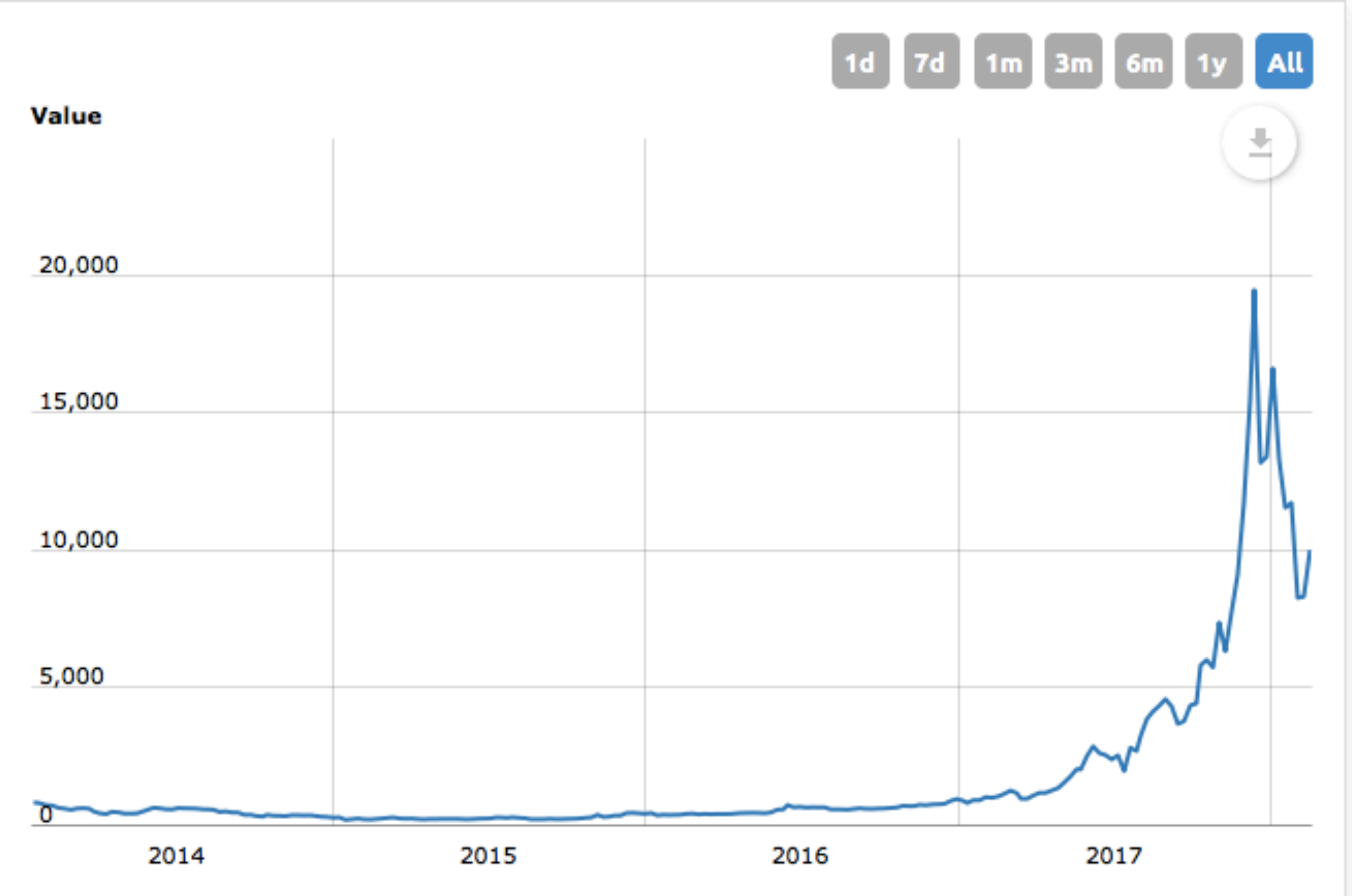
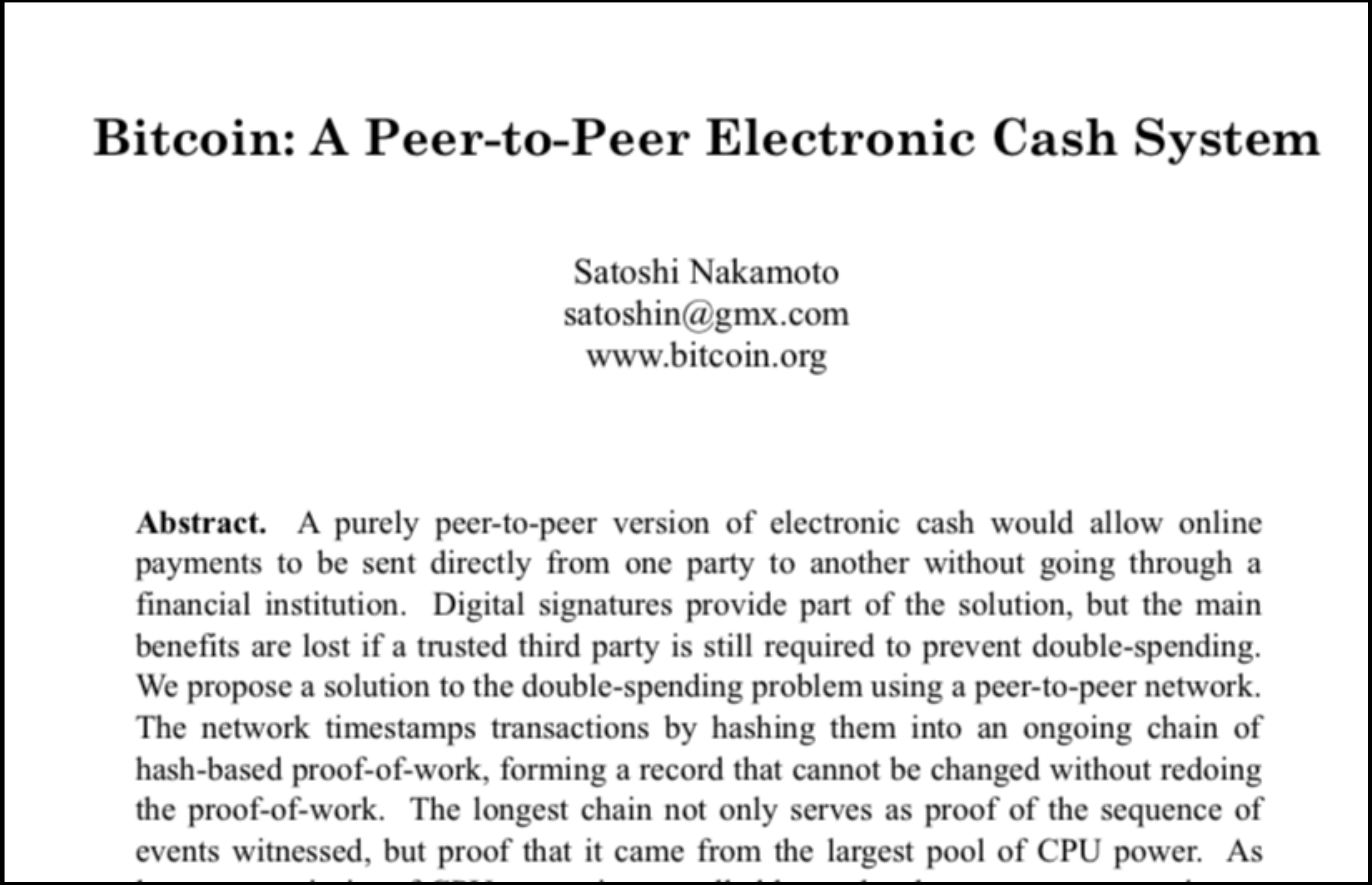
Blockchain Technology


