Lecture 10

Altcoins and the Cryptocurrency Ecosystem

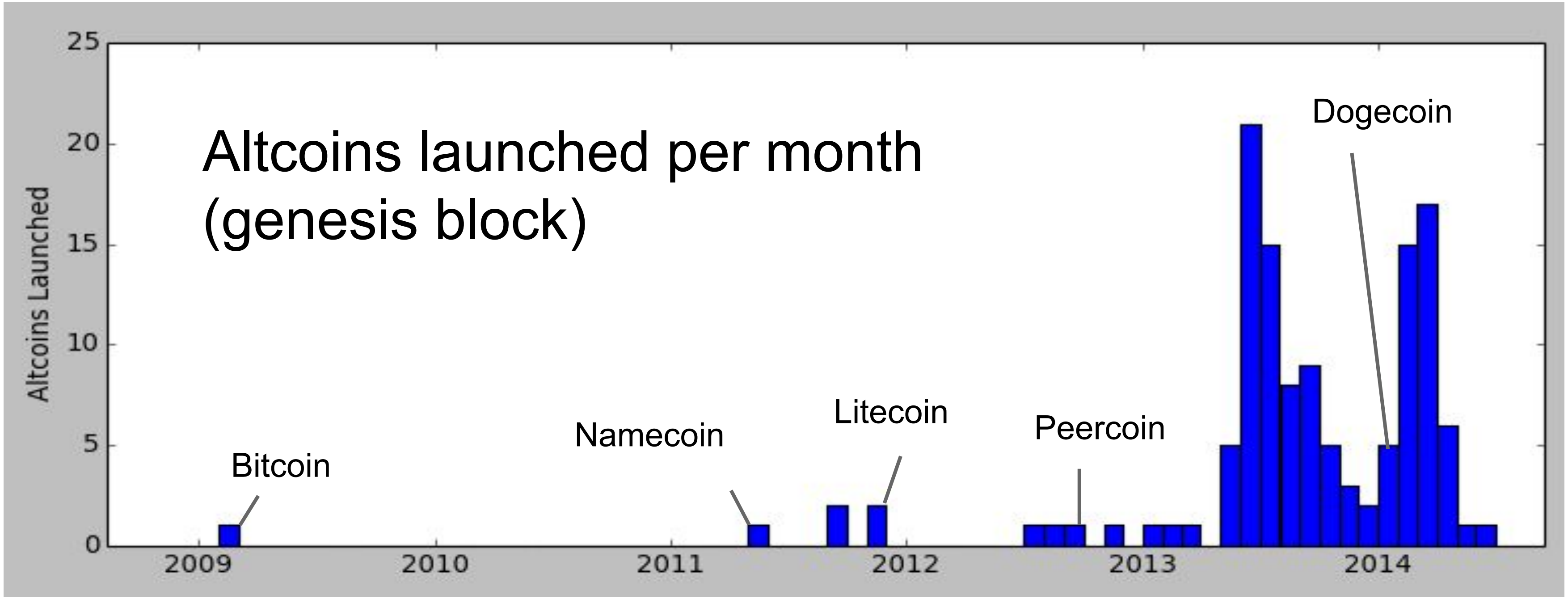
Lecture 10.1:

Short History of Altcoins

Data from mapofcoins.com

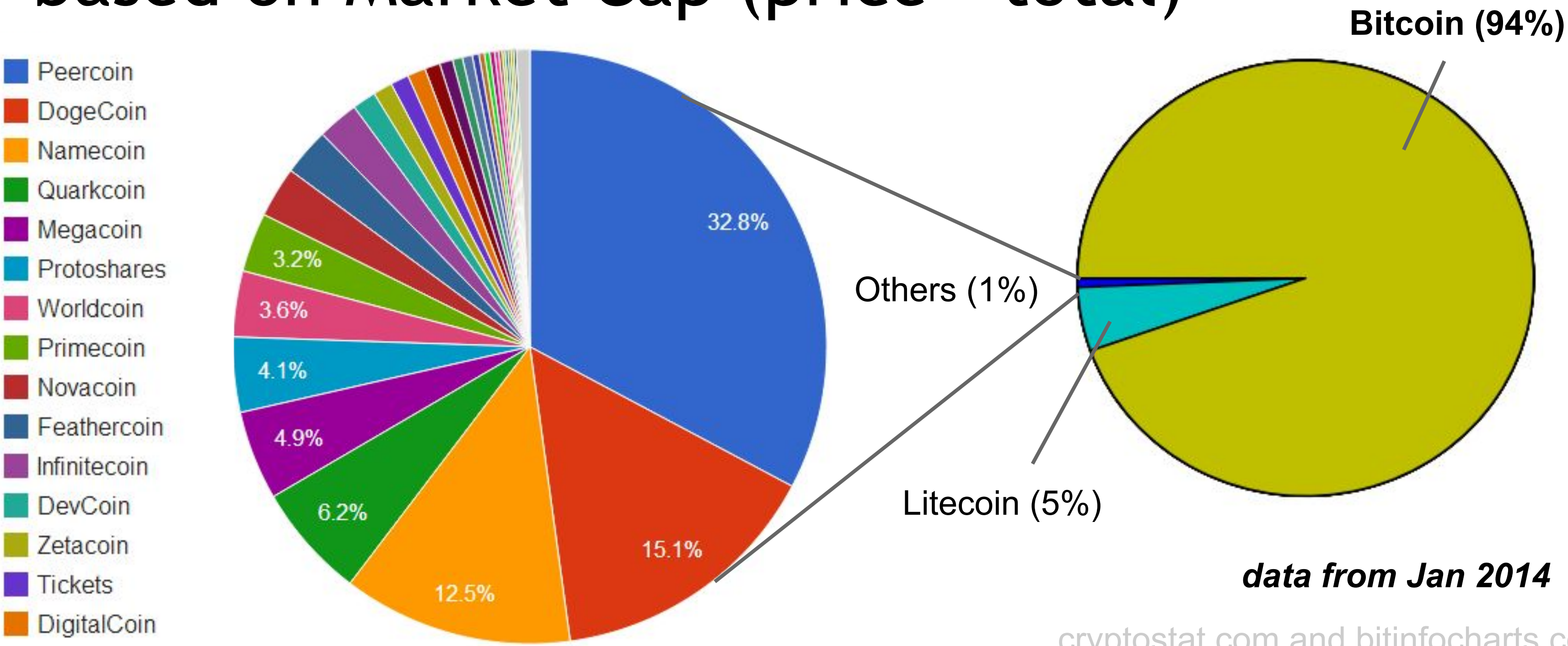
Bitcoin is not alone

Between 150-500 altcoins launched to date



Bitcoin and Litecoin are 99% of total

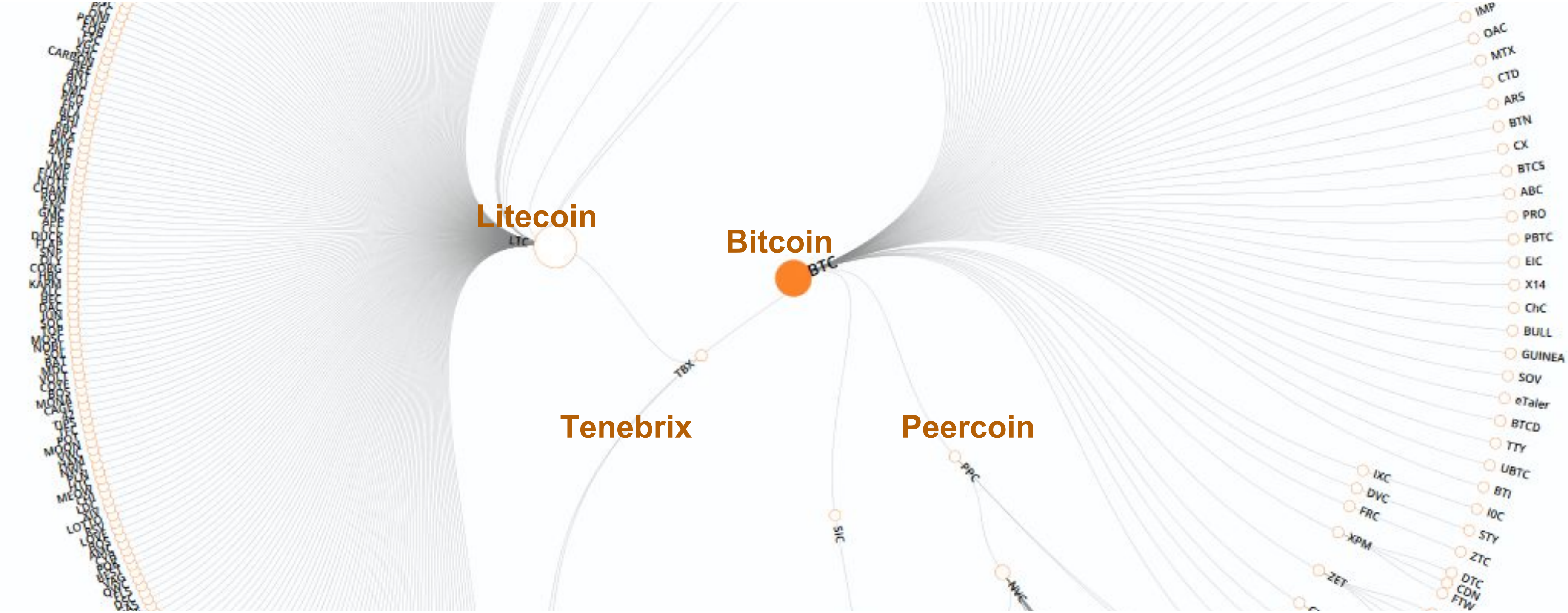
based on Market Cap (price * total)



data from Jan 2014

cryptostat.com and bitinfocharts.com

Altcoin genealogy



Graphic from mapofcoins.com

Features of altcoins

- Better (or different) security
  - Mining puzzle
- Contract/platform features
- Different parameters and monetary policy
  - inflation
  - inter block time
- Community or common interest support

Namecoin

First altcoin (launched in April 2011)

Feature: Domain Name Registration

http://example.bit/

New name costs 0.01 NMC (about 1 cent US)

- No renewal fee: must “ping” every 6 months
- Names (and subdomains) can be transferred/sold

Can be “merge-mined” with Bitcoin - defined later

Litecoin

- Litecoin launched in Sep. 2011
- Memory-hard mining puzzle
  - Intended to be GPU-resistant,
  - when Bitcoin mining was GPU-based
  - FPGA, ASICs, arrived but later than BTC

- 2nd most popular, 1st most widely forked
- Block rate is 4x faster

Peercoin (aka PPCoin)

Launched August 2012

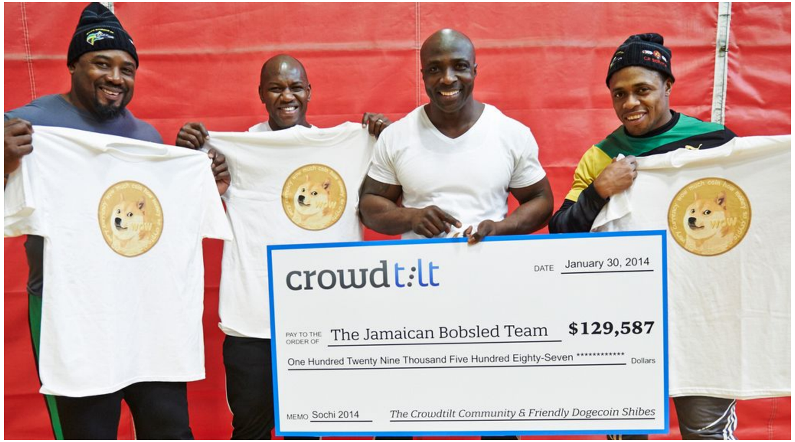
Hybrid mining:

- First Proof-of-Stake algorithm
    - mine by spending “stake” which accumulates
- Proof-of-Work can earn mining rewards
    - … but aren’t counted for choosing the main chain
- Also uses regularly published “checkpoints”
    - acts as a safeguard, planned to remove in future

Dogecoin: Culture

Launched in December 2013

Culture - tipping, charity, sponsorship


crowdtilt
DATE January 30, 2014
PAY TO THE ORDER OF The Jamaican Bobsled Team $129,587
One Hundred Twenty Nine Thousand Five Hundred Eighty-Seven ************ Dollars
MEMO Sochi 2014
The Crowdtilt Community & Friendly Dogecoin Shibes

98
DOGECOIN digital currency
DOGECOIN digital currency
98
FUSION

Dogecoin: “Random” block rewards

Goal: each block bonus is “random”

Implementation: block bonus is pseudorandom function of previous block hash

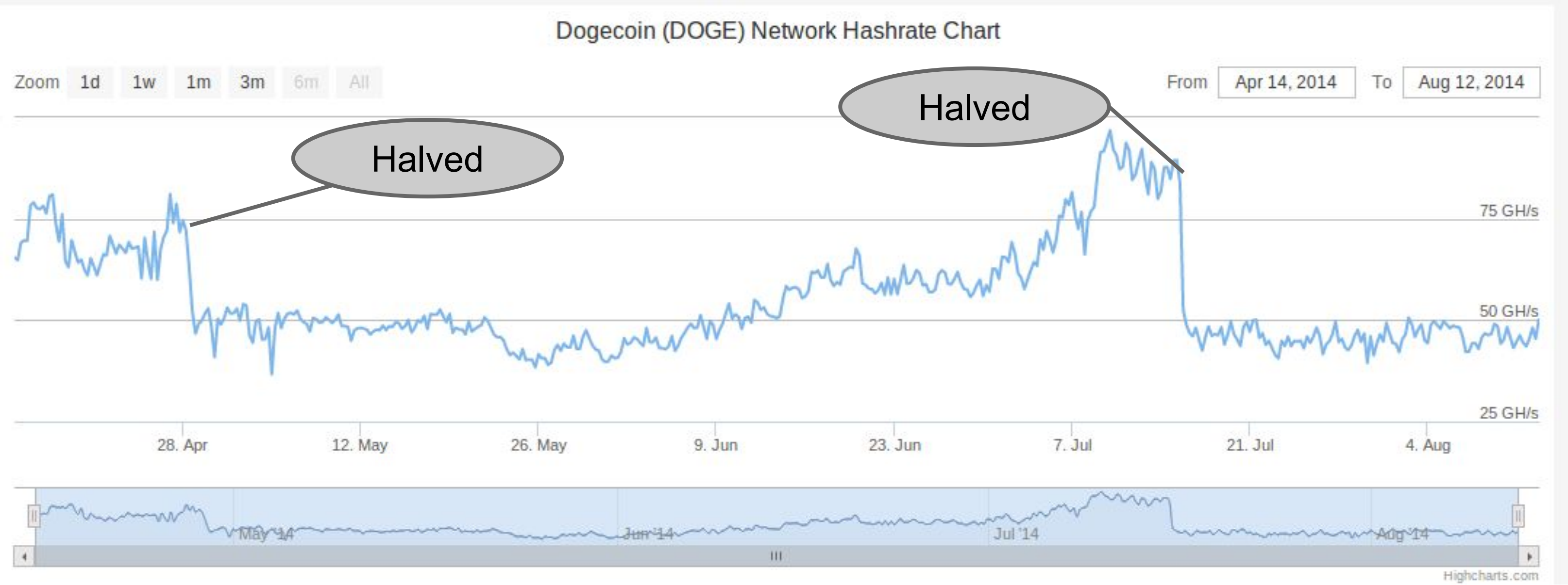
Problem: miners know next reward in advance

