Alternative Mining, Bitcoin Applications, and Altcoins

50.037 Blockchain Technology

Paweł Szałachowski

Alternative Mining

PoW in Bitcoin

- Reminder: PoW is needed to protect from Sybil attacks
    - In permissionless system such a protection has to be resource-based
- Based on H()
- Energy consuming
- Useless
- Easy to optimize (ASIC)
- Can we introduce mining with some better properties?
    - Bitcoin is hard to change but other systems could benefit

Requirements

- Quick to verify: every full node validates solutions
- Adjustable difficulty: {in,de}creasing network capabilities
- Fair: finding solutions should be proportional to resources invested
    - Progress free: finding solutions should be independent (probability)
    - Memoryless process: finding time forms exponential distribution
- SHA256(SHA256(.)) < TARGET satisfies them

ASIC-Resistant Mining

- Why ASIC-resistant mining?
    - Ideally, we would mine with CPUs (ASIC makes it worthless)
    - Mining is getting professional and concentrated
        - High entry barrier
    - Energy consumption
    - (There are also arguments against: it is proven/secure, it is always possible to specialize hardware, …)
- Design mining such that ASICs are unprofitable
    - Such that general-purpose computers can compete
        - (1 computer/CPU: 1 vote)

Memory-Hard Mining

- Memory-hard mining
    - Instead of a lot CPU time, require a large amount of memory
- Memory-bound mining
    - (another concept) where memory access time is important
- Combination of memory-hard and memory-bound mining
- More challenging to build ASICs that need to compute something + access memory
    - SHA256 is not memory hard

scrypt

- ASIC-resistance hash functions is not a new problem
  - Password hashing and cracking resistance

```
def scrypt(N, seed):
    V = [0] * N  // initialize memory buffer of length N

  // Fill up memory buffer with pseudorandom data
  V[0] = seed
  for i = 1 to N:
     V[i] = SHA-256(V[i-1])

  // Access memory buffer in a pseudorandom order
  X = SHA-256(V[N-1])
  for i = 1 to N:
     j = X % N  // Choose a random index based on X
     X = SHA-256(X ^ V[j]) // Update X based on this index

  return X
```

scrypt

- scrypt with memory is O(N), without $O(N^2)$
- Some time-memory trade-offs still possible
- Verification cost
    - For large N (should be large), the verification requires significant memory
        - SPV clients may be too resource constraint
- With low N, ASICs can be built
- Used in practice
    - Other cryptocurrencies
- Other approaches (different than scrypt): Cuckoo Cycle, X11, …

Proof of Useful Work

- Natural Goal: get something useful from mining computations
- Still should meet the requirements
    - Quick verification, Adjustable, and Fair
- Previous distributed computing projects
    - Difficult to employ as cryptocurrency mining

Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new “largest prime number” twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants
Folding@home	2000	Atomic-level simulations of protein folding	Greatest computing capacity of any volunteer computing project. More than 118 scientific papers.

Primecoin

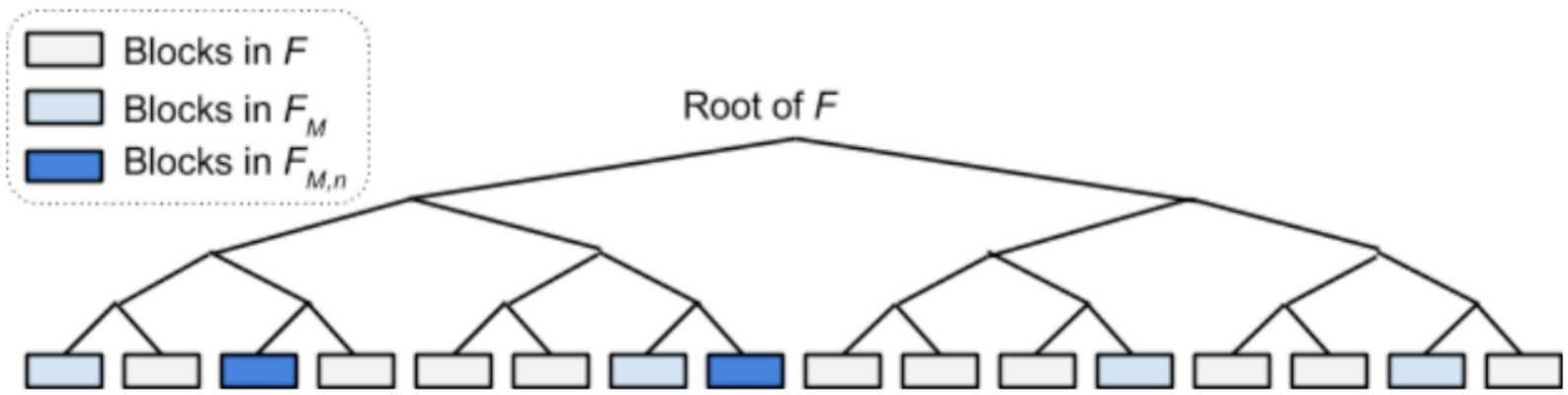
- Cunningham chains
  - $p_1,p_2,\ldots,p_k$ such that $p_i = 2p_{i-1}+1$
  - The longest known chain has 19 primes, conjectured (not proven) that there is a chain for any k
- Mining requires three parameters m,n,k
  - For the previous block hash x, take m bits of x and consider any k-long chain in which the first prime in the chain is an n-bit prime and has the same m leading bits as x
  - Increasing n increases difficulty linearly, increasing k increases difficulty exponentially, m should be large enough such that precomputing values is infeasible
- Deployed in Primecoin (the longest Cunningham chain found)
- Is that really useful?

