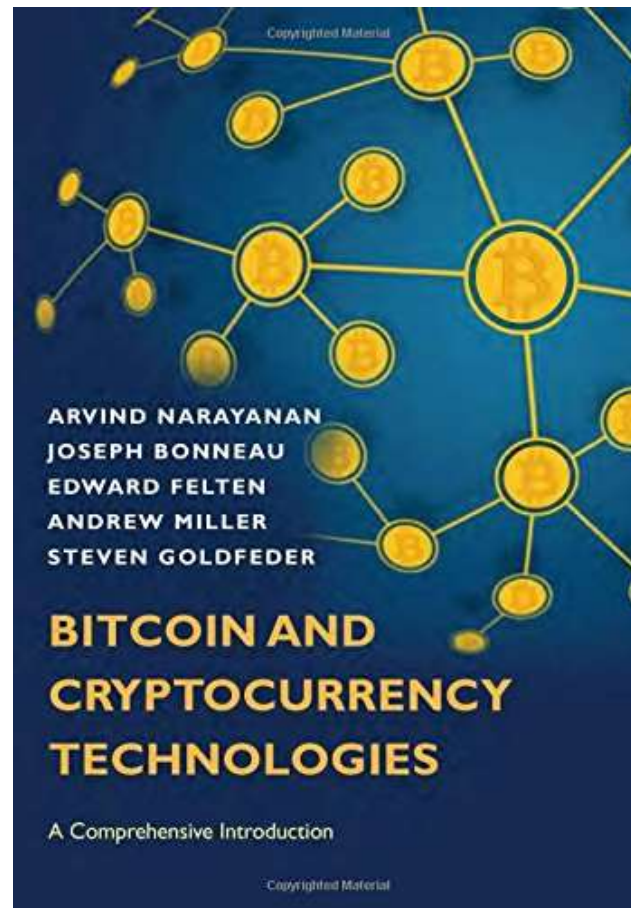


Blockchain & Business Application

Lecture:

Altcoins and the Cryptocurrency Ecosystem

Chapter 10



- 2009: Bitcoin
- 2011: Namecoin (Bitcoin-like)
- How to count?
- What is “altcoin”? Old CC’s?

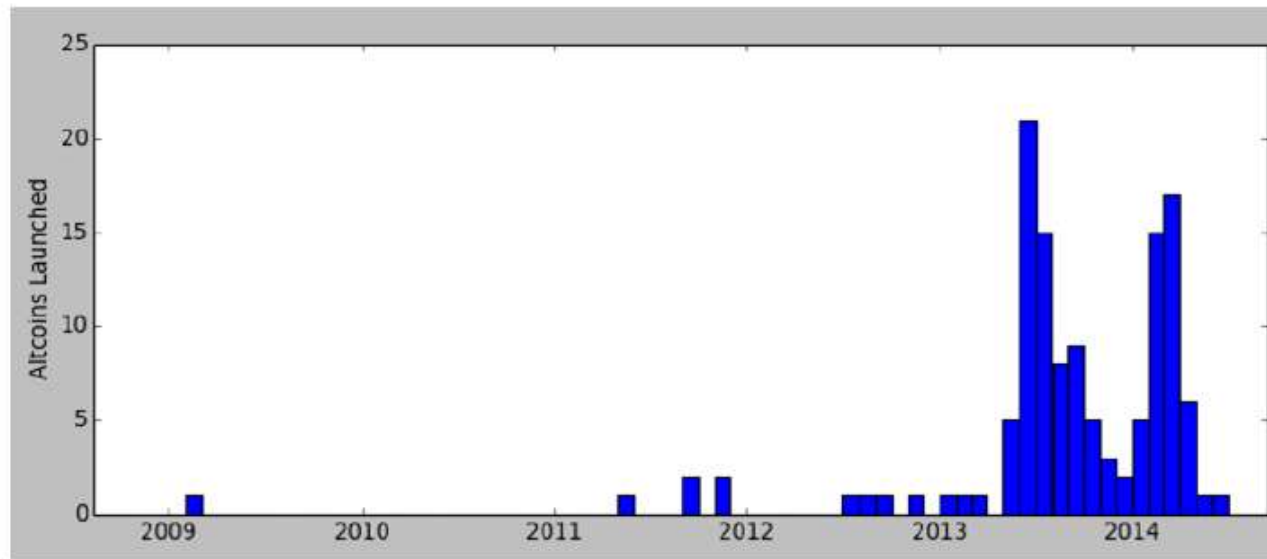










































Figure 10.1: Altcoins launched per month (measured by genesis block creation).

FALIH UZATDIN, IUO-2021

coinmarketcap.com (June 2019)