switch to other altcoin when reward is low

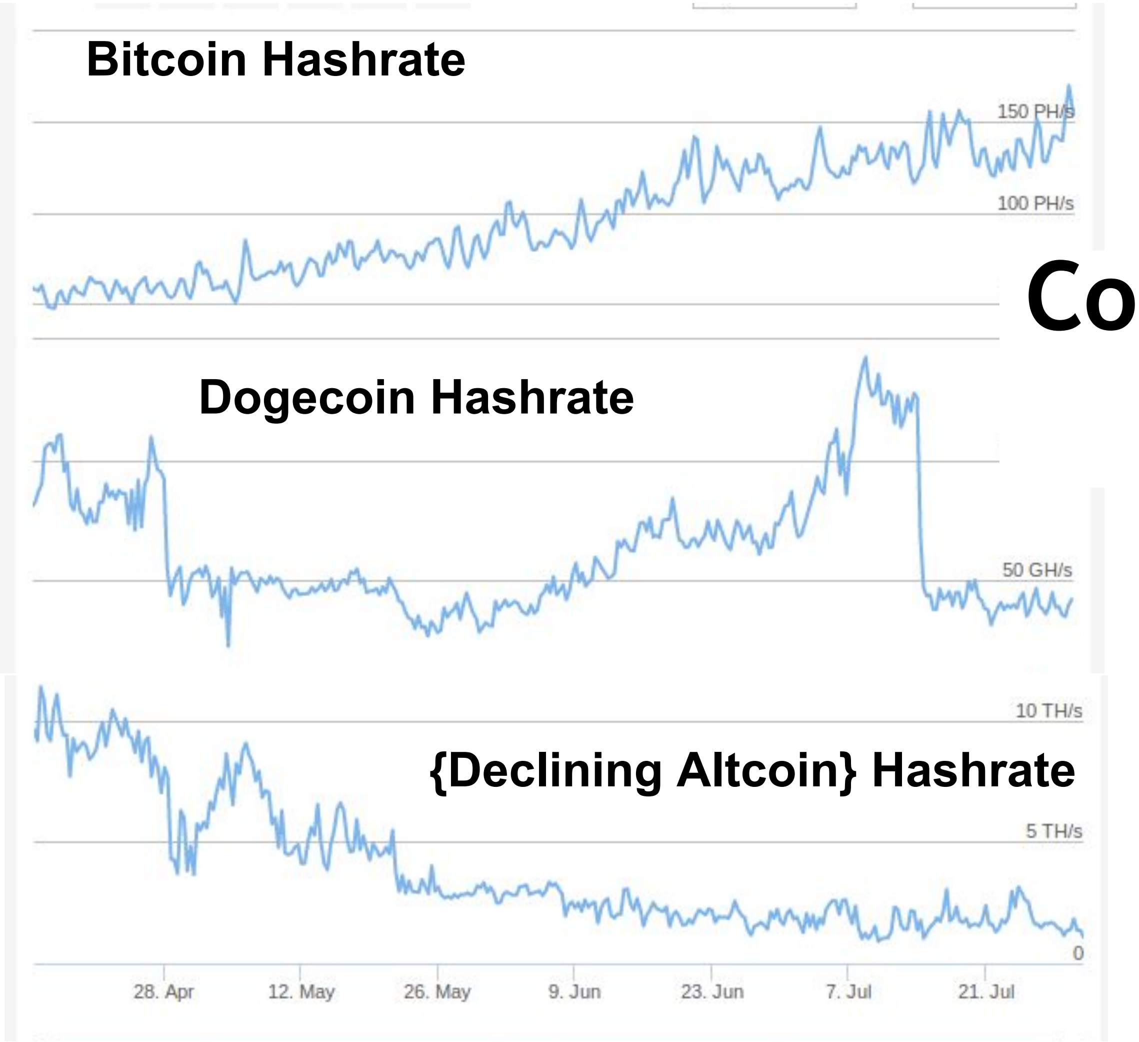
Feature removed in March 2014

Dogecoin: Mining reward half-life

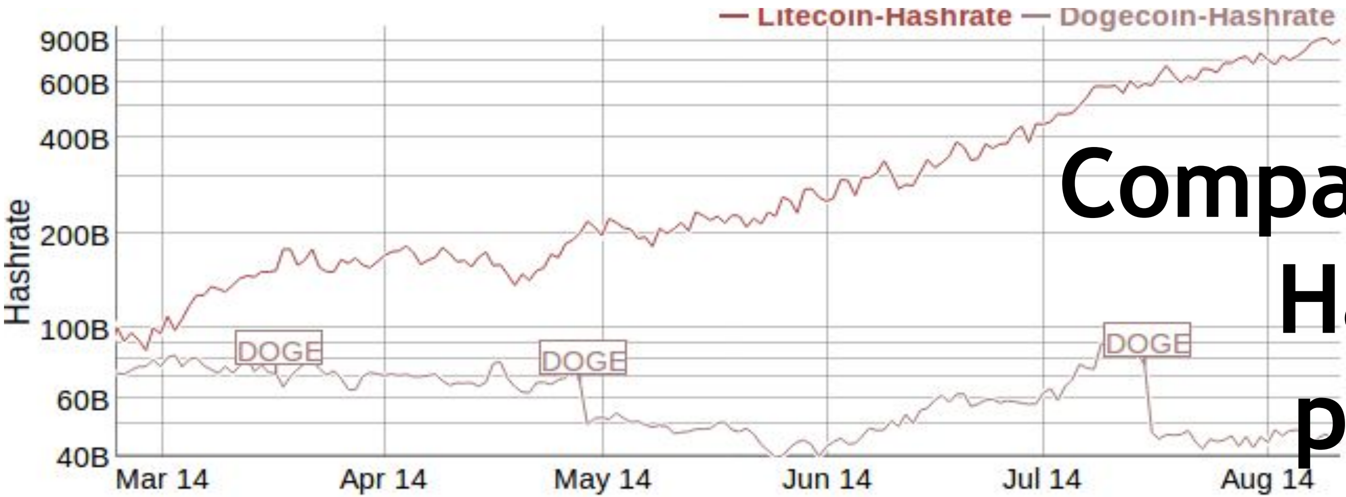
Mining reward cut in half every two months