Permacoin and Proof Of Storage

- Instead of computing extensively, prove that you are storing some dataset
  - If the dataset is useful then miners' equipment is useful
- F is a large file that everyone agrees it is worth archiving
  - Libraries, experimental data, web archive, …
  - Miners could collectively archive it by storing its portions
- Not everyone has to store it, but everyone has to make sure that some data belongs to F

Permacoin and Proof Of Storage

- Each miner stores a random subset F_M of F
  - A miner from hash of its public key K_M generates a k_1-long list of blocks F_M (note that this list is pseudorandom), download, and store them
- With the previous block hash x, the miner chooses nonce and hashes it to generate a k_2-long ($k_2<k_1$) subset $F_{M,n}$ of F_M
- If $H(F_{M,n} \| n) < TARGET$, then this is a valid solution and can be propagated
  - Presence proofs for blocks are propagated too
- Verify: a) $F_{M,n}$ is correctly derived from K_M and nonce, b) each block of $F_{M,n}$ is part of F, c) $H(F_{M,n} \| n) < TARGET$



Mining Misc.

- Proof-of-X (mainly, resource-based)
- Many ideas around
  - Proof of Luck, Proof of Elapsed Time, Proof of DoS, …
- Proof of Stake (will discuss later)
  - Why to *vote* with resources and not just stakes?
- Nonoutsourceable mining

Bitcoin Applications

Cryptocurrency

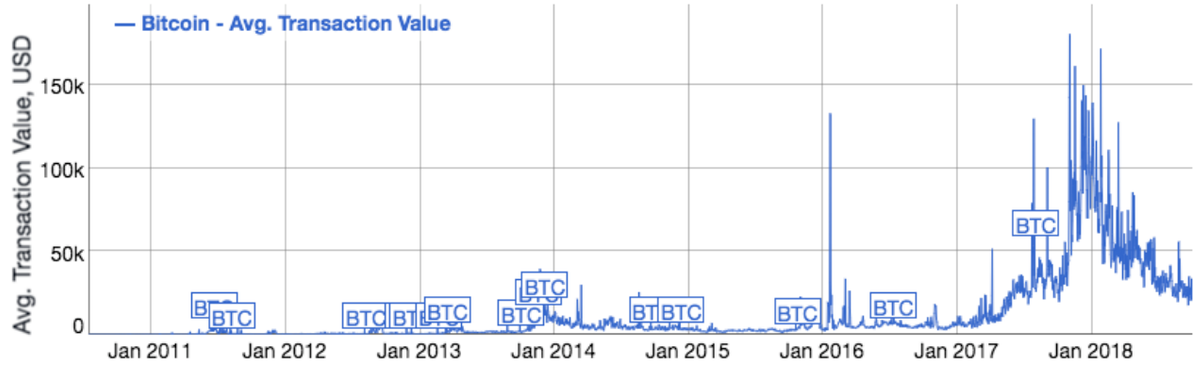
- Monetary (token) transfers
  - Electronic cash?
  - Electronic gold?
  - Settlement system?