1d
7d
1m
3m
6m
1y
All
Value
20,000
15,000
10,000
5,000
0
2014
2015
2016
2017

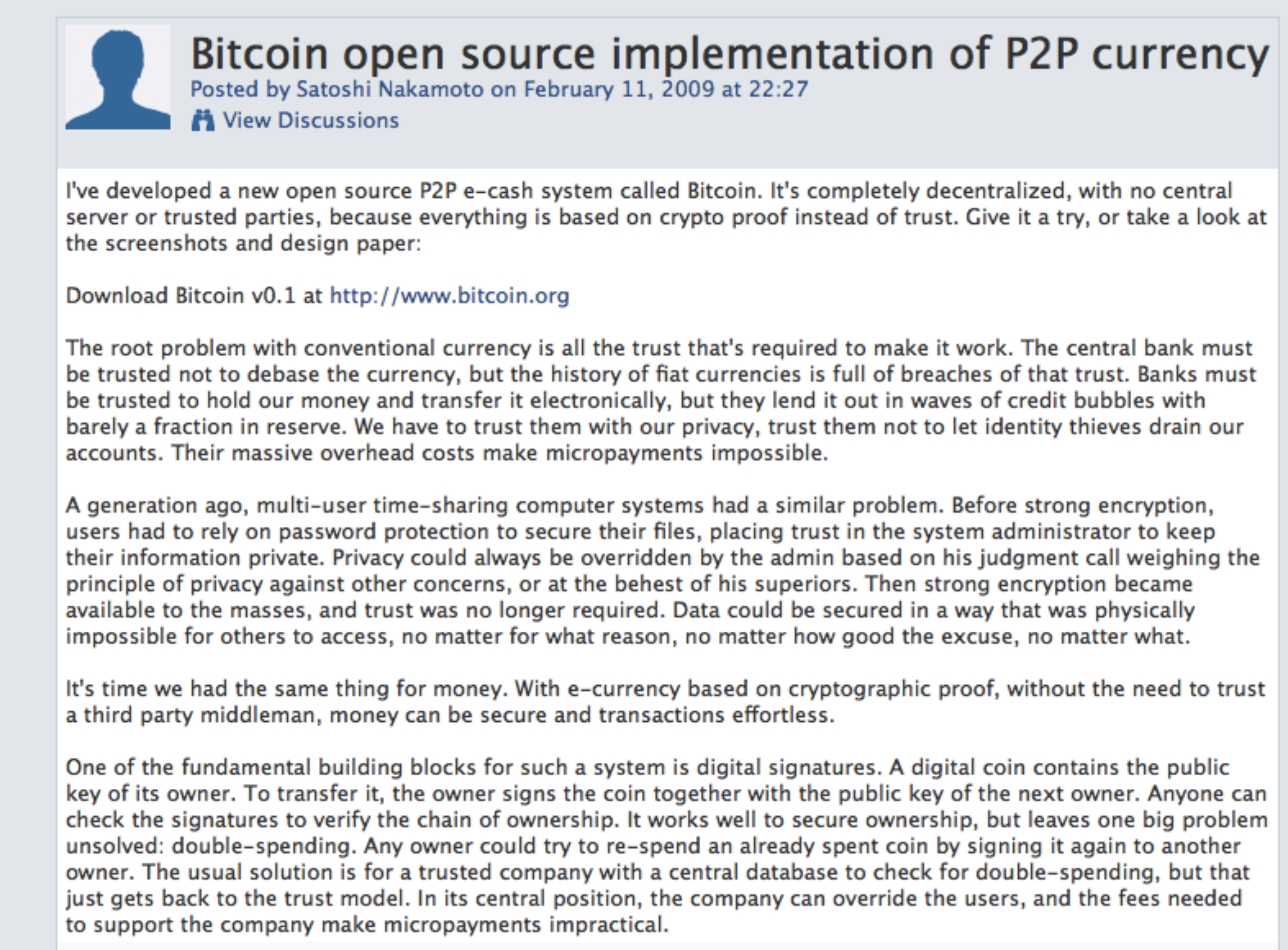


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As

Double-Spending Problem



Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

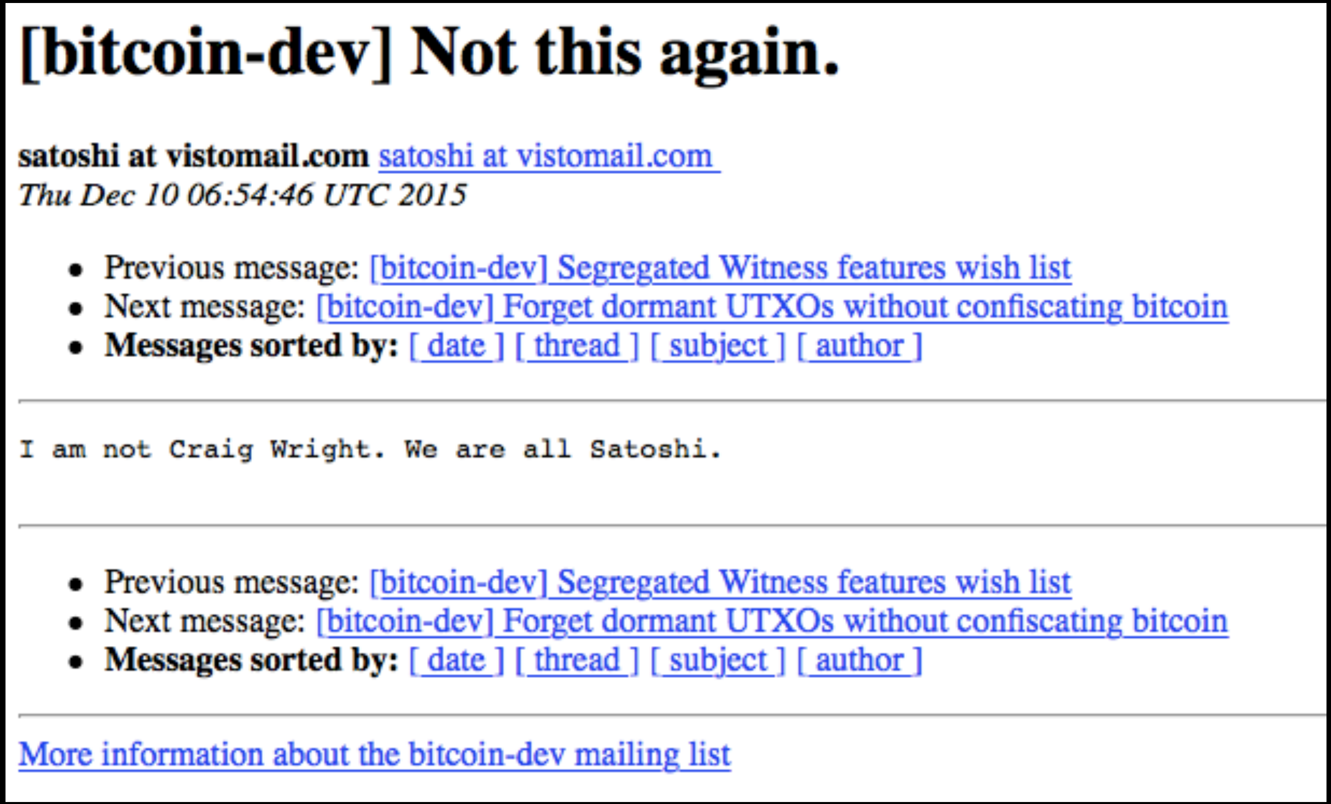
Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.



[bitcoin-dev] Not this again.

satoshi at vistomail.com satoshi at vistomail.com
Thu Dec 10 06:54:46 UTC 2015

- Previous message: [bitcoin-dev] Segregated Witness features wish list
- Next message: [bitcoin-dev] Forget dormant UTXOs without confiscating bitcoin
- **Messages sorted by:** [date] [thread] [subject] [author]

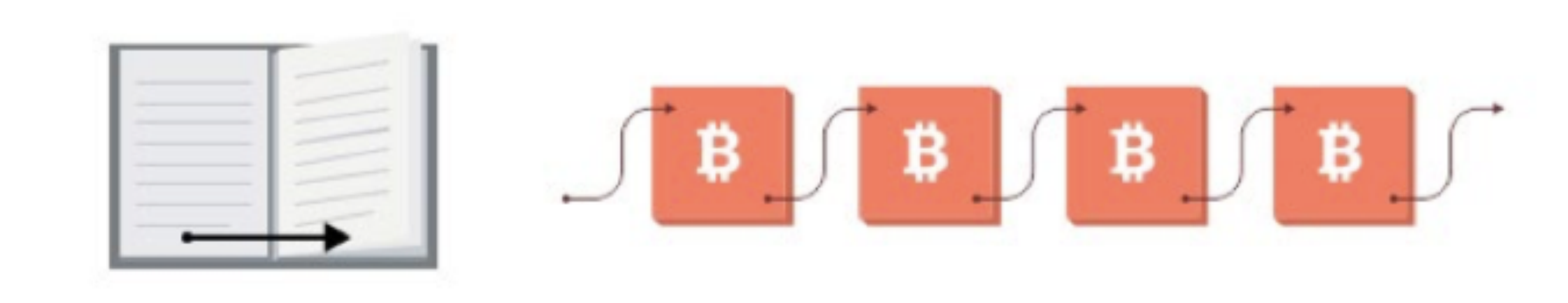
```
I am not Craig Wright. We are all Satoshi.
```

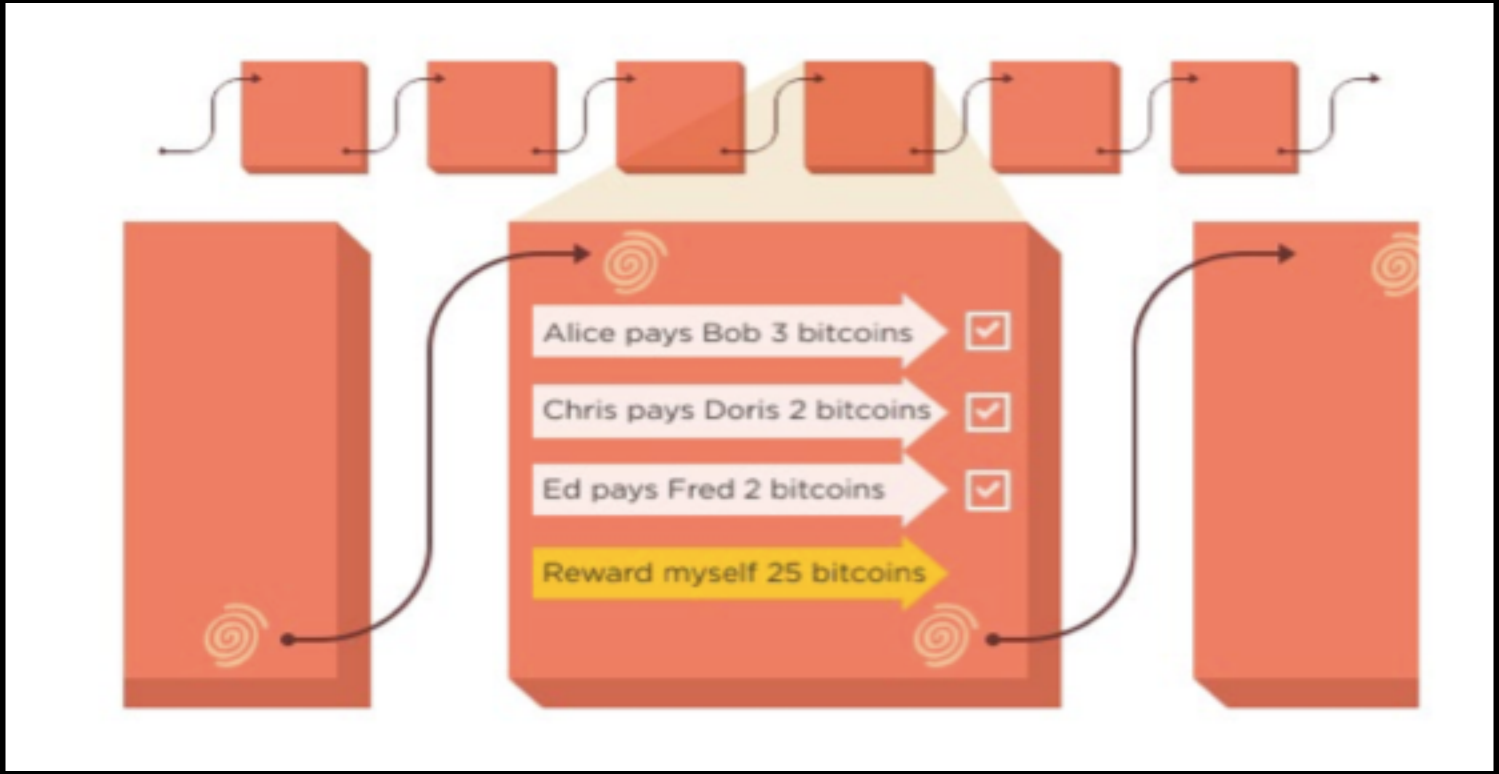
- Previous message: [bitcoin-dev] Segregated Witness features wish list
- Next message: [bitcoin-dev] Forget dormant UTXOs without confiscating bitcoin
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the bitcoin-dev mailing list