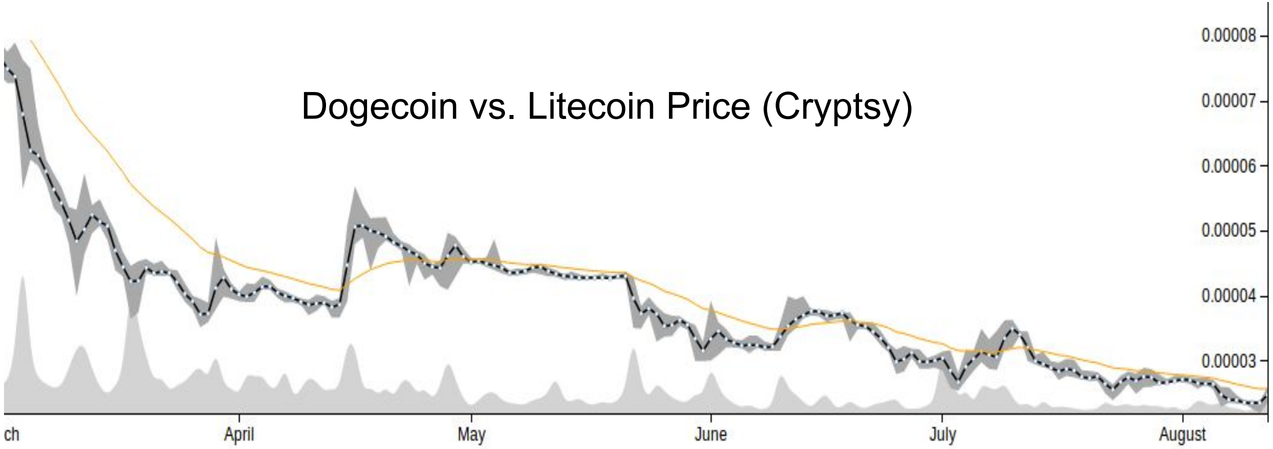


Compare altcoins: Hashrate/time



Compare altcoins: Hashrate and price change




Dogecoin vs. Litecoin Price (Cryptsy)

Metrics for comparing altcoins

- Market cap (price * total number of coins)
  - Overestimates value (but by how much?)
  - Doesn’t account for lost / out-of-circulation coins
- Exchange volume
  - Depends on nature of third party exchanges
  - Can be moved deliberately
- Total hashpower (for similar puzzles)
- Merchant support and usage?

Lecture 10.2:

Interaction between Bitcoin and altcoins

Mining attacks

Even a small miner (or mining pool) on a large network can demolish a small altcoin

Attacks like this have happened before:

Jan 2012: CoiledCoin - by Eligius pool

Jul 2013: TerraCoin - unknown

Nov 2013: WorldCoin - unknown

Merge mining

Ordinarily, mining is exclusive

Each attempt either has a chance to be a Bitcoin block,
or has a chance to be an Altcoin block

Obstacle to bootstrapping

What if we could mine Altcoin blocks
AND Bitcoin blocks at once?

Merge mining

Ordinarily, mining is exclusive

Each attempt either has a chance to be a Bitcoin block,

or has a chance to be an Altcoin block

Previous Bitcoin block

Bitcoin transactions

```
H(prev || merkl_root || nonce) < TARGET
```

Previous Altcoin block

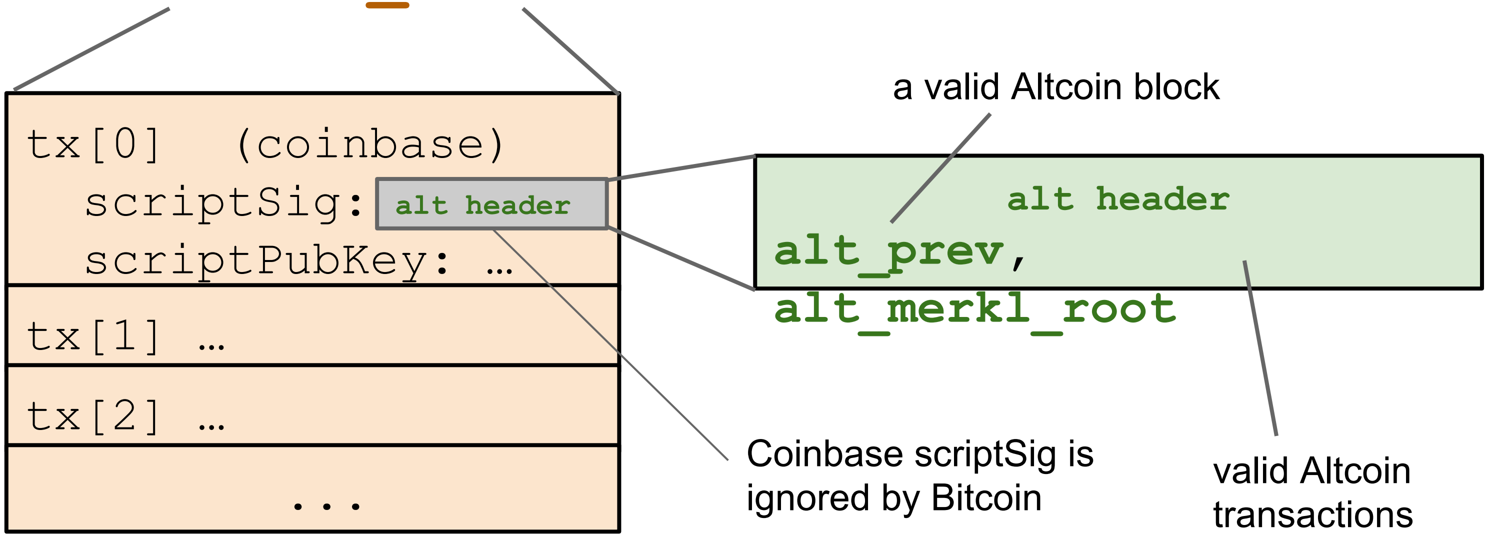
Altcoin transactions

```
H(alt_prev || alt_merkl_root || nonce) < TARGET
```

Merge mining: How it works

```
H(prev || merkl_root || nonce) < TARGET
```

```
H(prev || merkl_root || nonce) < TARGET
```



```
tx[0]  (coinbase)
  scriptSig: alt header
  scriptPubKey: …
tx[1] …
tx[2] …
...
```

```
alt header
alt_prev,
alt_merkl_root
```

a valid Altcoin block

Coinbase scriptSig is ignored by Bitcoin

valid Altcoin transactions

Merge mining

Merge mining is a mixed blessing

- Easier to recruit participants
- Cheaper for attackers (e.g. CoiledCoin)
- Miners might not validate transactions