Cryptocurrencies ▾										
Exchanges ▾										
Watchlist										
USD ▾										
← Back to Top 100										
#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d	
1	 Bitcoin	BTC	\$165,077,711,090	\$9,289.95	17,769,500	\$15,963,551,584	0.00%	1.31%	14.42%	***
2	 Ethereum	ETH	\$28,646,835,680	\$268.82	106,564,409	\$5,698,132,180	-0.15%	-0.03%	3.81%	***
3	 XRP	XRP	\$18,354,267,950	\$0.431845	42,501,950,124 *	\$1,163,581,342	-0.30%	-0.05%	6.99%	***
4	 Litecoin	LTC	\$8,472,996,429	\$135.99	62,305,175	\$4,375,058,549	-0.16%	-0.04%	0.72%	***
5	 Bitcoin Cash	BCH	\$7,387,059,935	\$413.89	17,847,675	\$1,268,834,487	-0.24%	-0.45%	3.50%	***
6	 EOS	EOS	\$6,297,199,427	\$6.85	919,863,767 *	\$1,610,938,429	-0.16%	-0.47%	4.98%	***
7	 Binance Coin	BNB	\$4,892,282,345	\$34.65	141,175,490 *	\$493,217,863	0.10%	-1.86%	-1.74%	***
8	 Bitcoin SV	BSV	\$4,005,430,599	\$224.45	17,845,598	\$279,365,343	-0.06%	-0.08%	11.17%	***
9	 Tether	USDT	\$3,537,593,389	\$1.00	3,534,666,959 *	\$15,173,019,906	0.02%	-0.05%	-0.34%	***
10	 Stellar	XLM	\$2,384,033,130	\$0.122832	19,408,944,303 *	\$272,458,616	-0.25%	-2.34%	-2.58%	***
2241	 Hilux	HLX	\$?	\$0.014386	?	\$?	0.00%	0.00%	12.76%	***
2242	 Stellar Gold	XLMG	\$?	\$0.008425	? *	\$?	0.00%	0.00%	19.61%	***
2243	 Gratz	GRAT	\$?	\$0.003233	? *	\$?	0.00%	0.00%	-99.94%	***
2244	 TRUNK COIN	TRO	\$?	\$0.005912	? *	\$?	0.00%	0.00%	-29.27%	***

coinmarketcap.com (July 2020)

Cryptocurrencies ▾ Exchanges ▾ Watchlist							
Filters USD ▾ Next 100 → View All							
Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$170,068,491,885	\$9,227.43	\$14,035,852,406	18,430,756 BTC	0.12%	
Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
3	 Tether	\$9,206,016,854	\$1.00	\$17,808,525,614	9,187,991,663 USDT *	0.21%	
4	 XRP	\$8,817,362,562	\$0.199227	\$866,195,996	44,257,803,618 XRP *	-0.43%	
5	 Bitcoin Cash	\$4,327,471,022	\$234.42	\$852,186,905	18,459,969 BCH	-0.72%	
6	 Bitcoin SV	\$3,396,585,080	\$184.01	\$991,965,457	18,458,471 BSV	1.34%	
7	 Cardano	\$3,161,400,239	\$0.121934	\$348,226,830	25,927,070,538 ADA	1.28%	
8	 Litecoin	\$2,874,001,045	\$44.21	\$1,599,512,910	65,013,454 LTC	0.06%	
9	 Binance Coin	\$2,822,931,174	\$18.15	\$256,706,012	155,536,713 BNB *	4.64%	
10	 Crypto.com Coin	\$2,620,783,989	\$0.144671	\$59,208,669	18,115,525,114 CRO *	0.83%	
2710	 Egas	\$?	\$0.000437	\$?	? EGAS *	11.07%	
2711	 BTCUP	\$?	\$8.53	\$?	? BTCUP *	0.00%	
2712	 BTCDOWN	\$?	\$11.07	\$?	? BTCDOWN *	0.00%	
2713	 Vether	\$?	\$1.94	\$?	? VETH *	0.00%	

* Not Mineable

← Previous 100 View All

coinmarketcap.com (Oct 5, 2020)

☆ Watchlist

Cryptocurrencies




















Derivatives

DeFi

Storage

Yield Farming

Show rows100Filters

☆ 1	 Bitcoin BTC	\$10,668.33	▲ 1.04%	▼ 2.08%	\$197,450,773,581	\$56,564,904,549 5,302,135 BTC	18,508,131 BTC	
☆ 2	 Ethereum ETH	\$352.33	▲ 1.6%	▼ 1.7%	\$39,769,462,837	\$11,159,572,628 31,673,251 ETH	112,874,230 ETH	
#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	
						\$1,429,204,013 USD		
☆ 4	 XRP XRP	\$0.249611	▲ 7.21%	▲ 1.87%	\$11,273,045,675	\$2,086,205,059 8,357,816,131 XRP	45,162,407,484 XRP	
☆ 5	 Binance Coin BNB	\$29.06	▲ 2.63%	▲ 9.77%	\$4,195,941,050	\$539,545,905 18,568,890 BNB	144,406,560 BNB	
☆ 6	 Bitcoin Cash BCH	\$221.14	▲ 1.01%	▼ 3.29%	\$4,099,056,432	\$1,192,014,290 5,390,286 BCH	18,535,925 BCH	
☆ 7	 Polkadot DOT	\$4.19	▲ 3.58%	▼ 2.97%	\$3,570,655,086	\$301,345,555 71,959,232 DOT	852,647,705 DOT	
☆ 8	 Chainlink LINK	\$9.47	▲ 2.8%	▼ 11.87%	\$3,313,463,869	\$752,326,032 79,467,929 LINK	350,000,000 LINK	
☆ 9	 Cardano ADA	\$0.098568	▲ 6.12%	▼ 4.71%	\$3,066,687,311	\$598,725,378 6,074,252,843 ADA	31,112,484,646 ADA	
☆ 10	 Litecoin LTC	\$46.33	▲ 1.59%	▼ 0.68%	\$3,039,306,365	\$2,178,305,292 47,016,659 LTC	65,600,553 LTC	

- Many altcoins
 - borrow concepts from Bitcoin,
 - often directly forking its code base
 - otherwise adopting some of Bitcoin's code.
- Some make only very minor modifications to Bitcoin
 - changing the value of some parameters of the system,
 - continue to incorporate changes made by Bitcoin's developers.

- All altcoins that we know of
 - begin with a new genesis block
 - their own alternate view of transaction history,
 - (rather than forking Bitcoin's block chain after a certain point in history)
- For our purposes, we don't need a precise definition of an altcoin.
- Instead we'll loosely refer to any cryptocurrency launched since Bitcoin as an altcoin.