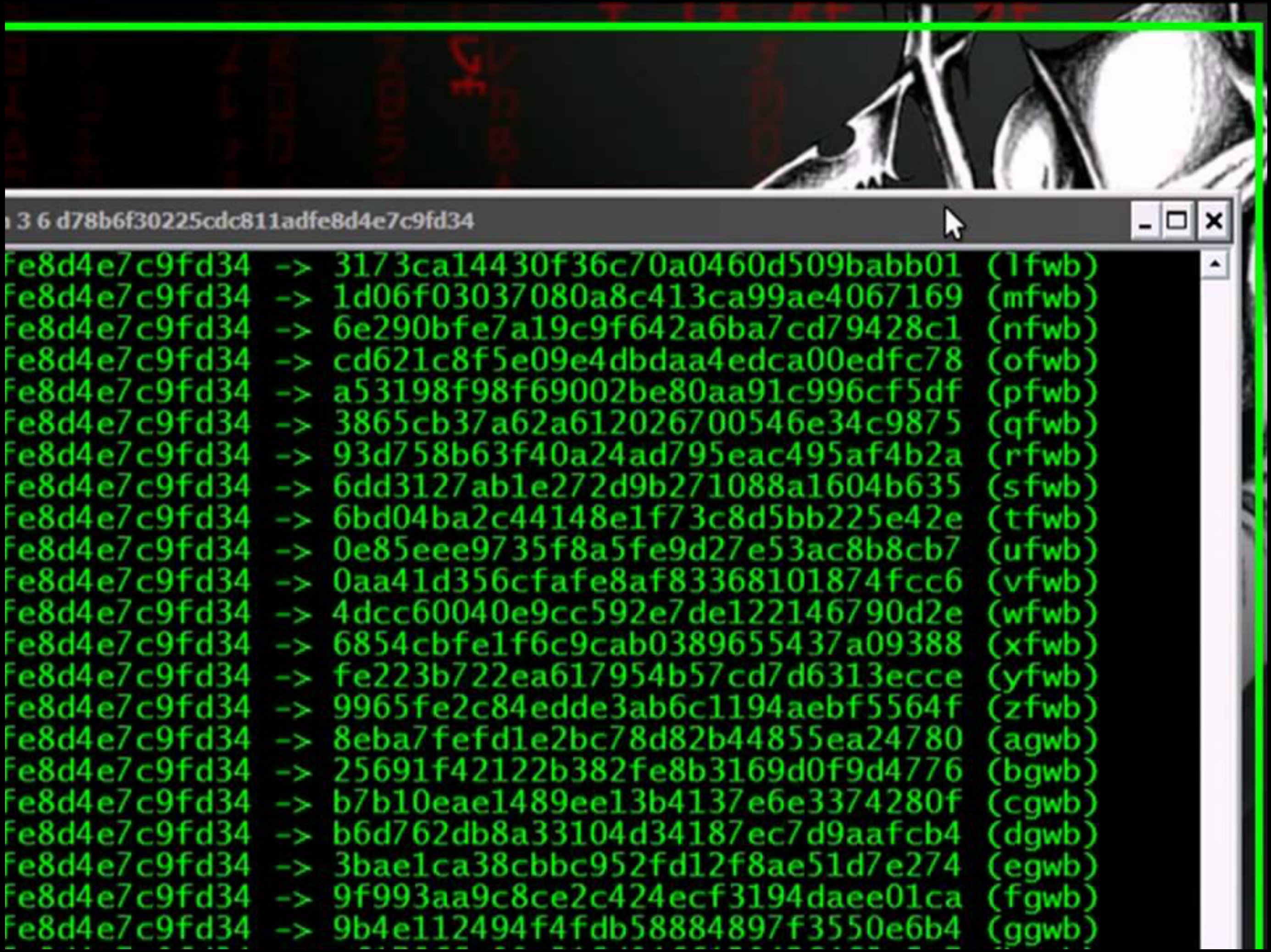
Blockchain vs. Crypto

Decentralization

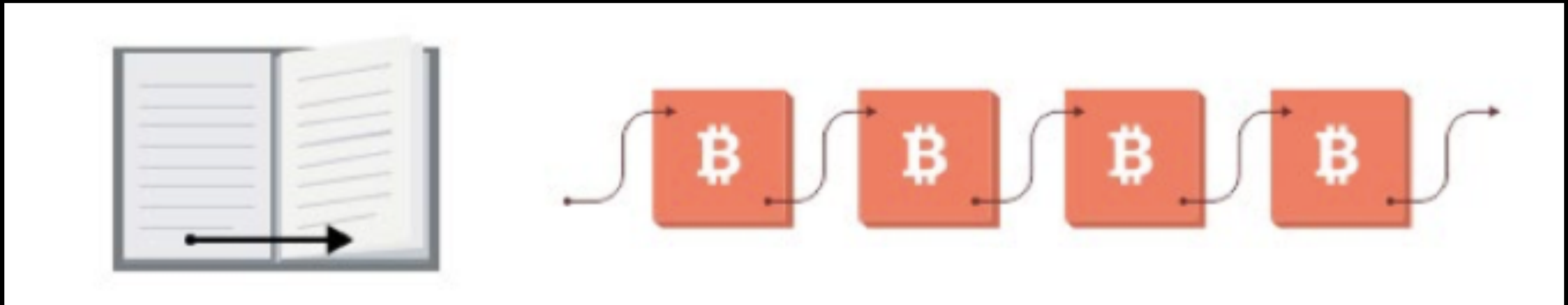


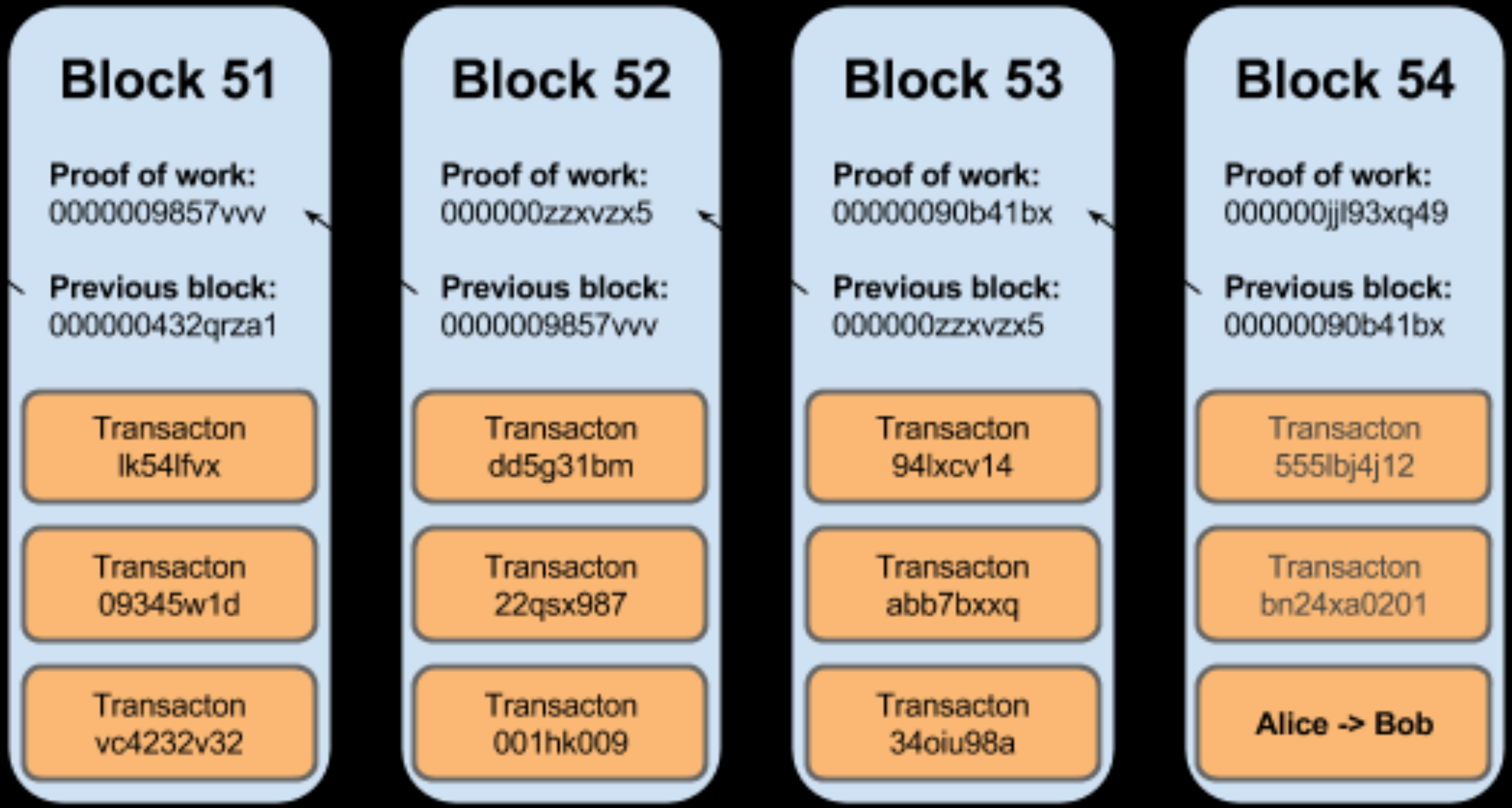


Alice pays Bob 3 bitcoins ☑
Chris pays Doris 2 bitcoins ☑
Ed pays Fred 2 bitcoins ☑
Reward myself 25 bitcoins



```
 3 6 d78b6f30225cdc811adfe8d4e7c9fd34
fe8d4e7c9fd34 -> 3173ca14430f36c70a0460d509babb01 (lfwb)
fe8d4e7c9fd34 -> 1d06f03037080a8c413ca99ae4067169 (mfwb)
fe8d4e7c9fd34 -> 6e290bfe7a19c9f642a6ba7cd79428c1 (nfwb)
fe8d4e7c9fd34 -> cd621c8f5e09e4dbdaa4edca00edfc78 (ofwb)
fe8d4e7c9fd34 -> a53198f98f69002be80aa91c996cf5df (pfwb)
fe8d4e7c9fd34 -> 3865cb37a62a61202670054 6e34c9875 (qfwb)
fe8d4e7c9fd34 -> 93d758b63f40a24ad795eac495af4b2a (rfwb)
fe8d4e7c9fd34 -> 6dd3127ab1e272d9b271088a1604b635 (sfwb)
fe8d4e7c9fd34 -> 6bd04ba2c44148e1f73c8d5bb225e42e (tfwb)
fe8d4e7c9fd34 -> 0e85eee9735f8a5fe9d27e53ac8b8cb7 (ufwb)
fe8d4e7c9fd34 -> 0aa41d356cfafe8af83368101874fcc6 (vfwb)
fe8d4e7c9fd34 -> 4dcc60040e9cc592e7de122146790d2e (wfwb)
fe8d4e7c9fd34 -> 6854cbfe1f6c9cab0389655437a09388 (xfwb)
fe8d4e7c9fd34 -> fe223b722ea617954b57cd7d6313ecce (yfwb)
fe8d4e7c9fd34 -> 9965fe2c84edde3ab6c1194aebf5564f (zfwb)
fe8d4e7c9fd34 -> 8eba7fefd1e2bc78d82b44855ea24780 (agwb)
fe8d4e7c9fd34 -> 25691f42122b382fe8b3169d0f9d4776 (bgwb)
fe8d4e7c9fd34 -> b7b10eae1489ee13b4137e6e3374280f (cgwb)
fe8d4e7c9fd34 -> b6d762db8a33104d34187ec7d9aafcb4 (dgwb)
fe8d4e7c9fd34 -> 3bae1ca38cbbc952fd12f8ae51d7e274 (egwb)
fe8d4e7c9fd34 -> 9f993aa9c8ce2c424ecf3194daee01ca (fgwb)
fe8d4e7c9fd34 -> 9b4e112494f4fdb58884897f3550e6b4 (ggwb)
```