Many mining pools merge-mine several coins

- GHash.IO: Bitcoin, Namecoin, IXCoin, Devcoin

Atomic cross chain swaps

with TierNolan's protocol

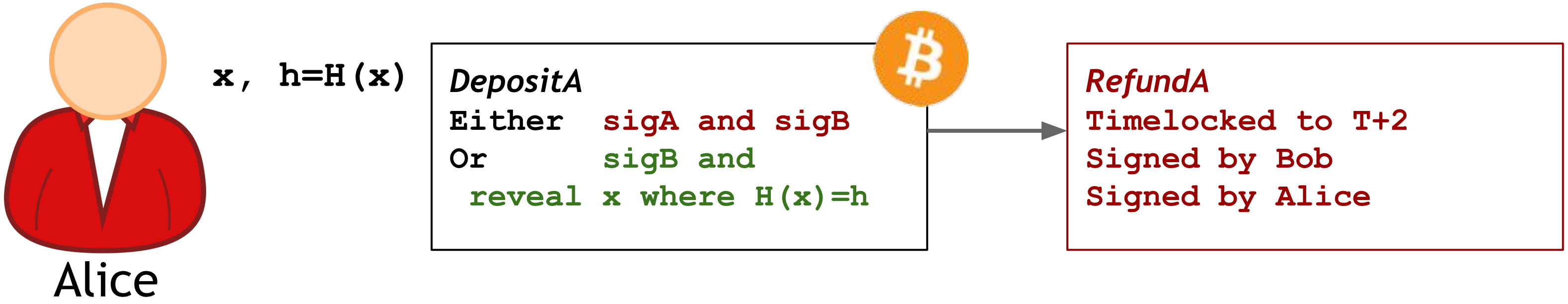
Problem: Alice has 1 BTC, Bob has 1 LTC

They want to swap, but who goes first?

Goal: Either both transactions complete, or neither do

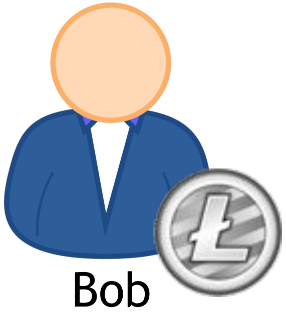
Atomic cross chain swaps

Step 1: Alice generates secret **x**, Alice&Bob sign ***RefundA***



```
DepositA
Either   sigA and sigB
Or       sigB and
 reveal x where H(x)=h
```

```
RefundA
Timelocked to T+2
Signed by Bob
Signed by Alice
```

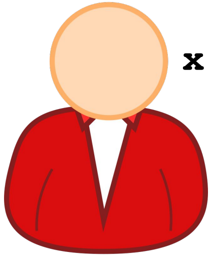


- Alice generates ***DepositA***, but doesn’t publish it yet
- Alice generates ***RefundA***, and gets Bob’s signature on it
- Once ***RefundA*** is signed, she publishes ***DepositA***

- If Bob learns **x** before time **T+2** , he can ***take the 1BTC***
- If Alice does not reveal **x**, she can ***claim her refund*** at **T+2**

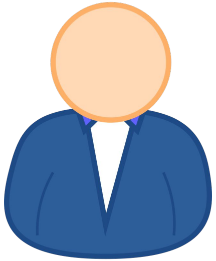
Atomic cross chain swaps

Step 2: Bob deposits 1LTC, Alice&Bob sign *RefundB*



`x, h=H(x)`

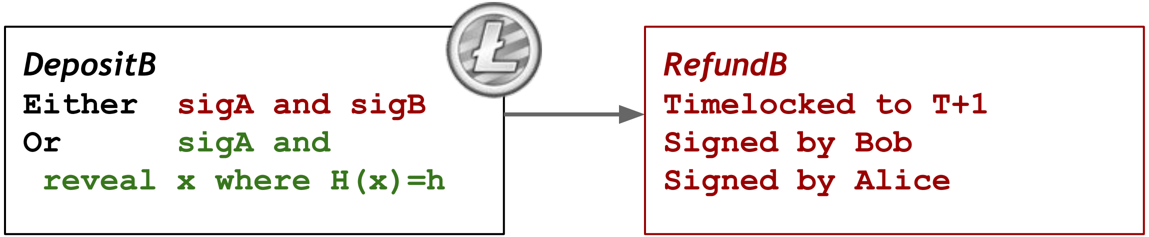
Alice



Bob

- Bob generates ***DepositB***, but doesn't publish it yet
- Bob generates ***RefundB***, and gets Alice's signature on it
- Once ***RefundB*** is signed, he publishes ***DepositB***

- If Alice reveals **x** before time **T+1** , she can ***take the 1LTC***
- If Alice does not reveal **x**, Bob can ***claim his refund***



DepositB

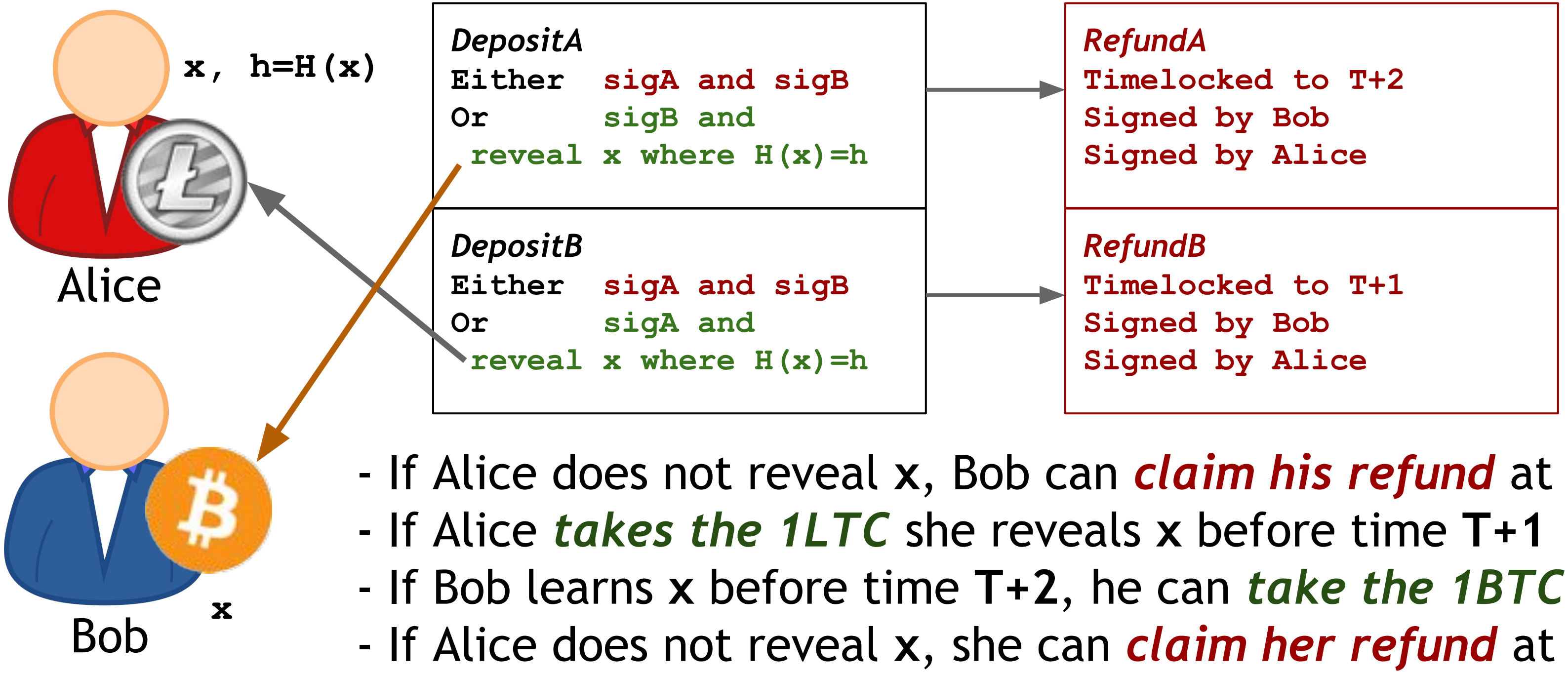
```
Either   sigA and sigB
Or       sigA and
 reveal x where H(x)=h
```