- Non-altcoin systems like Ripple and Stellar:
 - these are distributed consensus protocols
- They achieve consensus in a model where
 - nodes have identifiers
 - need to be aware of each other
- Bitcoin is not like that
- Despite other similarities, not Altcoins

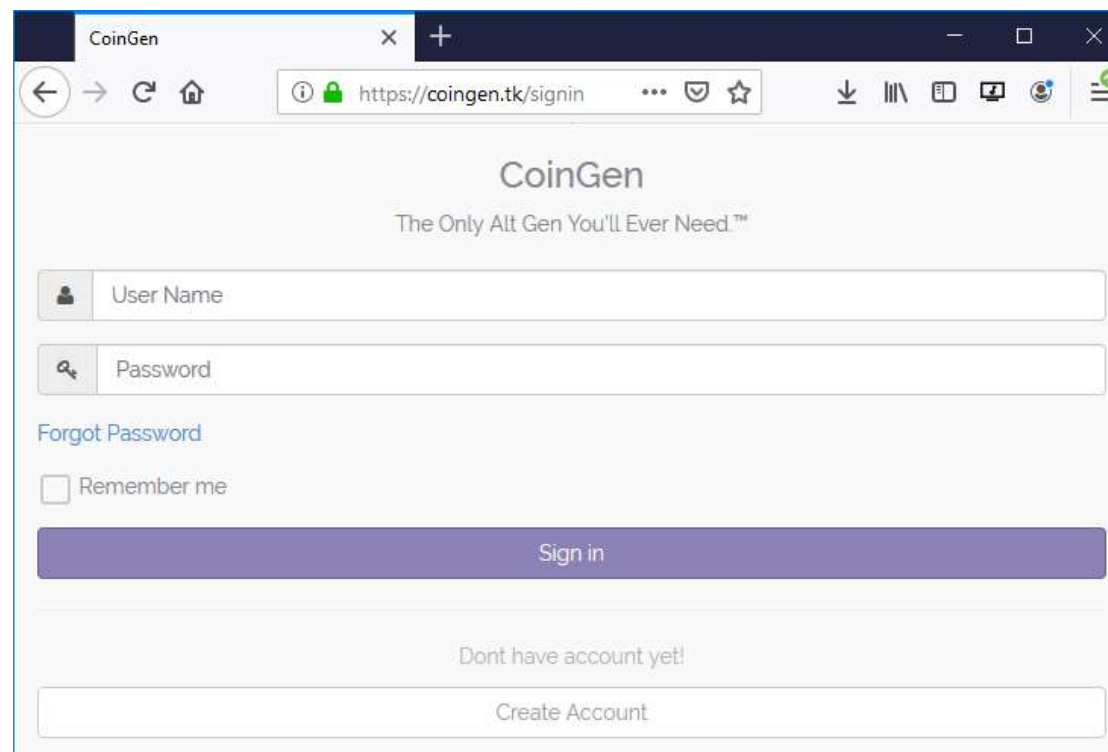
Why launch an altcoin?

- Some kind of story to tell
- Reason to exist:
 - Claim some characteristic that distinguishes it
- Simply change some built-in parameters of Bitcoin.
 - average time between blocks,
 - block size limit,
 - schedule of rewards being created,
 - inflation rate of the altcoin.
- Or give the community special roles

How to launch an altcoin

- Forking existing code base of some existing
- **Easy part:** Add/modify technical features
- Coingen, for a small fee:
 - specify various parameters
 - the proof-of-work algorithm
 - name, currency code, logo.
 - Click to fork&download Bitcoin

- Meet Coingen, the tool that brings out the Satoshi Nakamoto in you



The image shows a web browser window with the title 'CoinGen'. The address bar displays 'https://coingen.tk/signin'. The page content includes the 'CoinGen' logo and the tagline 'The Only Alt Gen You'll Ever Need.™'. There are two input fields: 'User Name' with a person icon and 'Password' with a key icon. Below the password field is a link for 'Forgot Password'. A 'Remember me' checkbox is present. A large purple 'Sign in' button is centered. At the bottom, there is a link 'Dont have account yet!' and a 'Create Account' button.

CoinGen

The Only Alt Gen You'll Ever Need.™

User Name

Password

[Forgot Password](#)

☐ Remember me

Sign in

[Dont have account yet!](#)

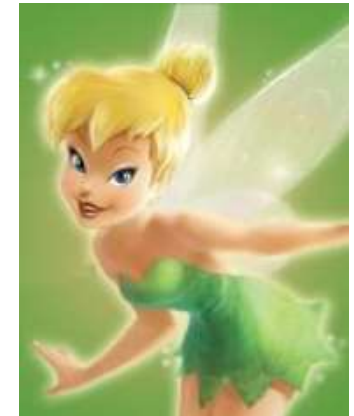
Create Account

- Hard part
- Bootstrapping!
 - Nobody uses your coins
 - Nobody wants 'cos no value
 - No security 'cos no miners
- Need to attract all types stakeholders coin
 - developers, miners, investors,
 - merchants, customers, payment services

- Similar to any other platform
- e.g. a new smartphone operating system, attract
 - users,
 - device manufacturers,
 - app developers
 - various others
- Each of these groups needs the others
- But usually just economic, not security issues
 - No hash power → double spends, forkings..