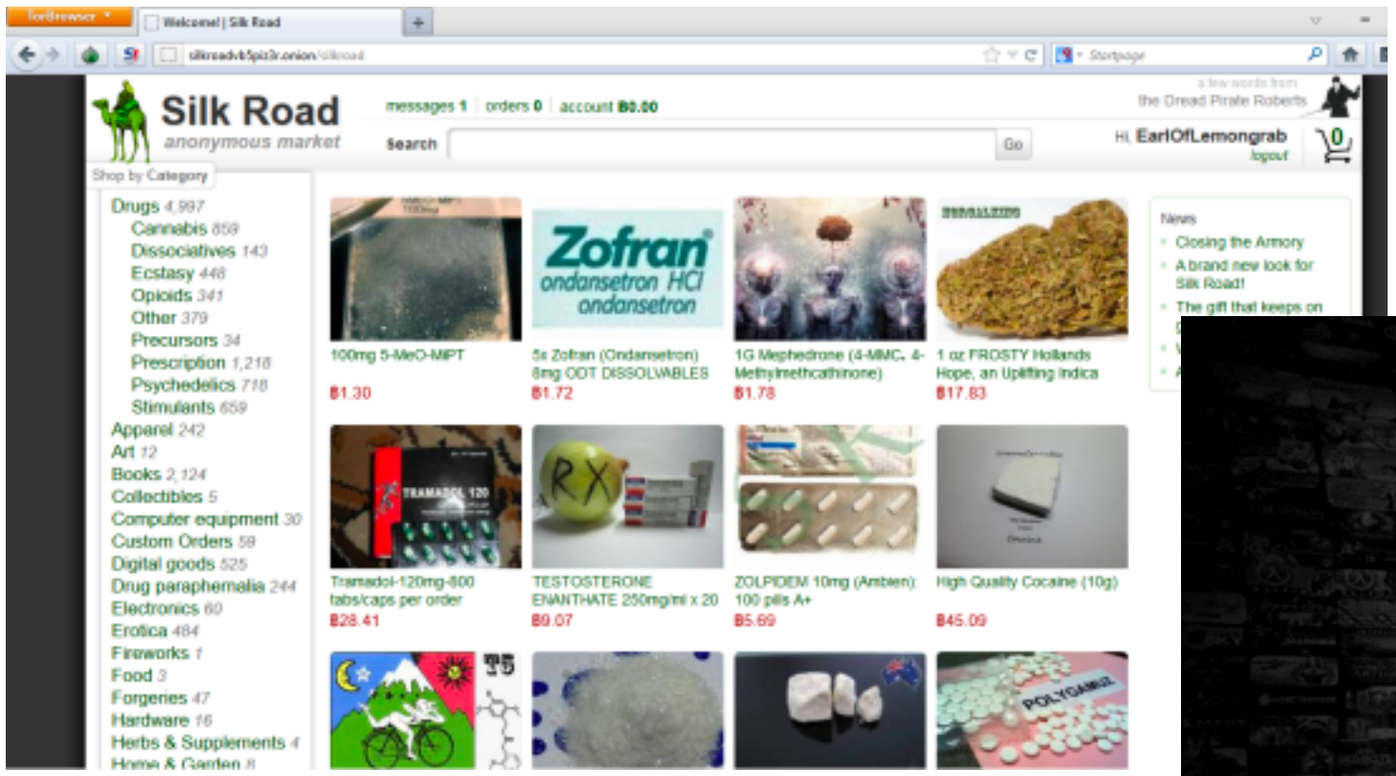
(Fee: 0.0001 BTC - 11.11 sat/WU - 44.44 sat/B - Size: 225 bytes) 2018-03-02 06:32:54

17q2VQxBeisajEZfpcy1EdMtcpPay737MN - (Unspent)	200 BTC
1MiQrT5sEKTUGNMbd9WS3yPPkSjWdpYA2r - (Spent)	6,799.9999 BTC

6,999.9999 BTC

	Value of transaction per card in U.S. dollars
American Express	141
MasterCard	80
Visa	81
JCB	73




Silk Road
anonymous market
messages 1 | orders 0 | account ฿0.00
Search
Go
Hi, EarlOfLemongrab
logout
Shop by Category
Drugs 4,997
Cannabis 859
Dissociatives 143
Ecstasy 448
Opioids 341
Other 379
Precursors 34
Prescription 1,218
Psychedelics 718
Stimulants 659
Apparel 242
Art 12
Books 2,124
Collectibles 5
Computer equipment 30
Custom Orders 59
Digital goods 525
Drug paraphernalia 244
Electronics 60
Erotica 484
Fireworks 1
Food 3
Forgeries 47
Hardware 16
Herbs & Supplements 4
100mg 5-MeO-MIPT
฿1.30
5x Zofran (Ondansetron) 8mg ODT DISSOLVABLES
฿1.72
1G Mephedrone (4-MMC, 4-Methylmethcathinone)
฿1.78
1 oz FROSTY Hollands Hope, an Uplifting Indica
฿17.83
Tramadol-120mg-800 tabs/caps per order
฿28.41
TESTOSTERONE ENANTHATE 250mg/ml x 20
฿9.07
ZOLPIDEM 10mg (Ambien) 100 pills A+
฿5.69
High Quality Cocaine (10g)
฿45.09
News
Closing the Armory
A brand new look for Silk Road!
The gift that keeps on