RefundB

```
Timelocked to T+1
Signed by Bob
Signed by Alice
```

Atomic cross chain swaps

Step 3: Alice reveals **x**, both players *claim their coins*



DepositA
```
Either   sigA and sigB
Or       sigB and
          reveal x where H(x)=h
```

DepositB
```
Either   sigA and sigB
Or       sigA and
          reveal x where H(x)=h
```

RefundA
```
Timelocked to T+2
Signed by Bob
Signed by Alice
```

RefundB
```
Timelocked to T+1
Signed by Bob
Signed by Alice
```

- If Alice does not reveal x, Bob can ***claim his refund*** at **T+1**
- If Alice ***takes the 1LTC*** she reveals x before time **T+1**
- If Bob learns x before time **T+2**, he can ***take the 1BTC***
- If Alice does not reveal x, she can ***claim her refund*** at **T+2**

Atomic cross chain swaps

- This protocol could provide secure, decentralized exchange between Altcoins

- This has not been seen in the wild
  - Disadvantages: multiple transactions, DoS risk

- Third party exchanges are used instead

Summary so far

- Bitcoin and hundreds of Altcoins coexist

  Compete and interact supportively or destructively

- Merge mining - several Altcoins at once
  - Even without explicit support from Bitcoin
- Hash commits - interdependent transactions
  - Possible with existing script languages

Lecture 10.3:

Lifecycle of an Altcoin

Launching an Altcoin

- Easy part:

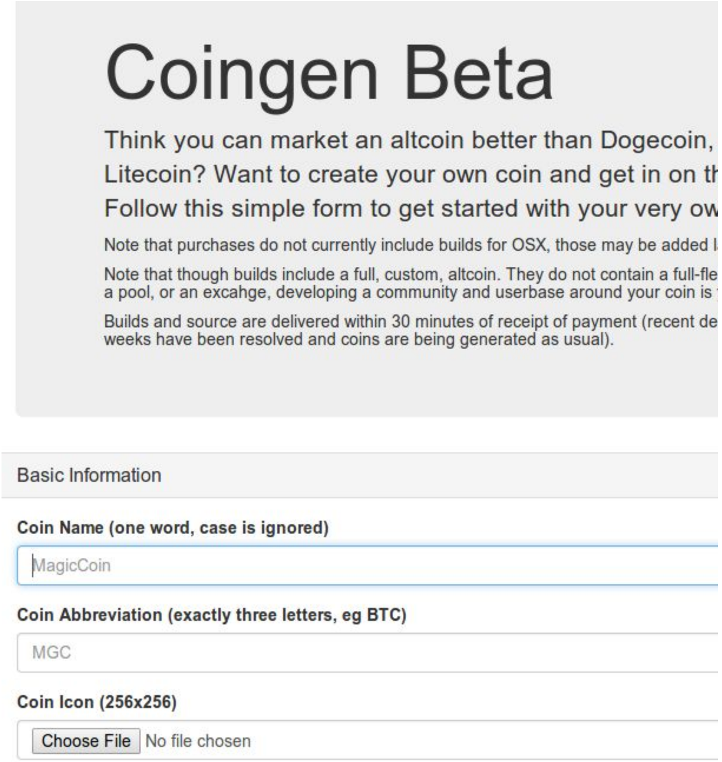
  Fork an existing codebase, modify to taste

  Announce software on Bitcoin forum

- Hard part: Bootstrapping interest
  - Miners
  - Stakeholders
  - Developers
  - Liquidity

archive of http://coingen.bluematt.me/

Automated Altcoin Generator



Coingen Beta

Think you can market an altcoin better than Dogecoin, Litecoin? Want to create your own coin and get in on th Follow this simple form to get started with your very ow

Note that purchases do not currently include builds for OSX, those may be added l

Note that though builds include a full, custom, altcoin. They do not contain a full-fle a pool, or an excahge, developing a community and userbase around your coin is

Builds and source are delivered within 30 minutes of receipt of payment (recent de weeks have been resolved and coins are being generated as usual).

Basic Information

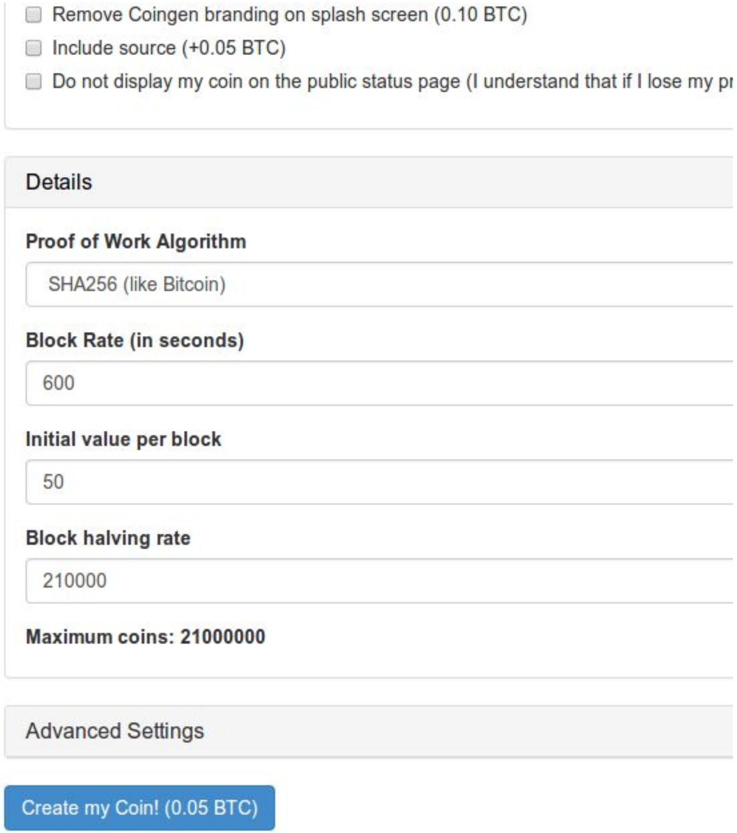
Coin Name (one word, case is ignored)

MagicCoin

Coin Abbreviation (exactly three letters, eg BTC)