Block 51

Proof of work:
0000009857vvv

Previous block:
000000432qrza1

Transacton
lk54lfvx

Transacton
09345w1d

Transacton
vc4232v32

Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transacton
dd5g31bm

Transacton
22qsx987

Transacton
001hk009

Block 53

Proof of work:
00000090b41bx

Previous block:
000000zzxvzx5

Transacton
94lxcv14

Transacton
abb7bxxq

Transacton
34oiu98a

Block 54

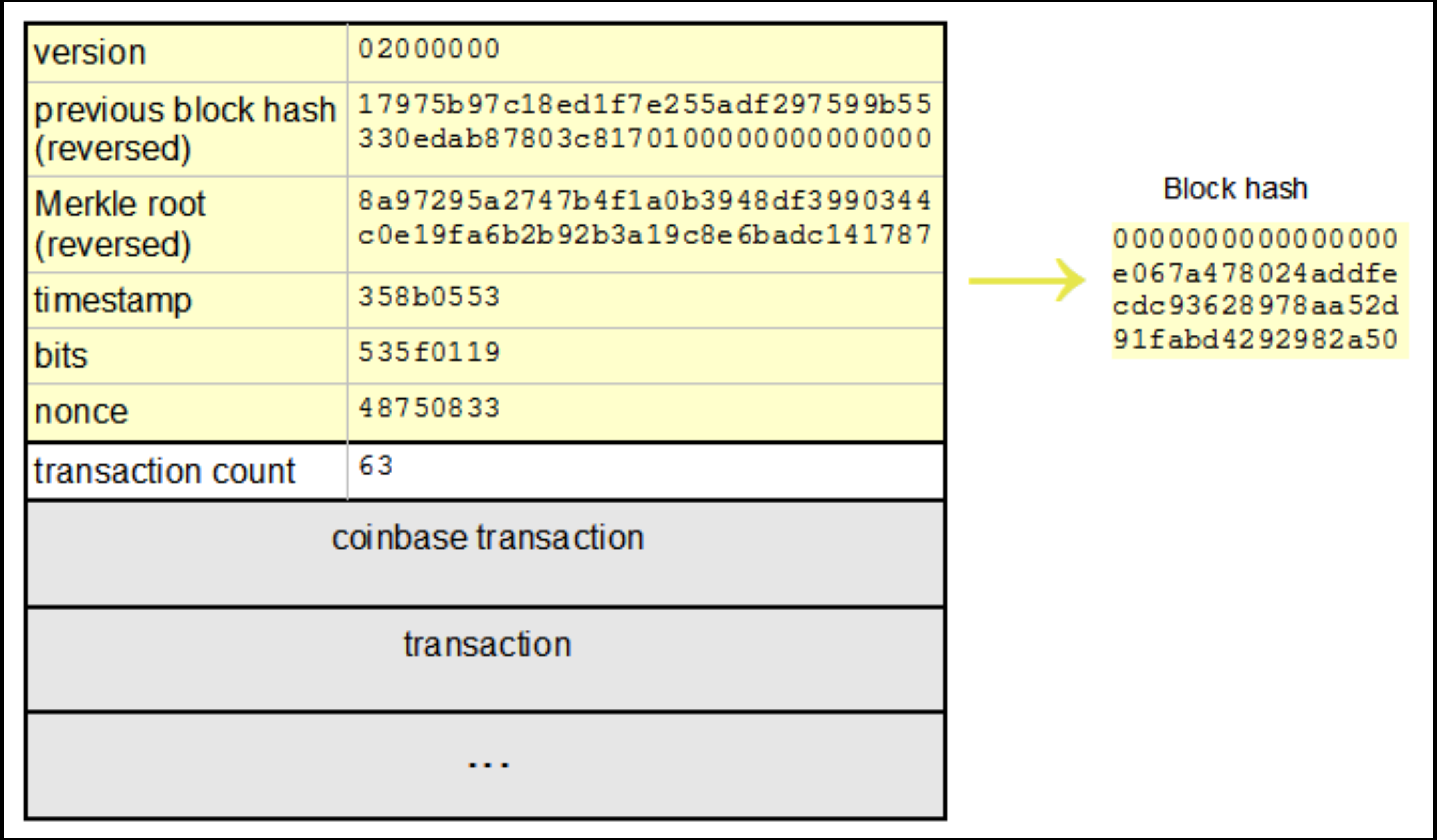
Proof of work:
000000jjl93xq49

Previous block:
00000090b41bx

Transacton
555lbj4j12

Transacton
bn24xa0201

Alice -> Bob



version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63

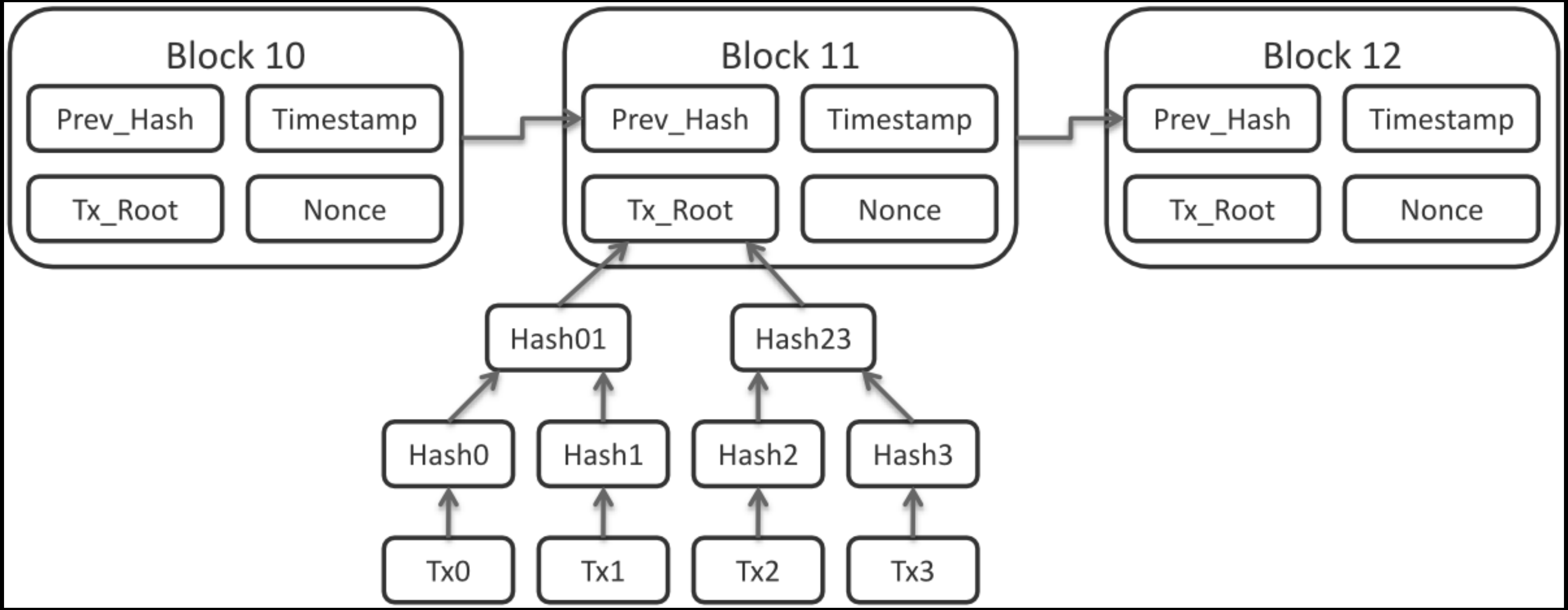
coinbase transaction

transaction

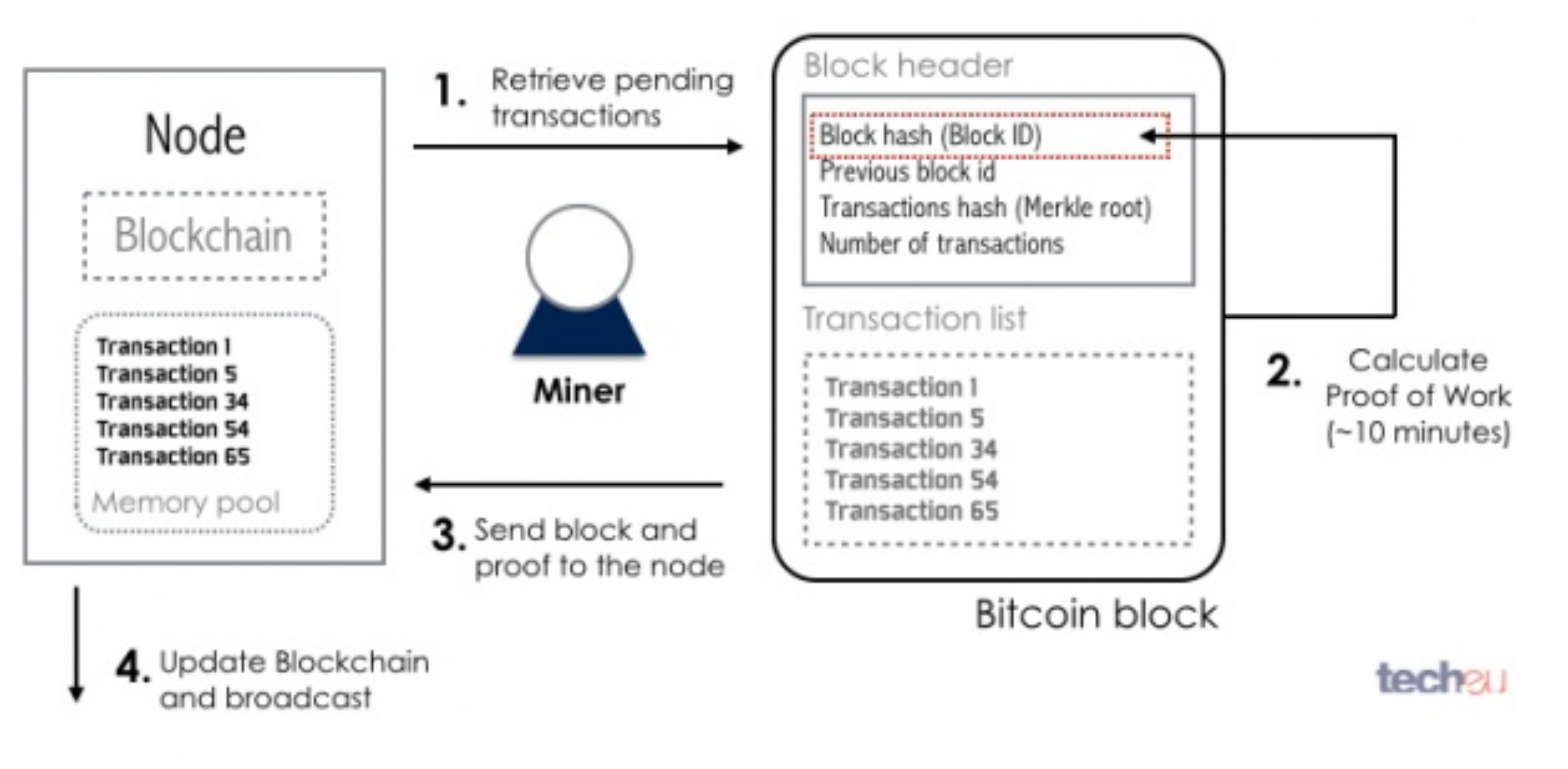
...

Block hash

0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50

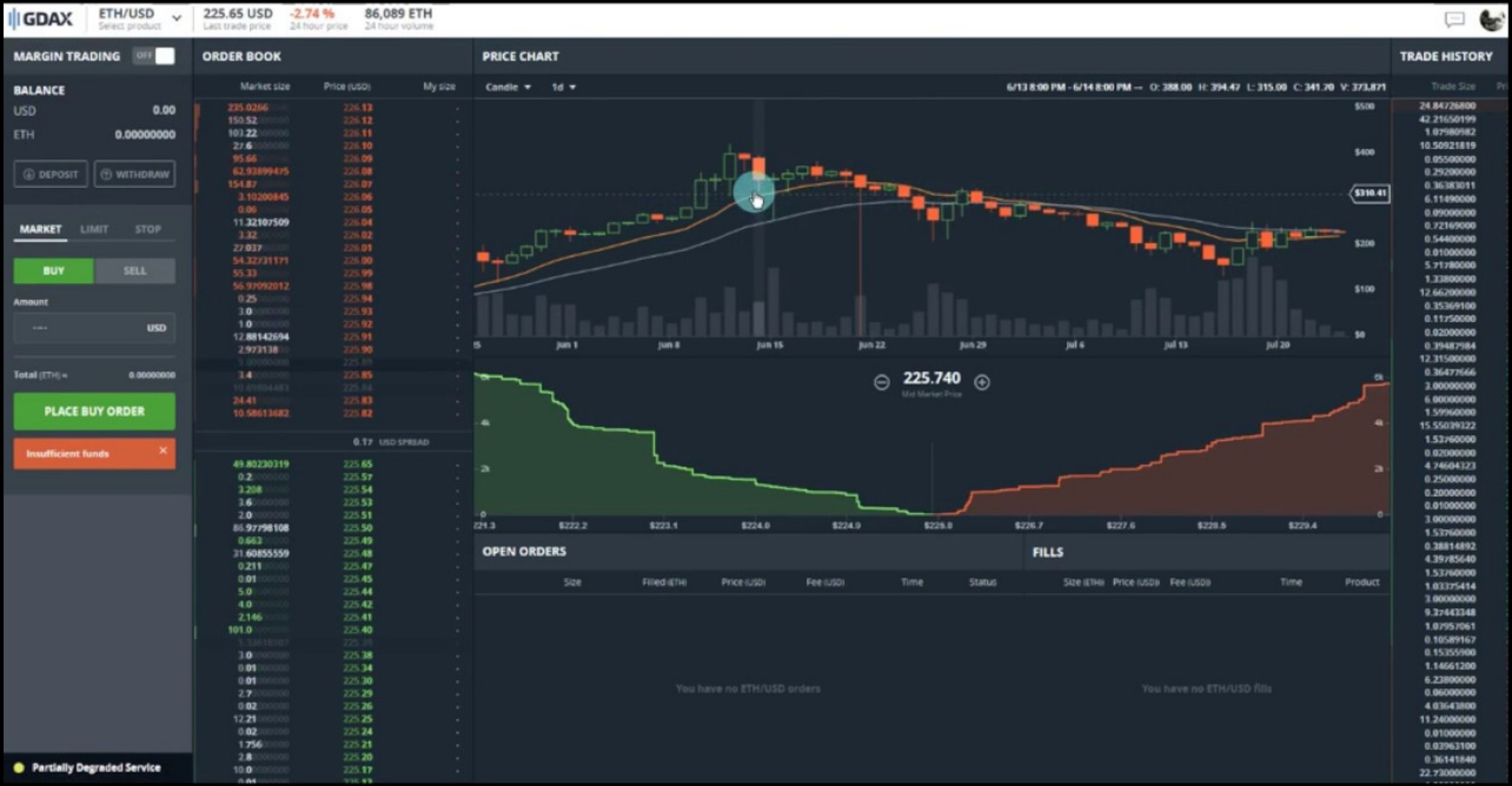

Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Nonce


Node
Blockchain
Transaction 1
Transaction 5
Transaction 34
Transaction 54
Transaction 65
Memory pool
1. Retrieve pending transactions
Miner
3. Send block and proof to the node
4. Update Blockchain and broadcast
Block header
Block hash (Block ID)
Previous block id
Transactions hash (Merkle root)
Number of transactions