bitcoin
ACCEPTED HERE

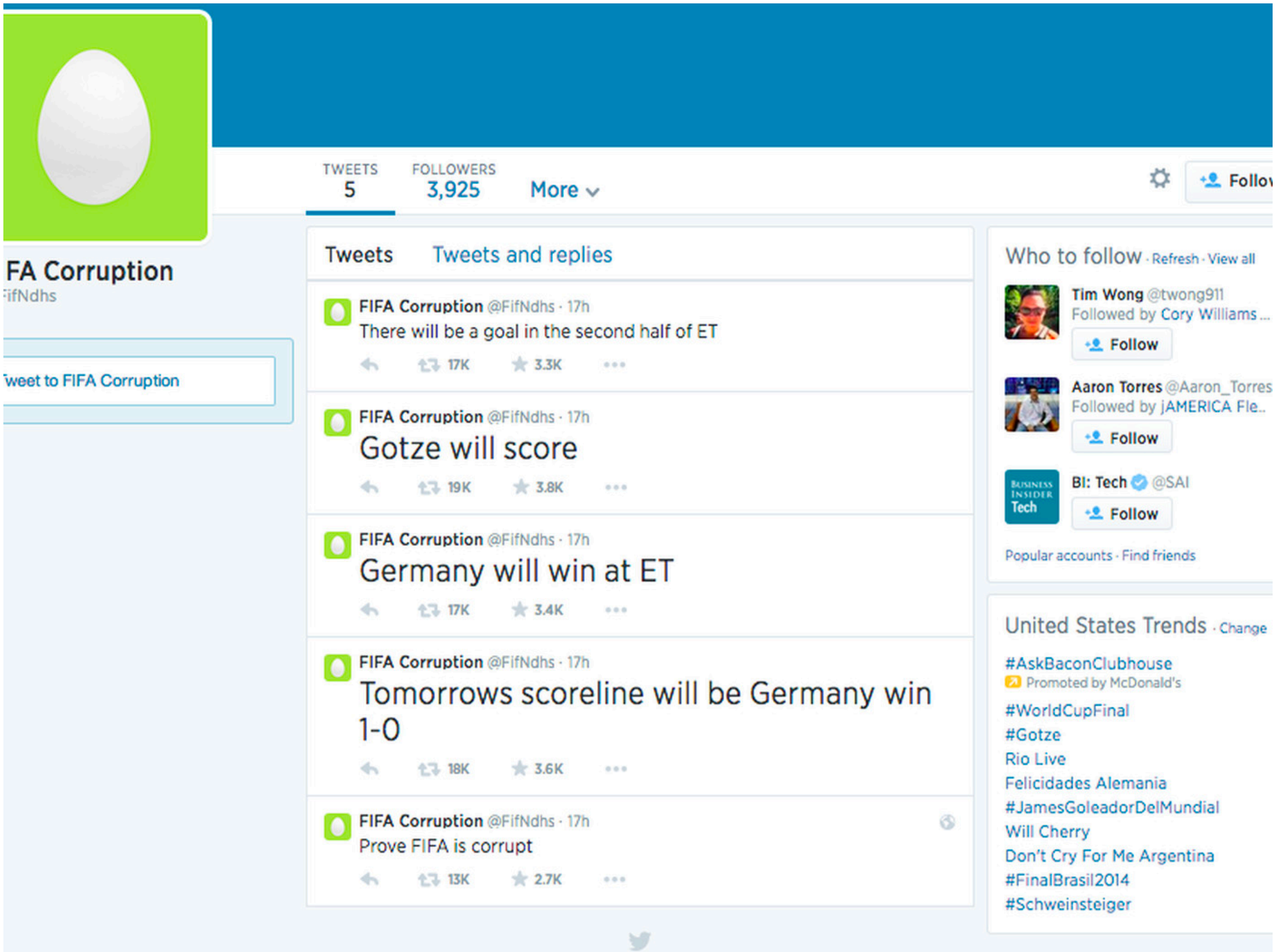

bitcoin
ACCEPTED HERE
SUBWAY
eat fres


ATM
ATM
bitcoin
ATM24Hrs
LASER
ZONE

Append-only Log

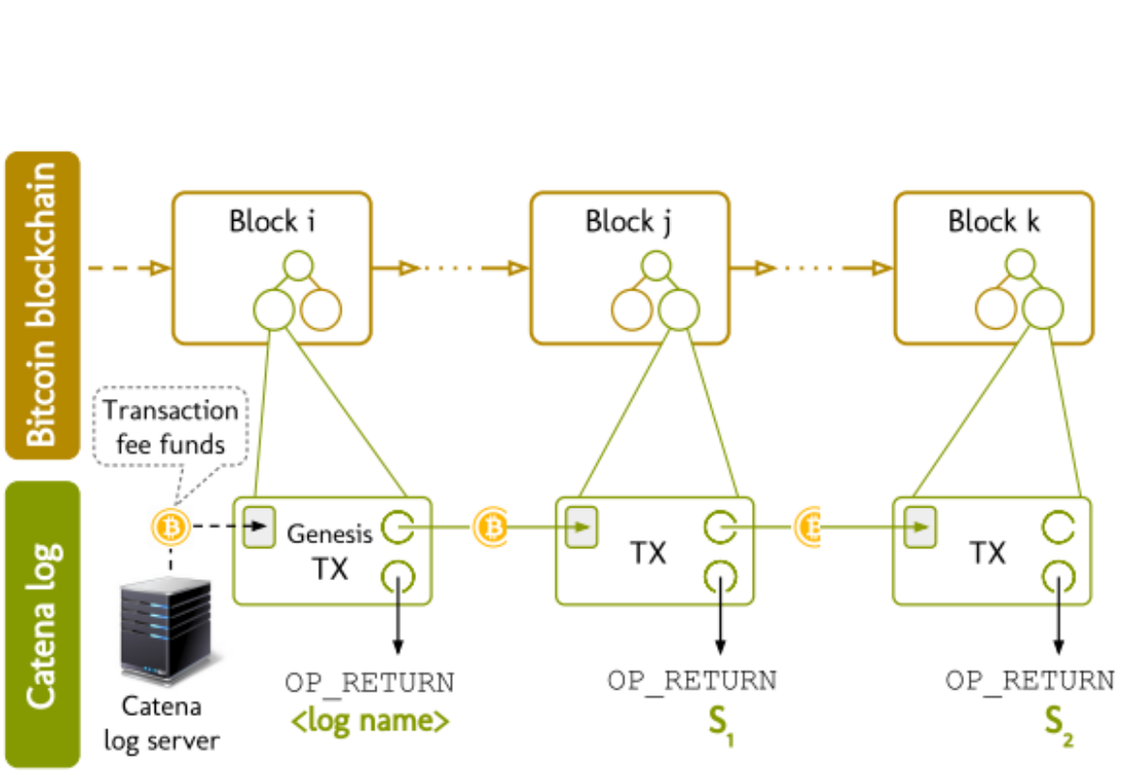
- Nice properties
    - Append-only by design, Transparent, Available, Censorship resistant, …
- Timestamping
    - Documents, certificates, predictions, results, notes, …
        - How to prove that you knew x at given point of time?
            - Commitments: publish H(r||x) for a random r, and reveal r||x later
            - Why Bitcoin helps? Block number, timestamps, no trusted party, ..
- Encoding
    - P2PKH (20 bytes only, a hack), OP_RETURN (220 bytes)
- Illicit Content

