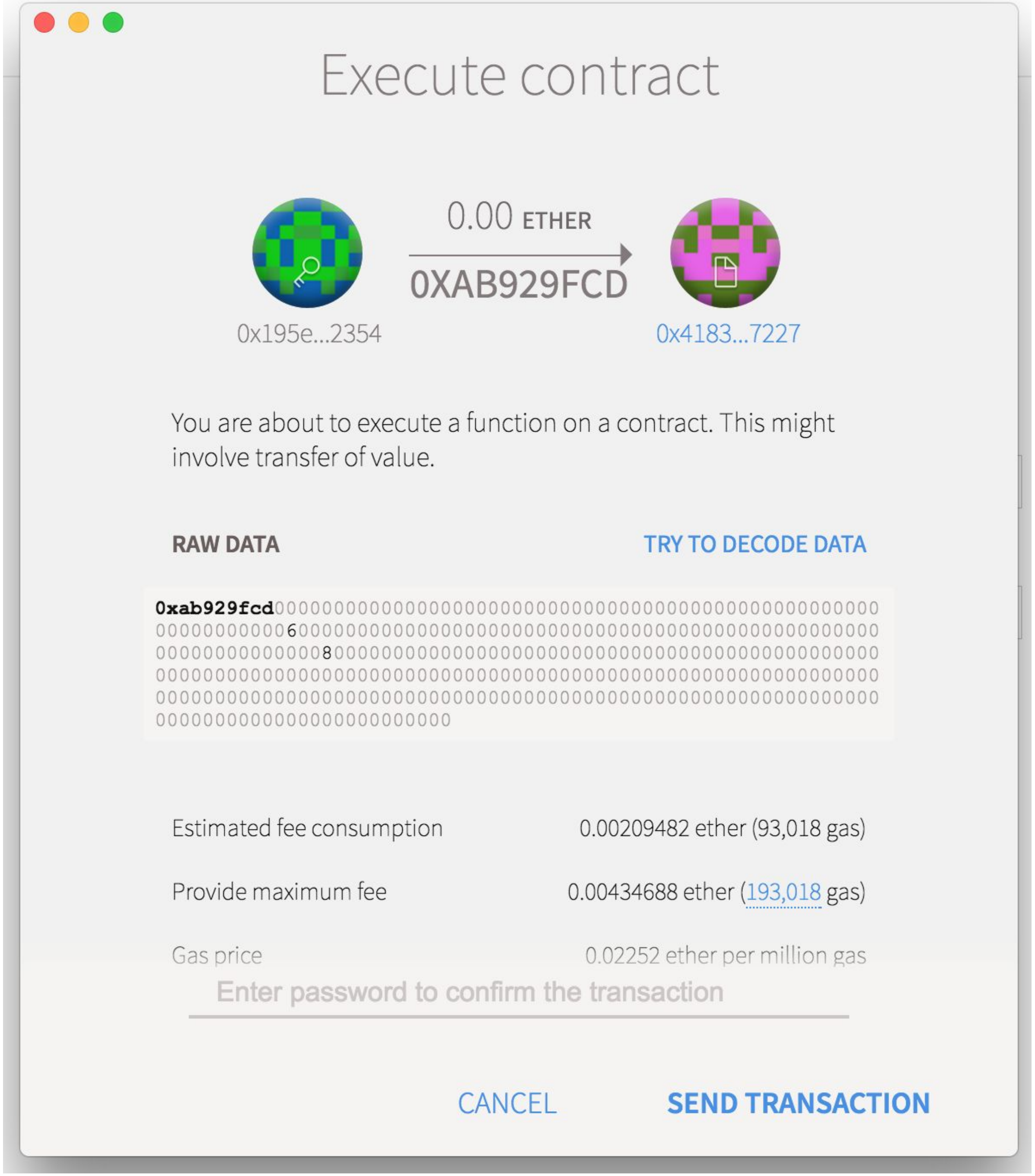
Multiple processes or “rules” could be run in parallel and compared