Transaction list
Transaction 1
Transaction 5
Transaction 34
Transaction 54
Transaction 65
Bitcoin block
2. Calculate Proof of Work (~10 minutes)
tech.eu

Demonstration

coinbase



BALANCE

USD 0.00

ETH 0.00000000

Amount

USD

Total (ETH) ≈ 0.00000000

Insufficient funds ×

6/13 8:00 PM - 6/14 8:00 PM → O: 388.00 H: 394.47 L: 315.00 C: 341.70 V: 373,871

ORDER BOOK

Market size	Price (USD)	My size
235.0266	226.13	-
150.52	226.12	-
103.22	226.11	-
27.6	226.10	-
95.66	226.09	-
62.93899475	226.08	-
154.87	226.07	-
3.10200845	226.06	-
0.06	226.05	-
11.32107509	226.04	-
3.32	226.02	-
27.037	226.01	-
54.32731171	226.00	-
55.33	225.99	-
56.97092012	225.98	-
0.25	225.94	-
3.0	225.93	-
1.0	225.92	-
12.88142694	225.91	-
2.973138	225.90	-
5.00000000	225.89	-
3.4	225.85	-
10.69804483	225.84	-
24.41	225.83	-
10.58613682	225.82	-
0.17 USD SPREAD		
49.80230319	225.65	-
0.2	225.57	-
3.208	225.54	-
3.6	225.53	-
2.0	225.51	-
86.97798108	225.50	-
0.663	225.49	-
31.60855559	225.48	-
0.211	225.47	-
0.01	225.45	-
5.0	225.44	-
4.0	225.42	-
2.146	225.41	-
101.0	225.40	-
5.33618107	225.39	-
3.0	225.38	-
0.01	225.34	-
0.01	225.30	-
2.7	225.29	-
0.02	225.26	-
12.21	225.25	-
0.02	225.24	-
1.756	225.21	-
2.8	225.20	-
10.0	225.17	-
0.01	225.12	