- No simple recipe for bootstrapping adoption,
- But in general **miners** will come once they believe
 - coinbase rewards they receive
 - will be worth the effort.
- To encourage, many give early miners great rewards.
- Bitcoin, pioneered this approach
- Some altcoins more aggressive

- Basic trick
 - Make people believe it is/will be valuable
 - Need a good story
 - Believers will make others believe



Pump-and-dump scams

- If creator succeed in bootstrapping → Richie Rich \$
- Attractive for everyone, including scams
 - buy up shares of some obscure altcoin,
 - then convince the public of this coin's supposed undiscovered potential ("pump it").
 - If succeed unload their shares and reap a profit ("dump it")
 - They left with \$, many left with no-value coins
- Common in stock market
- Many altcoins:
 - Not real innovation
 - Just "me-too"

Initial allocation

- In Bitcoin, (*new*) coins only through mining
- Some altcoins, for some reasons, initial alloc.
 - “pre-mine”
 - Give incentives to developers to create&bootstrap
 - Allocate to a diverse community
 - Clever way: Give your coins to Bitcoin owners 😊
 - Use proof-of-burn: Gain some altcoin by destroying yours bitcoins

- Here, proof-of-burn, also called
 - One way peg
 - Price ceiling
- Associate 1 altcoin = 1 bitcoin
 - Is actually $1 \text{ altcoin} \leq 1 \text{ bitcoin}$

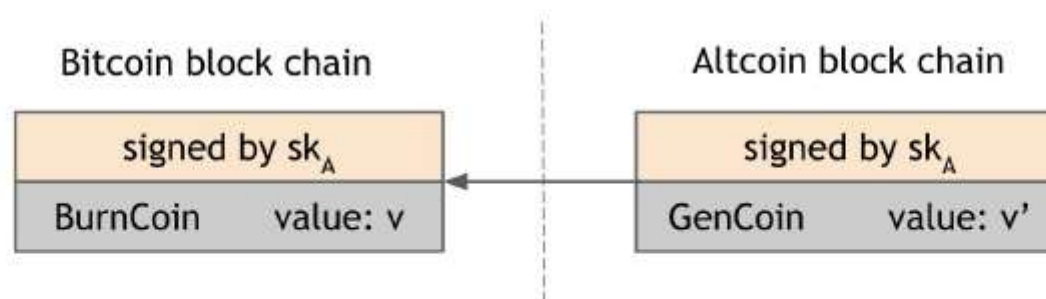


Figure 10.2: Allocating altcoins via proof-of-burn. The altcoin supports a GenCoin transaction that takes a *Bitcoin* transaction as input. GenCoin is signed by the same private key that signed the proof-of-burn (and using the same signature scheme). This ensures that the same user who burned bitcoins also created the GenCoin. If the peg ratio is 1:1, then v' must be no greater than v .

Other ways to increase the diversity of an altcoin

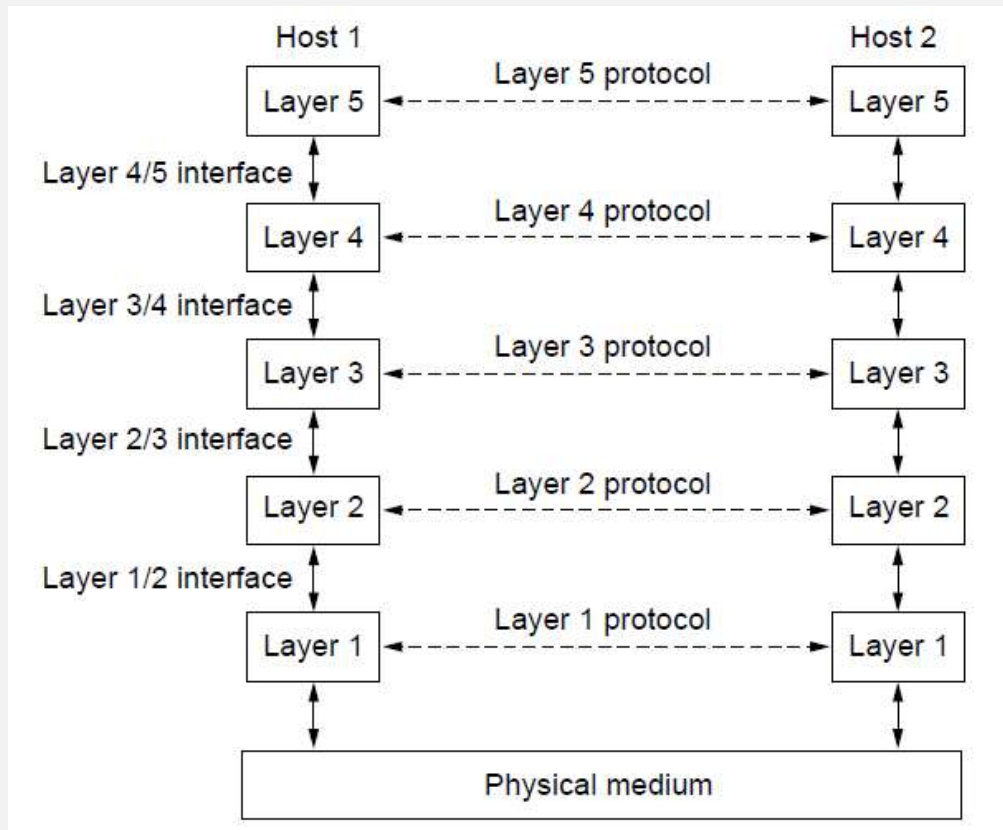
- Tipping
 - Make others hear about your altcoin
 - Require to login (via socialmedia?)
 - Install wallet software etc
- Faucet
 - Give anyone who visits your website/enter e-mail address

Before starting NameCoin:

A quick review of DNS in slides with gray background

From “Introduction to Computer Networking” course

The Application Layer



Uses transport services to build distributed applications

Application
Transport
Network
Link
Physical

DNS – Domain Name System

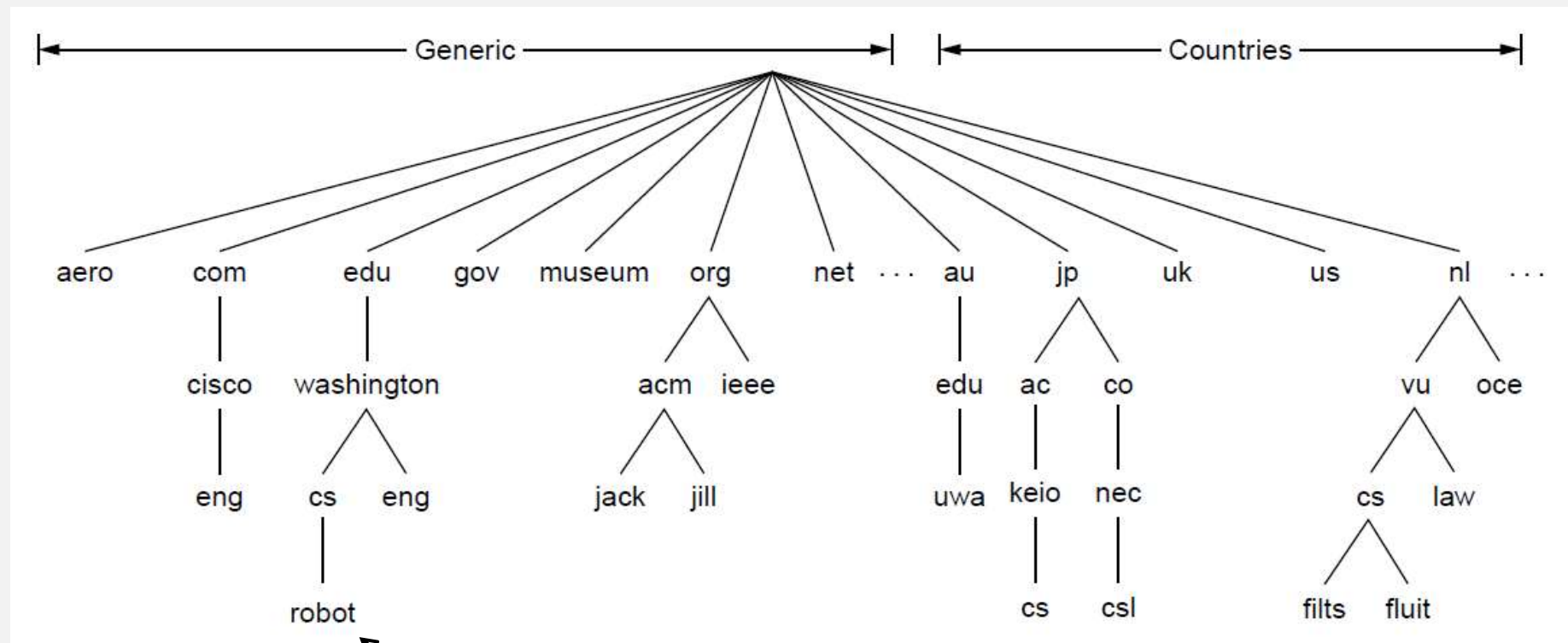
The DNS resolves high-level human readable names for computers to low-level IP addresses

- DNS name space »
- Domain Resource records »
- Name servers »

The DNS Name Space (1)

DNS namespace is hierarchical from the root down

- Different parts delegated to different organizations



The computer *robot.cs.washington.edu*

The DNS Name Space (2)

Generic top-level domains are controlled by ICANN who appoints registrars to run them

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

This one was controversial



Domain Resource Records (1)

The key resource records in the namespace are IP addresses (A/AAAA) and name servers (NS), but there are others too (e.g., MX)

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

Domain Resource Records (2)

; Authoritative data for cs.vu.nl				
cs.vu.nl.	86400	IN	SOA	star boss (9527,7200,7200,241920,86400)
cs.vu.nl.	86400	IN	MX	1 zephyr
cs.vu.nl.	86400	IN	MX	2 top
cs.vu.nl.	86400	IN	NS	star
star	86400	IN	A	130.37.56.205
zephyr	86400	IN	A	130.37.20.10
top	86400	IN	A	130.37.20.11
www	86400	IN	CNAME	star.cs.vu.nl
ftp	86400	IN	CNAME	zephyr.cs.vu.nl
flits	86400	IN	A	130.37.16.112
flits	86400	IN	A	192.31.231.165
flits	86400	IN	MX	1 flits
flits	86400	IN	MX	2 zephyr
flits	86400	IN	MX	3 top
rowboat		IN	A	130.37.56.201
		IN	MX	1 rowboat
		IN	MX	2 zephyr
little-sister		IN	A	130.37.62.23
laserjet		IN	A	192.31.231.216