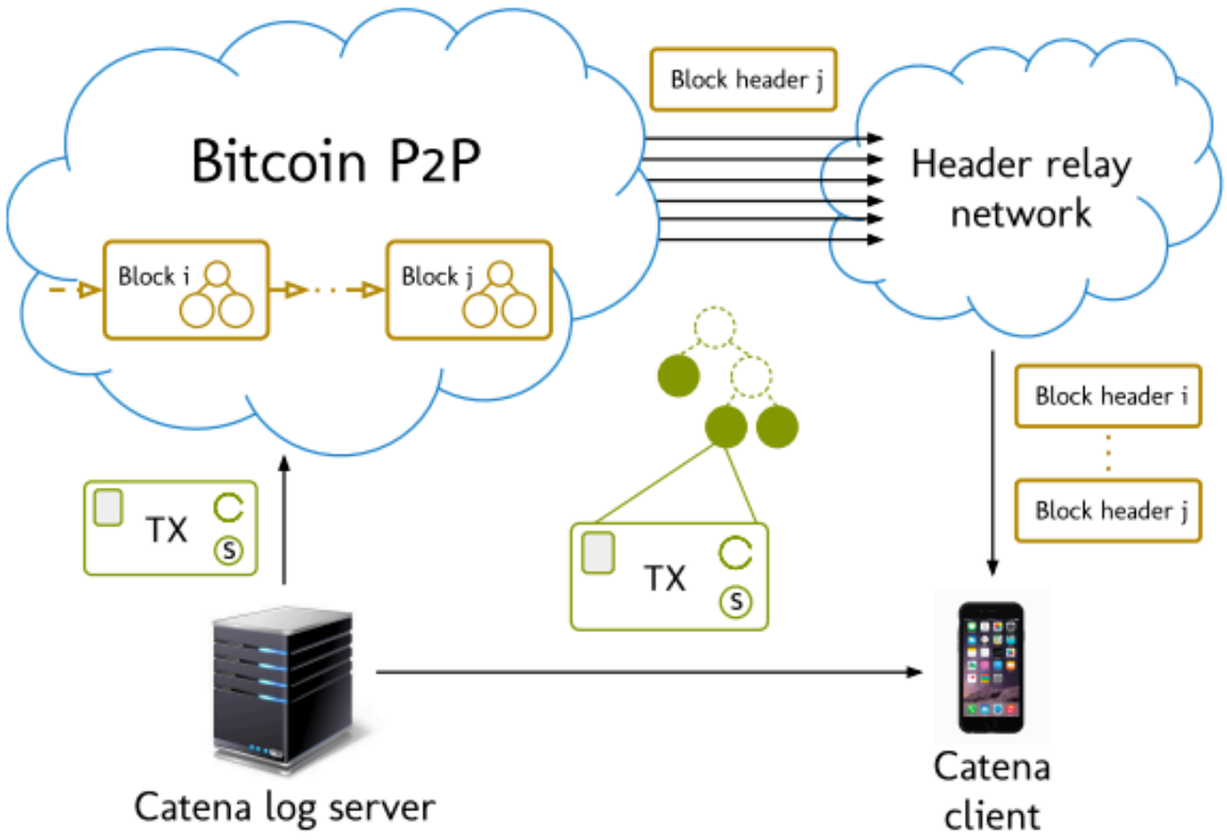
Predictions & Commitments



Catena

- Efficient Non-equivocation via Bitcoin
  - people.csail.mit.edu/alinush/papers/catena-sp2017.pdf