Effect of bias is greatly reduced

Guarantees free access for all forever

Payments for review or for hosting can be built into the protocol

Pitfalls



Execute contract

0.00 ETHER

0XAB929FCD

0x195e...2354

0x4183...7227

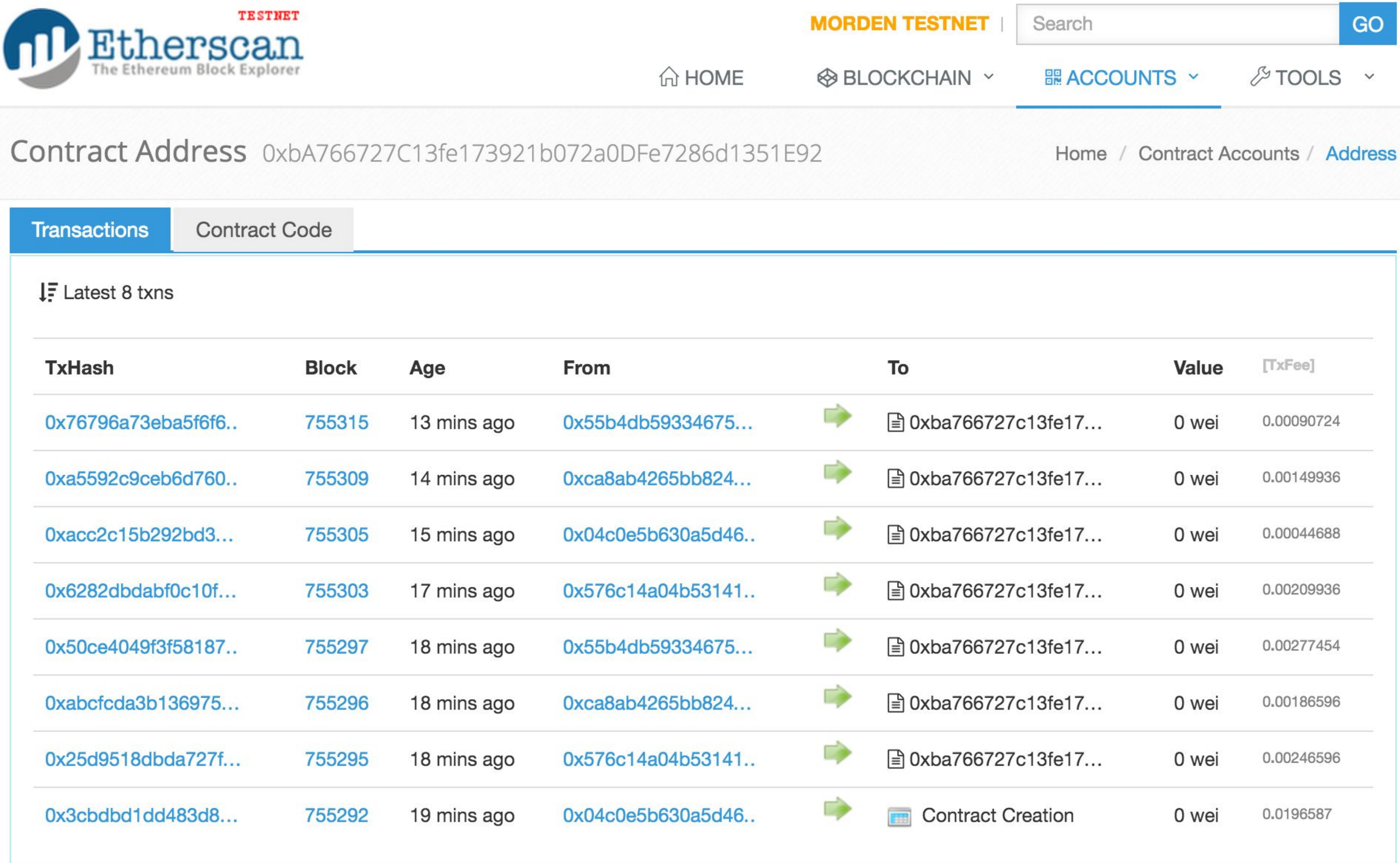
You are about to execute a function on a contract. This might involve transfer of value.

```
0xab929fcd000000000000000000000000000000000000000000000000000
0000000000060000000000000000000000000000000000000000000000000
0000000000000080000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000
```

Estimated fee consumption	0.00209482 ether (93,018 gas)
Provide maximum fee	0.00434688 ether (193,018 gas)
Gas price	0.02252 ether per million gas

Enter password to confirm the transaction

How do you trust the smart contract?



Contract Address 0xbA766727C13fe173921b072a0DFe7286d1351E92

Latest 8 txns

TxHash	Block	Age	From		To	Value	[TxFee]
0x76796a73eba5f6f6..	755315	13 mins ago	0x55b4db59334675...	➡	0xba766727c13fe17...	0 wei	0.00090724
0xa5592c9ceb6d760..	755309	14 mins ago	0xca8ab4265bb824...	➡	0xba766727c13fe17...	0 wei	0.00149936
0xacc2c15b292bd3...	755305	15 mins ago	0x04c0e5b630a5d46..	➡	0xba766727c13fe17...	0 wei	0.00044688
0x6282dbdabf0c10f...	755303	17 mins ago	0x576c14a04b53141..	➡	0xba766727c13fe17...	0 wei	0.00209936
0x50ce4049f3f58187..	755297	18 mins ago	0x55b4db59334675...	➡	0xba766727c13fe17...	0 wei	0.00277454
0xabcfcda3b136975...	755296	18 mins ago	0xca8ab4265bb824...	➡	0xba766727c13fe17...	0 wei	0.00186596
0x25d9518dbda727f...	755295	18 mins ago	0x576c14a04b53141..	➡	0xba766727c13fe17...	0 wei	0.00246596
0x3cbdbd1dd483d8...	755292	19 mins ago	0x04c0e5b630a5d46..	➡	Contract Creation	0 wei	0.0196587

Identity

github.com/maxwedwards/block-journal

@maxwedwards
me@maxedwards.me