TRADE HISTORY

Trade Size	Pr
24.84726800	
42.21650199	
1.07980982	
10.50921819	
0.05500000	
0.29200000	
0.36383011	
6.11490000	
0.09000000	
0.72169000	
0.54400000	
0.01000000	
5.71780000	
1.33800000	
12.66200000	
0.35369100	
0.11750000	
0.02000000	
0.39487984	
12.31500000	
0.36477666	
3.00000000	
6.00000000	
1.59960000	
15.55039322	
1.53760000	
0.02000000	
4.74604323	
0.25000000	
0.20000000	
0.01000000	
3.00000000	
1.53760000	
0.38814892	
4.39785640	
1.53760000	
1.03375414	
3.00000000	
9.37443348	
1.07957061	
0.10589167	
0.15355900	
1.14661200	
6.23800000	
0.06000000	
4.03643800	
11.24000000	
0.01000000	
0.03963100	
0.36141840	
22.73000000	

OPEN ORDERS

Size	Filled (ETH)	Price (USD)	Fee (USD)	Time	Status

You have no ETH/USD orders

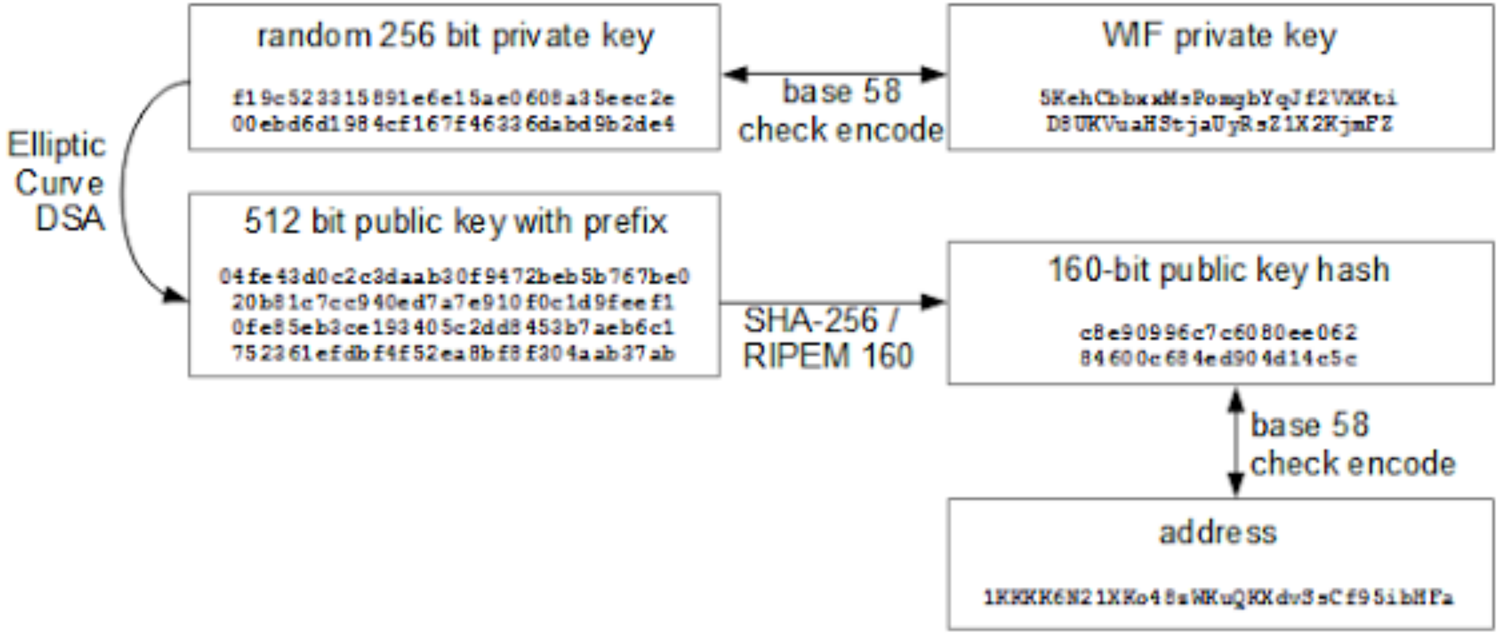
FILLS

Size (ETH)	Price (USD)	Fee (USD)	Time	Product

You have no ETH/USD fills

Addresses

Bitcoin Keys



random 256 bit private key

f19c523315891e6e15ae0608a35eec2e
00ebd6d1984cf167f46336dabd9b2de4

base 58
check encode

WIF private key

5KehCbbxxMsPomgbYqJf2VXKti
D8UKVuaHStjaUyRsZ1X2KjmFZ

Elliptic
Curve
DSA

512 bit public key with prefix

04fe43d0c2c3daab30f9472beb5b767be0
20b81c7cc940ed7a7e910f0c1d9feef1
0fe85eb3ce193405c2dd8453b7aeb6c1
752361efdbf4f52ea8bf8f304aab37ab

SHA-256 /
RIPEM 160

160-bit public key hash

c8e90996c7c6080ee062
84600c684ed904d14c5c

base 58
check encode

address

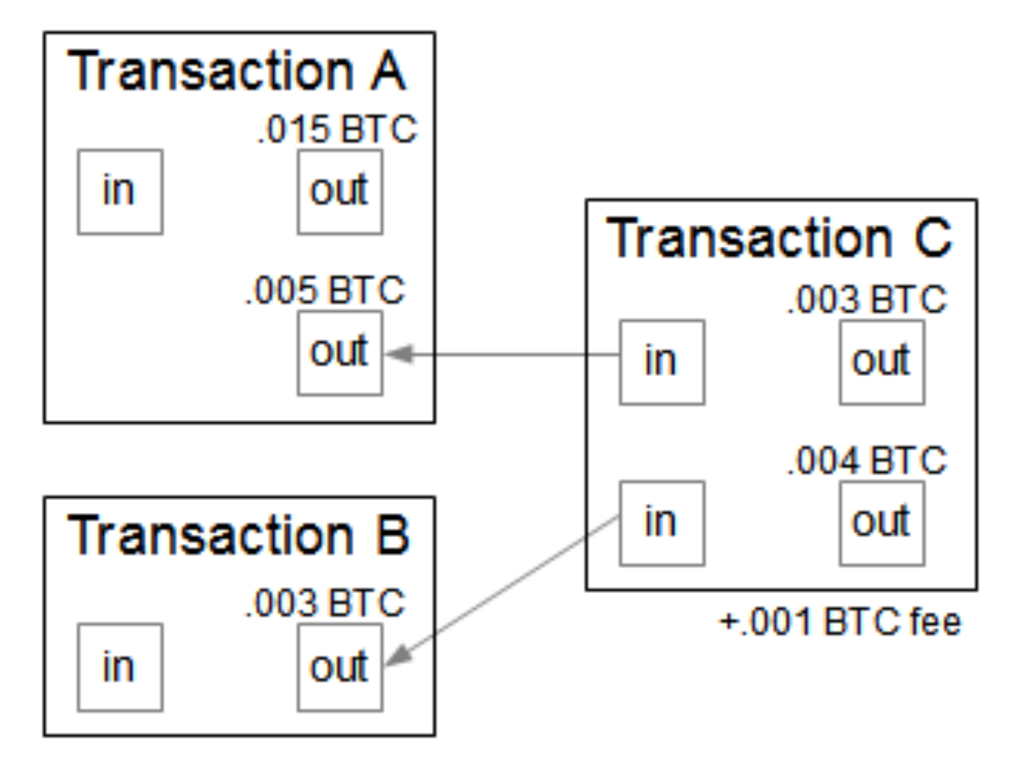
1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