Other Applications

- Overlay currencies
    - Just use Bitcoin as an append-only log and implement any rules on the top of it
- Smart property
    - Transactions are traceable, can that be helpful?
- Colored coins
    - Associate coins with some metadata (*color*)
    - Metadata can be authenticated (signed)

Other Applications

- Public randomness
  - How to generate public (trustworthy) randomness?
  - Many applications, from lotteries to cryptographic protocols
- Secure multiparty computations
  - The scripting language allows to build secure protocols
- Prediction markets
- …

Example: Coin Flipping Online

Round 1:

Each party picks a large random string — Alice picks x, Bob picks y, and Carol picks z.

The parties publish H(x), H(y), H(z) respectively.

Each party checks that H(x), H(y), H(z) are all distinct values (otherwise aborts the protocol).

Round 2:

The three parties reveal their values, x, y, and z.

Each party checks that the revealed values agree with the hashes published in Round 1.

The outcome is (x + y + z) % 3.

What if someone does not reveal their commitment?

Alice can make a *timed commitment* with a bond spendable to Bob if

- it is signed by Alice & Bob
- or, only but Alice but revealing x (the input)

Then they create a time locked transaction (nLockTime) paying the bond to Bob after some time t

scriptPubKey:

```
OP_IF
        <AlicePubKey> OP_CHECKSIGVERIFY <BobPubKey> OP_CHECKSIG
OP_ELSE
        <AlicePubKey> OP_CHECKSIGVERIFY OP_HASH <H(x)> OP_EQUAL
OP_ENDIF
```

scriptSig for Case 1:

```
<BobSignature> <AliceSignature> 0
```

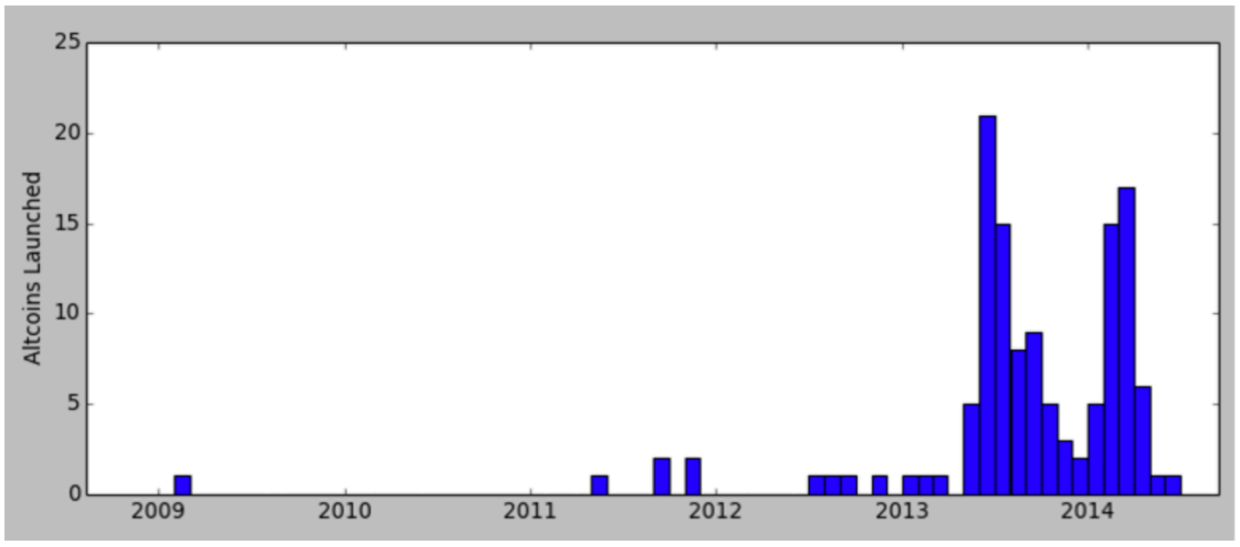
scriptSig for Case 2:

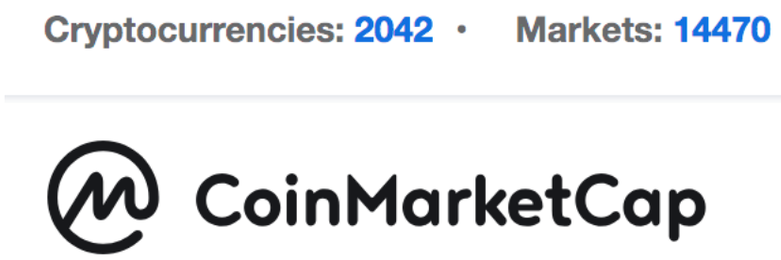
```
x <AliceSignature> 1
```

Altcoins

Altcoins

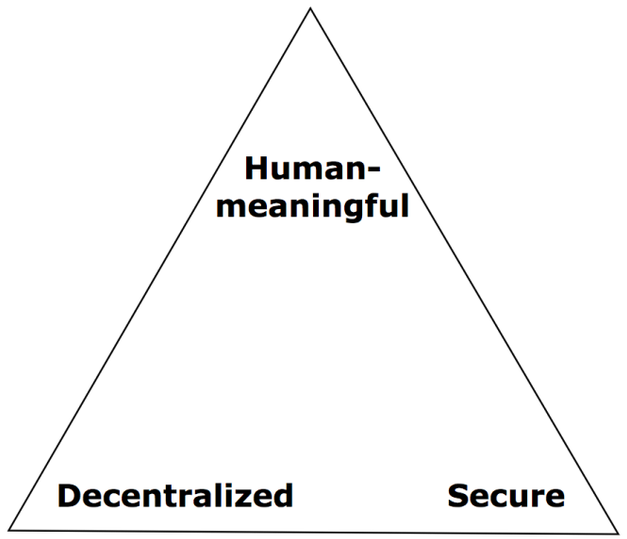
- Alternative cryptocurrencies
  - Unclear what is (not) an altcoin
  - Improve Bitcoin, give new properties or functionalities, scams, …
- Ecosystem is quite complex, how to do initial allocation, …

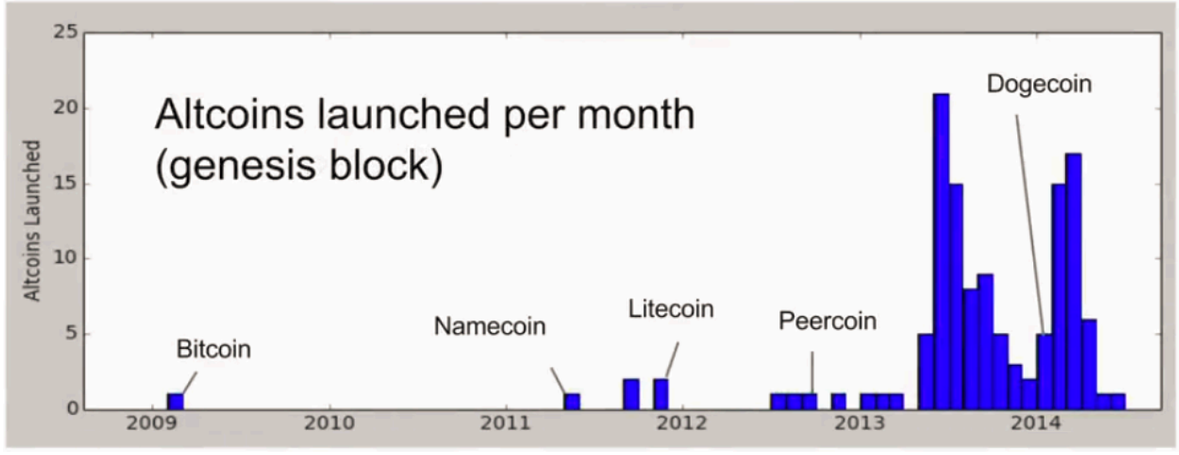




namecoin

- Recap: distributed naming is hard
- Namecoin
  - The first altcoin ever
    - Replace centralized DNS
- Bitcoin's fork
  - With name management
    - New opcodes: NAME_NEW, NAME_FIRSTUPDATE, NAME_UPDATE, …
- Did not get a significant adoption



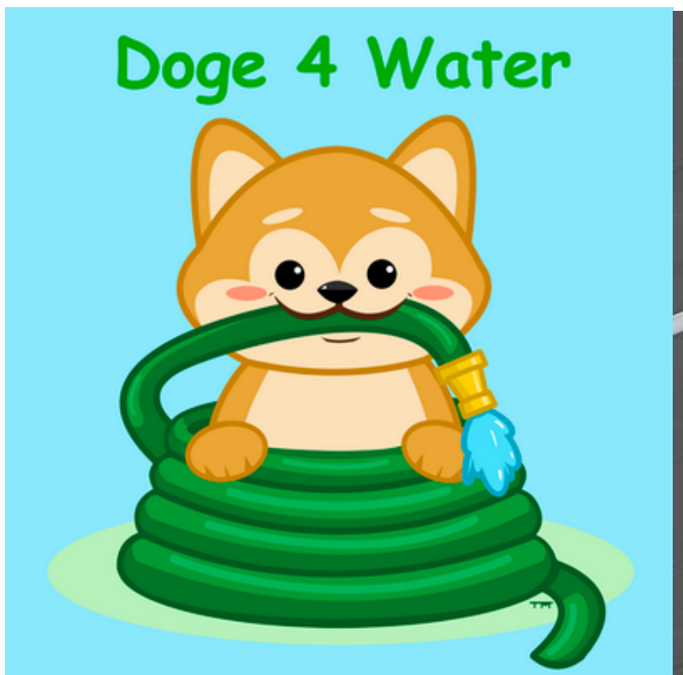


- Bitcoin’s fork aiming for efficiency
  - Block every 2.5 minutes
  - Uses scrypt in its PoW algorithms
- The first altcoin that is still popular