← Name server

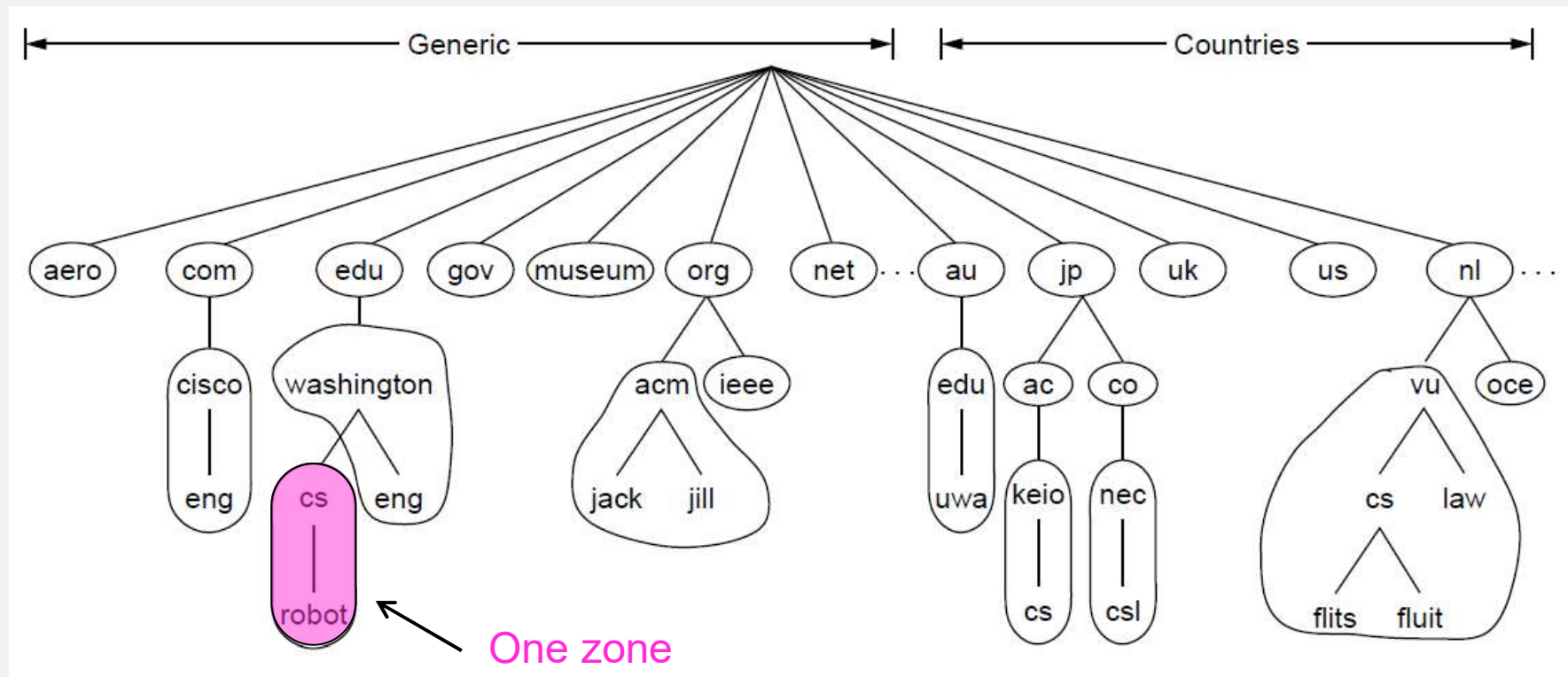
← IP addresses of computers

← Mail gateways

A portion of a possible DNS database for cs.vu.nl.

Name Servers (1)

Name servers contain data for portions of the name space called zones (circled).



Name Servers (2)

Finding the IP address for a given hostname is called resolution and is done with the DNS protocol.

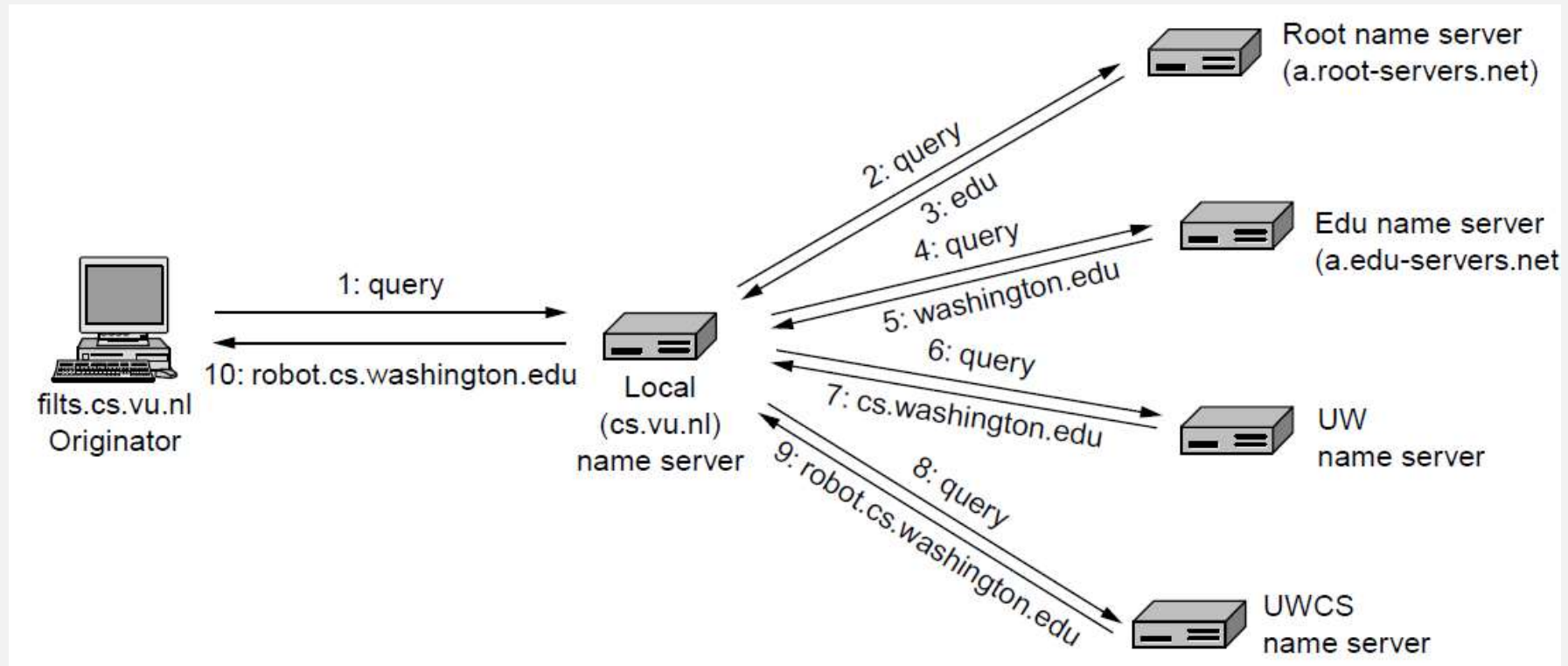
Resolution:

- Computer requests local name server to resolve
- Local name server asks the root name server
- Root returns the name server for a lower zone
- Continue down zones until name server can answer

DNS protocol:

- Runs on UDP port 53, retransmits lost messages
- Caches name server answers for better performance

Name Servers (3)



Example of a computer looking up the IP for a name

Namecoin '2011

- Bitcoin:
 - Secure global network
 - Tamper-proof (append-only-log)
 - Can't we use it for another app
 - e.g. Naming system? Decentralizing DNS

Namecoin: Rules

- View data entries as name/value pairs
 - names being globally unique
 - everyone allowed to look up the value mapped to a name
 - If name/value pair has the same name as a previous database entry → view it as an update
- Only the initial creator of the entry can update
 - associate each name with a Bitcoin address
 - update transactions to be signed by the p_k for that address.

Namecoin cont'

- It can be built on Bitcoin: Overlay currency
- Simpler to do in an altcoin
 - Write these rules as the altcoin's rules
 - So, rather than checking by each user,
 - Enforced by miners
- Global name/value store: Users can
 - define one or more names (fees applied)
 - transfer the control
 - Transfer the domain from A to B & Namecoins from B to A

Namecoin cont'

- DNS: {Name, Value} pair
 - Names: Domains
 - Values: IP's
- Browser plug-in
 - example.bit
 - Searches in namecoin registry, not DNS
- Interesting, technically & historically
- Against centralization of DNS
- Used mostly by “squatters” (buy lots of and then sell)

Litecoin '2011

- Most popular altcoin for years
- Most forked codebase
 - Even more than Bitcoin
- Basic distinction between Bitcoin
 - Memory-hard mining puzzle
- When Litecoin launched, Bitcoin was in GPU era
 - Was able to mine Litecoin with CPU (so, GPU-resistant)
 - Eventually GPU → FPGA → ASIC
 - Transition took longer than Bitcoin, why?
 - Just the hard puzzle, or the exchange rate?

Litecoin cont'

- So, it failed
 - But the idea for a “more” decentralized CC
 - Worked for bootstrapping!
-
- Only a few small differences from Bitcoin
 - Mining a block in each 2.5 mins
 - Followed & adapted Bitcoin's modifications

Proof-of-Stake and Virtual Mining



- Why not simply allocate mining “power” directly to all currency holders in proportion to how much currency they actually hold?



Advantages

- Remove wasteful right half → Environment
- No ASIC, No AR → Centralization
- CC's value → Miners tend to behave good

Implementing Virtual Mining

- Not
 - researched scientifically
 - analyzed practically
 - (Bitcoin is too dominant)
- Peercoin (2012)
 - Hybrid: proof-of-work & proof-of-stake
 - Coin-age, coin-stake: solving & adjusting difficulty

Peercoin '2012, vs. Oct 2020


341	 Peercoin	PPC	\$10,182,880	\$0.400338	25,435,700	\$256,700	-0.59%	-3.66%	0.44%	***
588	 Peercoin	PPC		\$0.235893	▲ 10.45%	▼ 8.97%	\$6,257,543		\$30,099.55	127,598 PPC

- First proof-of-stake altcoin
- One more interesting aspect
 - Admins kept a trusted public key as a safeguard
 - Destroyed decentralization!
 - It can be removed
 - But it is there! So, proof-of-stake did not work
 - Will it work if safeguard removed?

Dogecoin '2013



- CTRL-F “Doge”: 8 matches

30  **Dogecoin** DOGE \$377,797,911 \$0.003148 120,003,321,307 \$33,868,429 -0.27% 0.57% 3.12% ...

- Close fork of Litecoin → Technically not interesting
- Interesting community values
 - tipping,
 - generosity,
 - not taking cryptocurrency so seriously

Dogecoin '2013



- Named after Doge,
 - an Internet meme
 - featuring a grammatically-challenged Shiba Inu dog
- several interesting & successful marketing campaigns
 - Sponsored a NASCAR driver
 - raised over \$30,000 to support the Jamaica National Bobsled Team in 2014 Winter Olympics
- Bootstrapping could be successful with a non-technical narrative

Relationship Between Bitcoin and Altcoins

- Market capitalization:
 - Traditionally: price of a share * total number of shares
 - Altcoins: price of a coin * total number of coins
 - Bitcoin: %90 of the market!
 - Not the most important thing
 - Interpretation difficult: Exchange rate, future, new coins
 - Some coins may be lost → not in circulation

Relationship Between Bitcoin and Altcoins

- Mining Power:
 - If two altcoins using the same puzzle
 - Compare the hash rate
 - Zetacoin, same puzzle with Bitcoin
 - Hash rate was 1/100K of Bitcoin
 - Not only the current hash rate but its change by time
 - This way, we can compare coins with different puzzles

Relationship Between Bitcoin and Altcoins

- Other indicators:
 - Change in the exchange rate by time
 - In the long run, it is related to change in hash rate
 - Exchange volume with third parties
 - Not the transaction volume; why?
 - Number and size of the merchants and payment systems

Relationship Between Bitcoin and Altcoins

- “Network effect”
 - If there are two similar options, only one will win
 - May, or may not be technically superior
 - e.g. Blue-ray vs. HD-DVD
 - Bitcoin dominates (despite technically superiors)
 - But not as simple as disc formats!
 - Low Switching Cost
 - Various features, some even complementary → supports
 - Again over simplification. What is the value, risks, updates

Merge Mining

- Bitcoin's hash power of miners so big
 - Even more than all the power of altcoins
 - Altcoin Infanticide
 - They can attack?
 - Why? No gain?
-
- 2012, Eligius (bitcoin mining pool) decided that CoiledCoin is a scam.
 - They attacked and destroyed it

Merge Mining

- If an altcoin just forks from Bitcoin (no change)
- Mining power can be allocated to a single coin
- Bootstrapping problem
- Merging the mining?
- Design the altcoin
- Place some info to Bitcoin blocks (technical)
- Drawback: too slow. Solution?