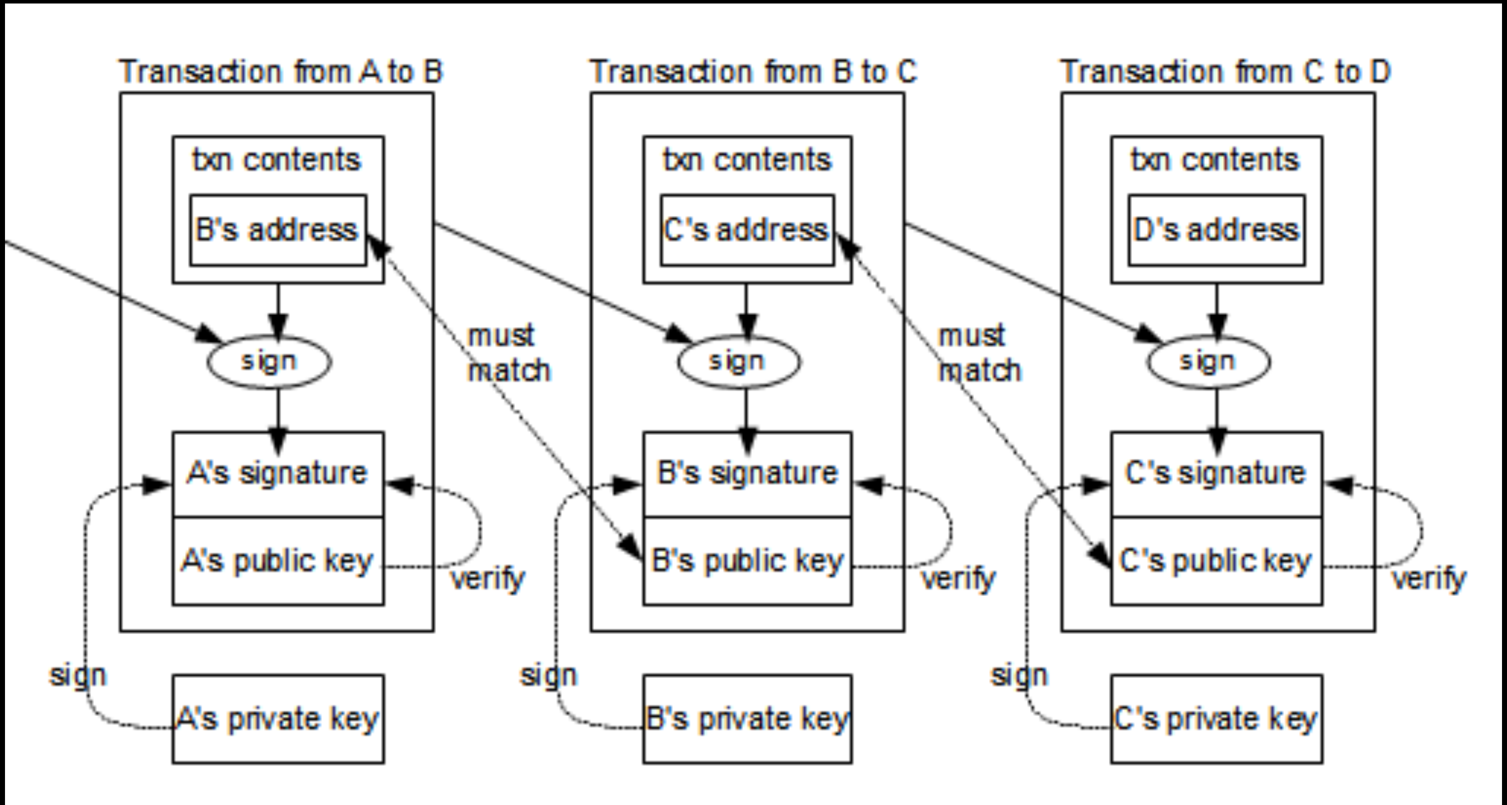
1Bv8dN7pemC5N3urfMDdAFReibefrBqCaK

e9873d79c6d87dc0fb6a5778633389f4453213303da61f20bd67fc233aa33262

2^{256}

directory.io

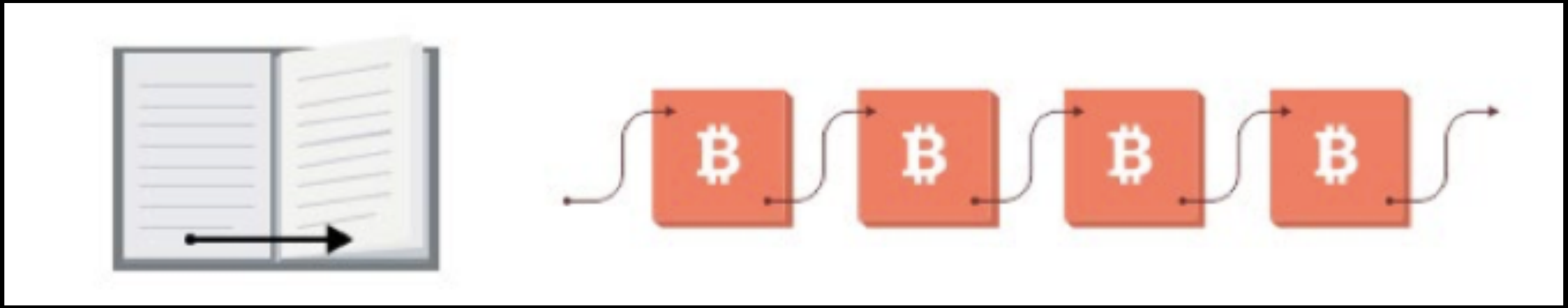

Transaction A
.015 BTC
in
out
.005 BTC
out
Transaction C
.003 BTC
in
out
.004 BTC
in
out
+.001 BTC fee
Transaction B
.003 BTC
in
out

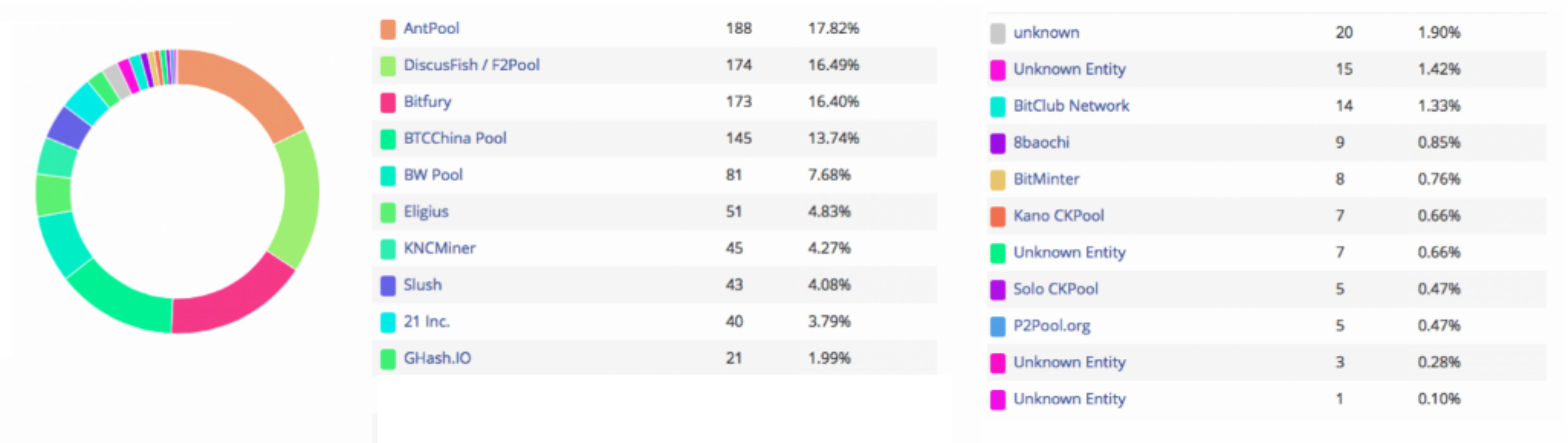

Transaction from A to B
Transaction from B to C
Transaction from C to D
txn contents
B's address
txn contents
C's address
txn contents
D's address
sign
sign
sign
must match
must match
A's signature
A's public key
B's signature
B's public key
C's signature
C's public key
verify
verify
verify
sign
sign
sign
A's private key
B's private key
C's private key

Security

51% attack

Mining: Proof of Work





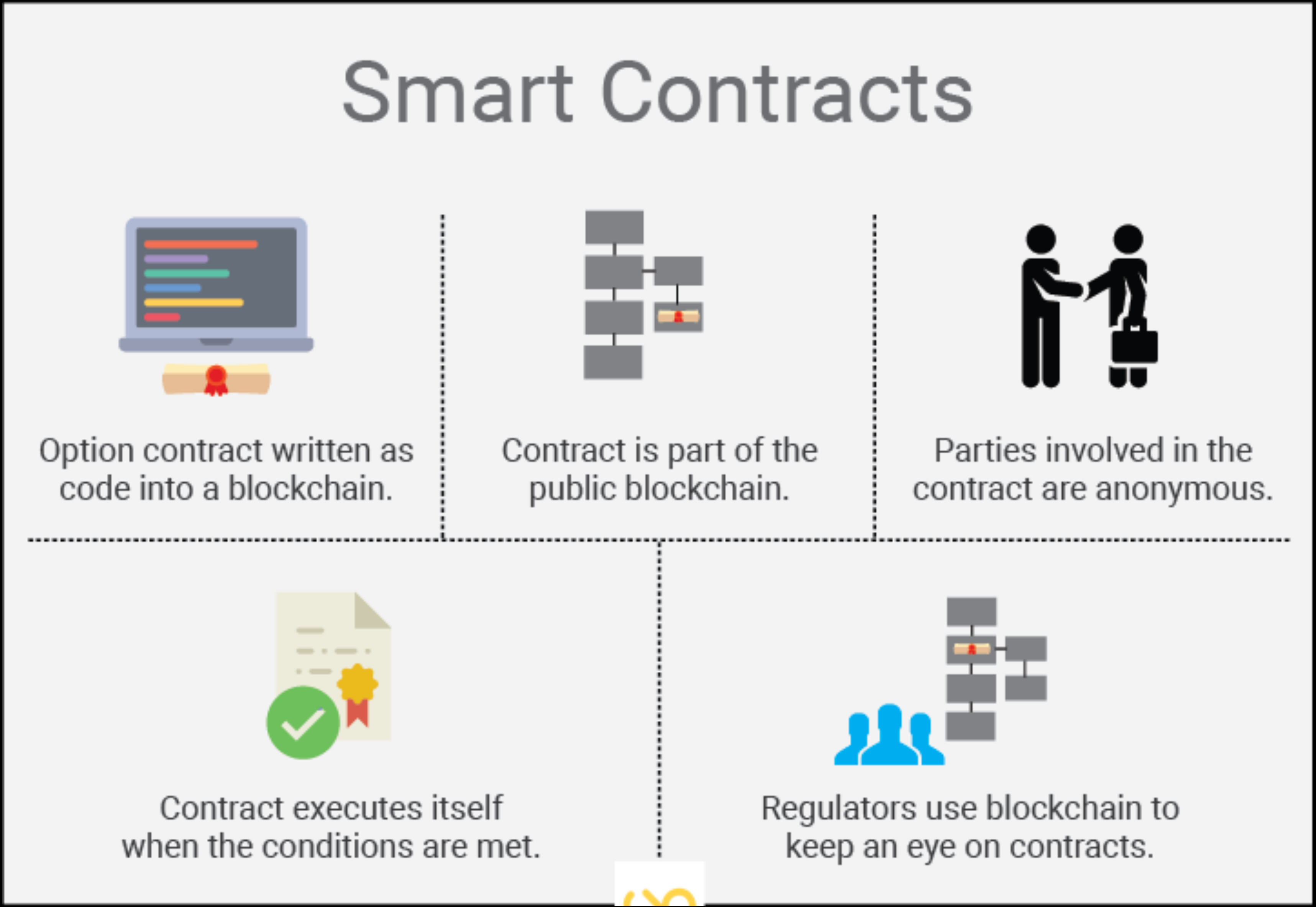
🟧	AntPool	188	17.82%
🟩	DiscusFish / F2Pool	174	16.49%
🟥	Bitfury	173	16.40%
🟩	BTCChina Pool	145	13.74%
🟦	BW Pool	81	7.68%
🟩	Eligius	51	4.83%
🟩	KNCMiner	45	4.27%
🟪	Slush	43	4.08%
🟦	21 Inc.	40	3.79%
🟩	GHash.IO	21	1.99%
⬜	unknown	20	1.90%
🟪	Unknown Entity	15	1.42%
🟦	BitClub Network	14	1.33%
🟪	8baochi	9	0.85%
🟨	BitMinter	8	0.76%
🟧	Kano CKPool	7	0.66%
🟩	Unknown Entity	7	0.66%
🟪	Solo CKPool	5	0.47%
🟦	P2Pool.org	5	0.47%
🟪	Unknown Entity	3	0.28%
🟪	Unknown Entity	1	0.10%