#	Name	Market Cap
1	Bitcoin	$114,109,570,816
2	Ethereum	$23,045,368,843
3	XRP	$19,273,020,265
4	Bitcoin Cash	$9,028,576,137
5	EOS	$5,209,127,736
6	Stellar	$4,548,889,354
7	Litecoin	$3,391,550,735

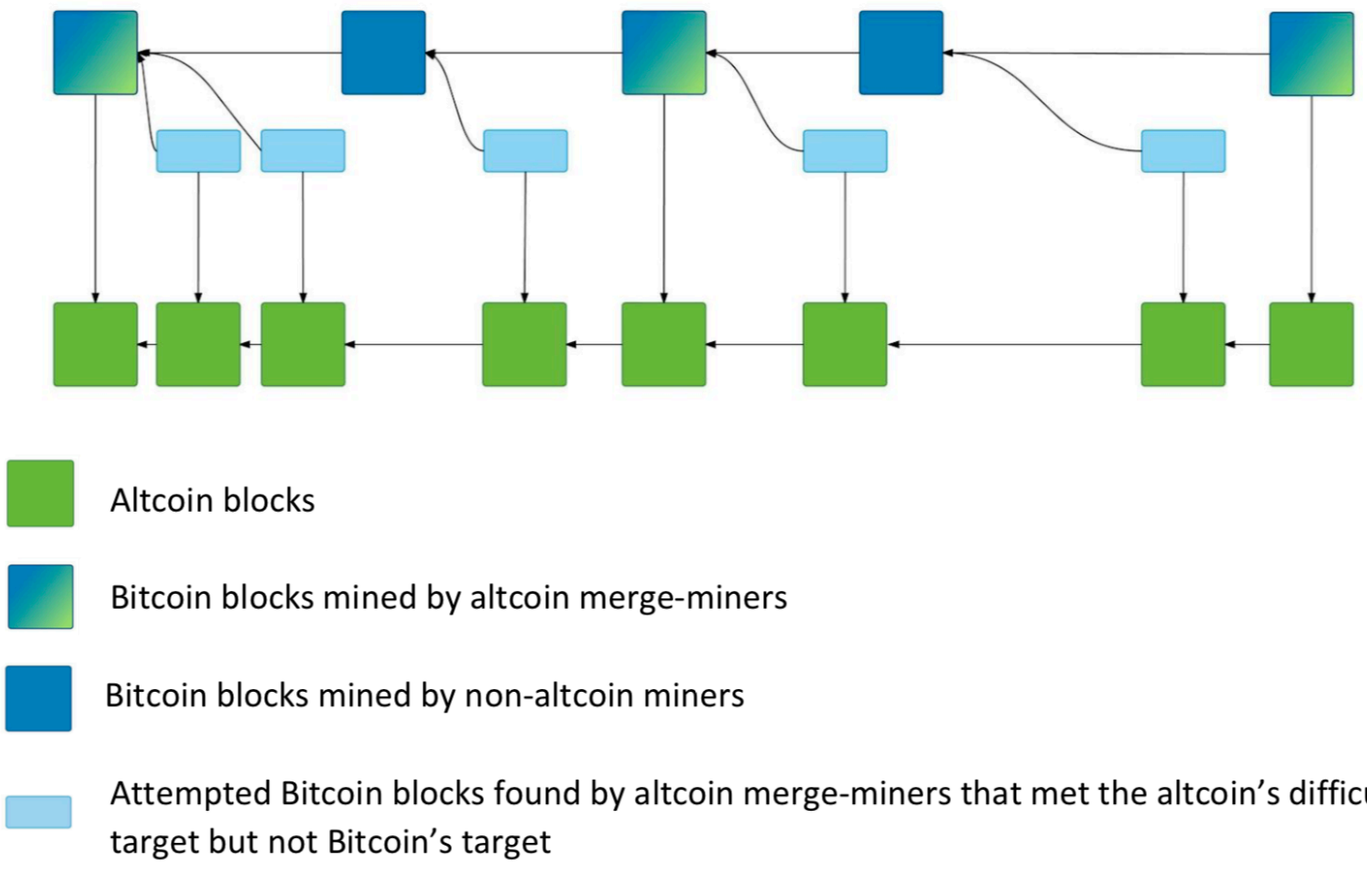
DOGECOIN

- Litecoin’s fork
  - Introduced as a joke
  - Quickly got popularity
  - Fundraising projects



Misc.

- Indicators: market cap, mining power, adoption, …
- Bitcoin - Altcoin interactions
- Altcoin infanticide
- Merge Mining
  - Design an altcoin that uses Bitcoin's mining
  - Put hash pointers to the altcoin in the Bitcoin blockchain
  - Coinbase transaction
  - Multiple benefits



Reading

- Textbook 8, 9, 10

- … and inline references