MGC

Coin Icon (256x256)



☐ Remove Coingen branding on splash screen (0.10 BTC)

☐ Include source (+0.05 BTC)

☐ Do not display my coin on the public status page (I understand that if I lose my pr

Details

Proof of Work Algorithm

SHA256 (like Bitcoin)

Block Rate (in seconds)

600

Initial value per block

50

Block halving rate

210000

Maximum coins: 21000000

Advanced Settings

Altcoin infrastructure

- Tipbots, faucets
- Logos, brand, marketing
- Exchanges, payment processors
- Developer tools, block explorer, testnet
- Steering foundation

Initial Allocation / Fundraising

Pre-mine: founders get a Altcoin stash

Pre-sale: founders get a stash of Bitcoin or $

Proof-of-Burn (Unilateral pegging):

Destroy 1 unit of Bitcoin, earn one unit of Altcoin

Ownership of Bitcoin “grandfathered” in

Airdrop: give coins to members of some group

Auroracoin

Launched Jan 24, ‘14

Airdrop: Every Iceland citizen can claim 31.8 AUC, starting Mar 25, ‘14

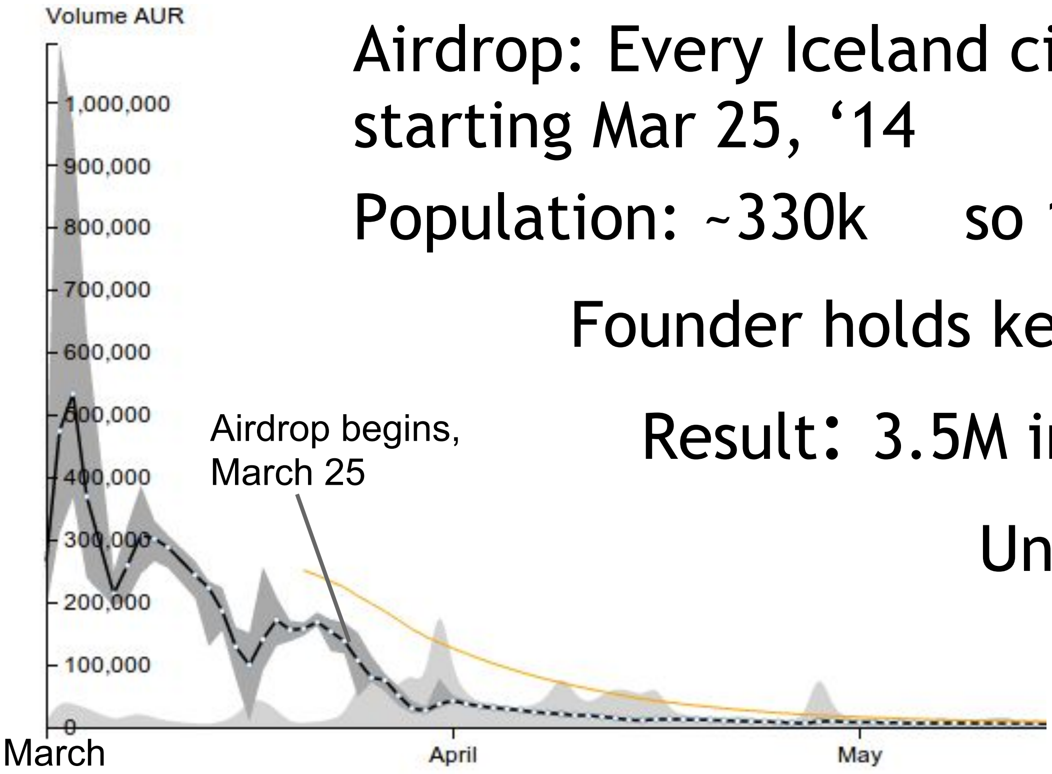
Population: ~330k   so 10.5M potential giveaway

Founder holds keys to 50% (10.5M of 21M)

Result: 3.5M in circulation

Uncertainty in money supply

Accountability?



Airdrop begins, March 25

The Pump-and-Dump cycle

1. Begin with an altcoin about to launch

    or an existing low-value, declining altcoin

2. Attacker buys lots of coins

3. Attacker launches marketing campaign to convince the public that altcoin has grassroots support

4. Attacker sells coins once price rises

5. Marketing campaign ends, altcoin declines

Arguments against altcoins

Position: altcoins harm the whole ecosystem

- Divided mining power means weak security
- Dilution of scarcity
- Pump-and-Dump schemes

Arguments for altcoins

Position: Altcoins essential part of ecosystem

- Competition leads to better systems
- Bitcoin community is too risk averse

  Altcoins are a testbed for new features
- Hedging against uncertainty/failure

  Multi headed hydra
- “Jubilee” - reset the allocation of wealth

Lecture 10.4:

Bitcoin-Backed Altcoins, “Side Chains”

Bitcoin-to-Altcoin value transfer

Launch an Altcoin, convince BTC users to join

Options discussed so far are extremes:

- “Grandfather”: all BTC holders get one

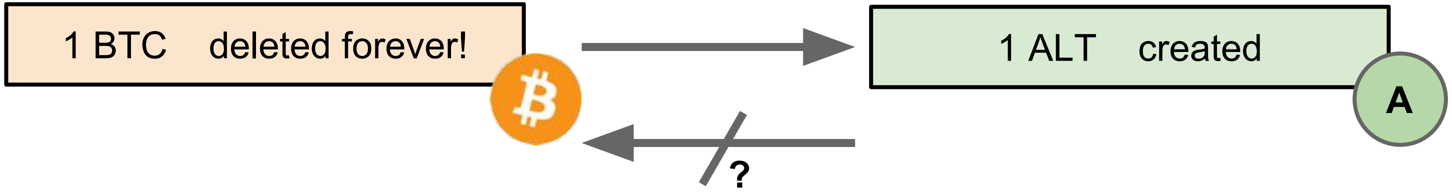
  no risk taken - Altcoin crashes, nothing changes

- Unilateral exchange: burn BTC, get ALT

  full risk taken - Altcoin crashes, lost your BTC

Bitcoin as a reserve currency

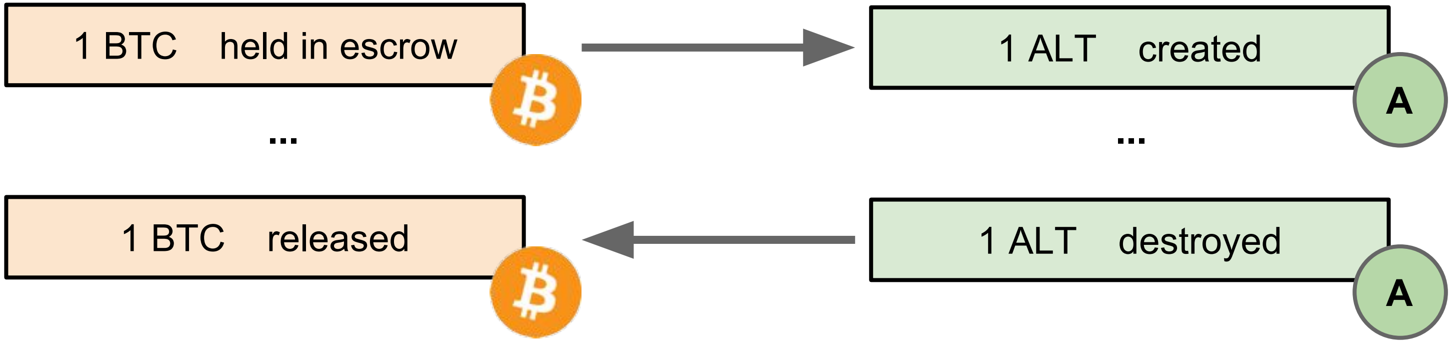
Unilateral peg



1 BTC deleted forever!

1 ALT created

Bilateral peg



1 BTC held in escrow

1 ALT created

...