MT.GOX

ETHEREUM

CONTRACT

Smart Contracts



Smart Contracts

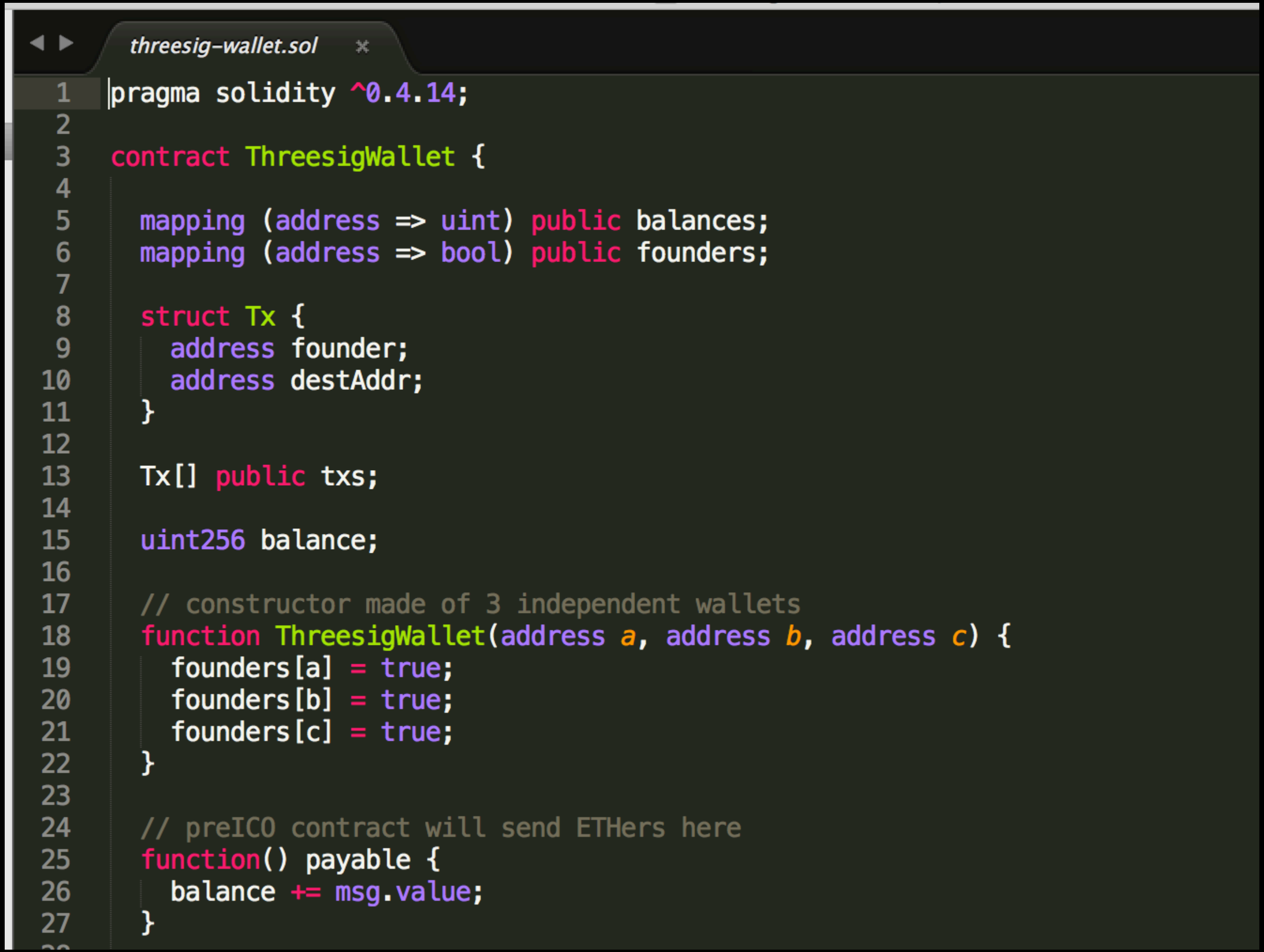
Option contract written as code into a blockchain.

Contract is part of the public blockchain.

Parties involved in the contract are anonymous.

Contract executes itself when the conditions are met.

Regulators use blockchain to keep an eye on contracts.



```
pragma solidity ^0.4.14;

contract ThreesigWallet {

  mapping (address => uint) public balances;
  mapping (address => bool) public founders;

  struct Tx {
    address founder;
    address destAddr;
  }

  Tx[] public txs;

  uint256 balance;

  // constructor made of 3 independent wallets
  function ThreesigWallet(address a, address b, address c) {
    founders[a] = true;
    founders[b] = true;
    founders[c] = true;
  }

  // preICO contract will send ETHers here
  function() payable {
    balance += msg.value;
  }
```

Decentralized Applications (DApps)

EtherTweet

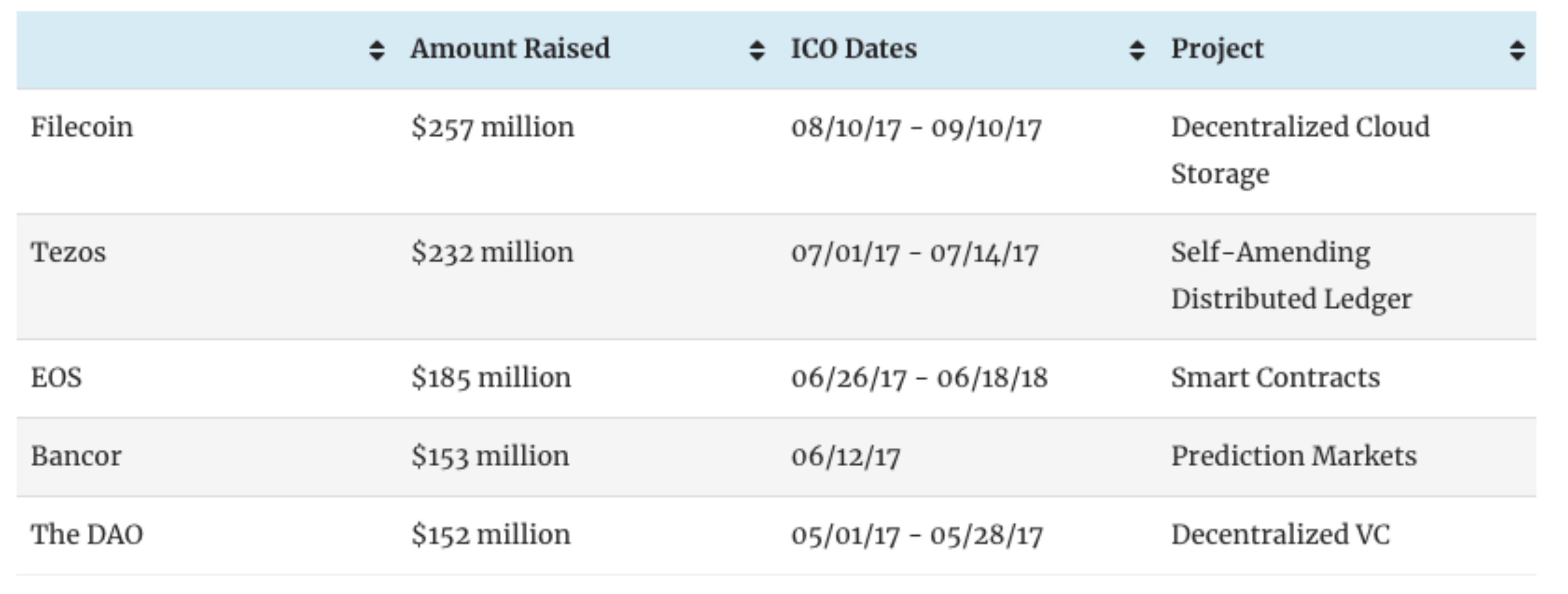
Microblogging on the Ethereum Blockchain

GNOSIS

Tokens: Usage Token vs. Work Token

ICO

Initial Coin Offering



	Amount Raised	ICO Dates	Project
Filecoin	$257 million	08/10/17 - 09/10/17	Decentralized Cloud Storage
Tezos	$232 million	07/01/17 - 07/14/17	Self-Amending Distributed Ledger
EOS	$185 million	06/26/17 - 06/18/18	Smart Contracts
Bancor	$153 million	06/12/17	Prediction Markets
The DAO	$152 million	05/01/17 - 05/28/17	Decentralized VC

Private Blockchains

Restrict Mining and/or Access

ImmunoTracker

Amazon: Supply Chain, Proof-of-Provenance

Electronic Voting

How to get started?

Explore the Technology

MultiChain

Private Blockchain Platform

Coin Sciences Ltd
www.multichain.com