...

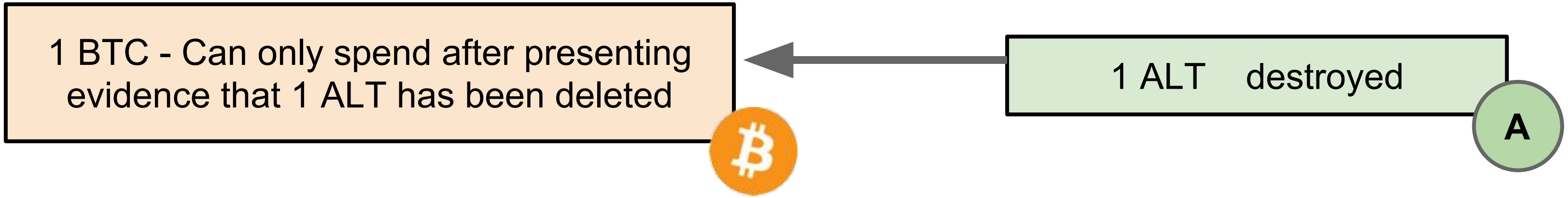
1 BTC released

1 ALT destroyed

Side chains

Proposal:

Bitcoin transactions that describe Altcoin's validation rules


1 BTC - Can only spend after presenting evidence that 1 ALT has been deleted
1 ALT destroyed
A

Naively, to support this transaction, every Bitcoin node must store all of the data for Altcoin

Side chains - Improving efficiency

Requires validating every transaction

Idea:

Only need to support ***SPV*** security

Instead of TX is in Longest ***Valid*** Blockchain,

TX is in Longest Blockchain

Only involves checking Block headers

1 BTC - Can only spend after presenting ***evidence*** that 1 ALT has been deleted

Goal: compact SPV proofs

If an Altcoin has a very fast block rate, checking an SPV proof may still be slow

O(N) time to check O(N) blocks

Idea: instead of just a chain, store blocks in a structure supporting probabilistic SPV proof

O(polylog N) time to check O(N) blocks

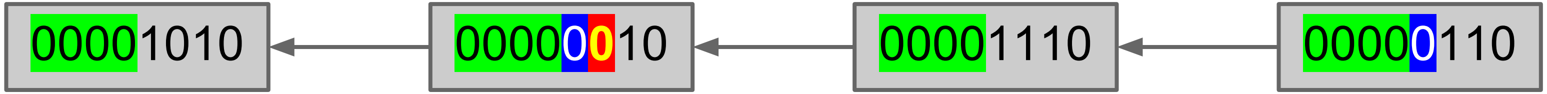
Proof-of-Work sample

Suppose we have 4 blocks of difficulty 2^{-4}

Every hash begins with at least 4 zero bit 0000

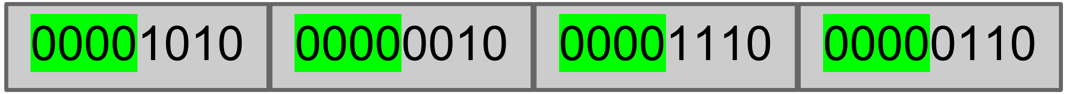
On average, half of the blocks have 5 00000

One of the blocks would have a 6th 000000



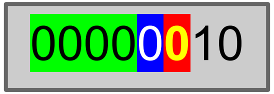
Proof-of-Work sample

Average number of hashes needed to find FOUR hashes with 4 zero bits is 4 * 2^4 = 64



00001010 00000010 00001110 00000110

Same as average needed just to find ONE hash with 6 zero bits.



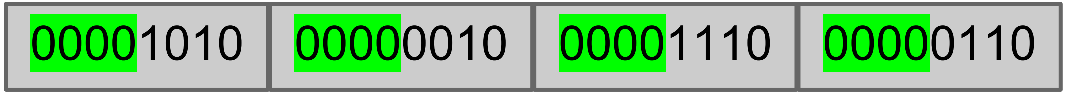
00000010

Idea: Why not just check block with most bits?

Proof-of-Work sample

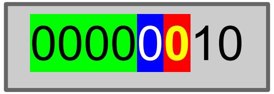
Suppose an attacker only computes 32 hashes

Probability of finding FOUR 4-hashes is 14%



00001010 | 00000010 | 00001110 | 00000110

Probability of finding ONE 6-hash is 40%



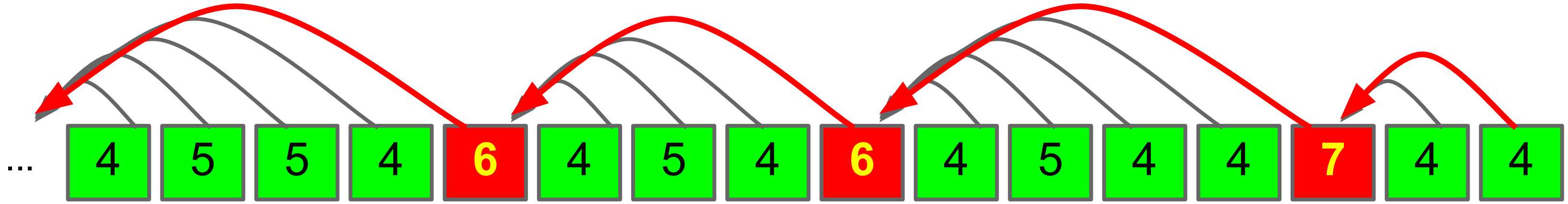
00000010

Lesson: more samples, more precise estimates

Proof-of-Work skiplist

Example: data structure for 1/4 samples

Every block points to prev AND to the most recent 6+



To checking a compact SPV proof, follow the red arrows

… this can be generalized to an ordinary skip list

Side Chains - Conclusion

- Altcoins that hold Bitcoin in reserve
  - Could smooth Altcoin launch risks

- Requires changes to Bitcoin for support

- Like other Altcoins, could be merge mined

  … or avoid merge mining with an alternate puzzle

Conclusion

- Bitcoin and hundreds of Altcoins coexist

  Compete and interact, supportively or destructively

  Atomic swaps, merge mining supported today

  More interactions may be supported in the future

- Questions:

  Will Altcoins consolidate or diversify further?

  Will Bitcoin be overtaken by an Altcoin?

  Embrace interaction with Altcoins or avoid them?

In the next lecture…

Lecture 11: The future of Bitcoin?

Can Bitcoin lead to a decentralized society?

Autonomous agents, smart property