Adjust your altcoin's mining target

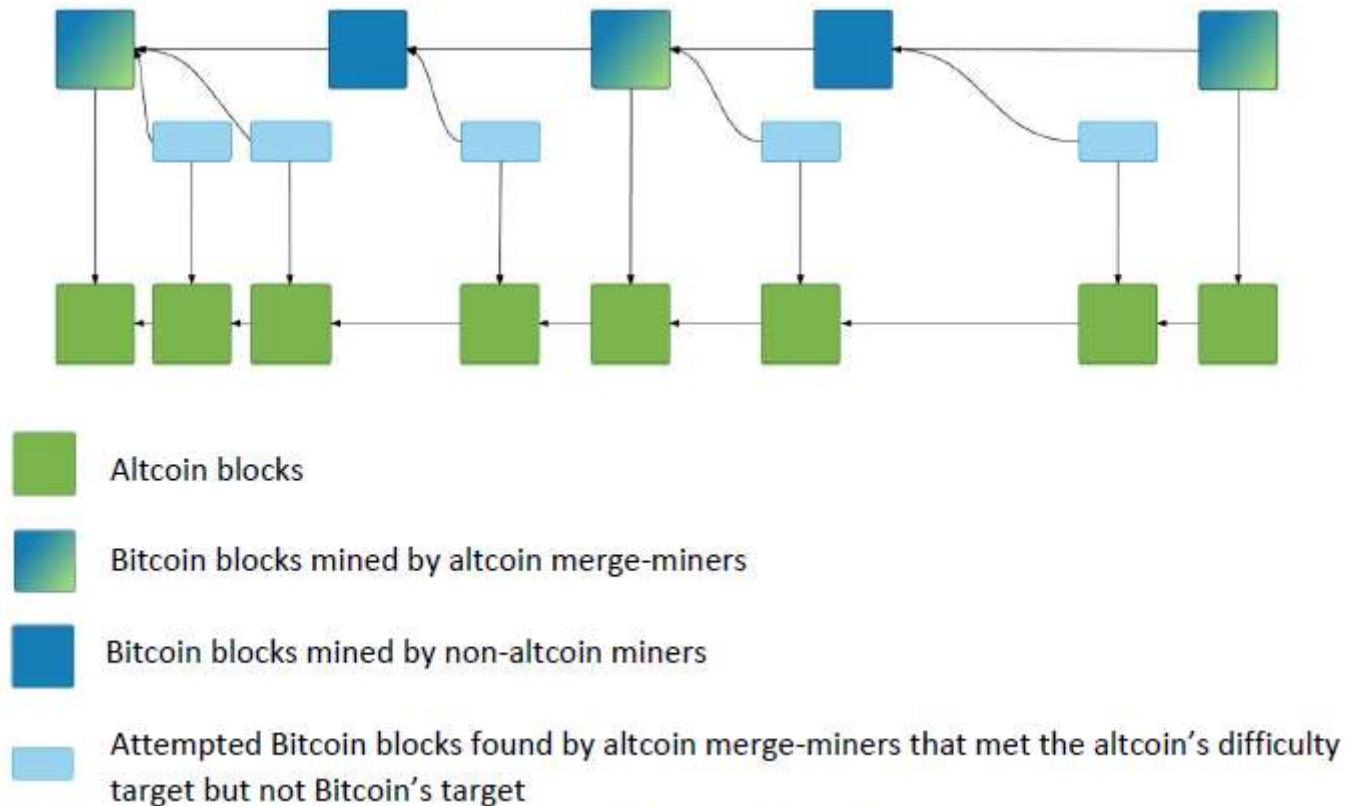


Figure 10.5: merge mining.

- Merge mining & Security
- Altcoin got some mining power of Bitcoin
- Huge investment required to attack altcoin
- Not really
- Eligius was a merge-mining!
- Complicated,
- Not clear whether merging is a good idea!

Bitcoin Scripts

- Script Language built specifically for Bitcoin, called “Script”
 - Stack-based
 - Simple & Compact
 - Native support for cryptographic operations
 - Compute Hash functions
 - Compute signatures
 - Verify signatures

Script

- Stack-based
 - Each instruction executed once
 - No loops
 - Number of instructions
 - How long it can take
 - How much memory it can use
 - Not Turing-complete, by design!
 - Arbitrary miners can't submit infinite-loops

```
for i in range(0,10,2):  
    print i
```

```
0  
2  
4  
6  
8
```

- Only two possible outcomes:
 - Execute normally with no errors → Valid,
 - Error → Invalid transaction
- Each instruction represented by 1 Byte
 - 256 in total ($2^8=256$)
 - 15 disabled, 75 reserved (to be added later)

Ethereum & Smart Contracts

- Bitcoin: “Turing-incomplete”
- More apps
- Instead of a new altcoin for each app
- Why not make a Turing-complete coin?
- Ethereum: Provides TC programming language

Ethereum & Applications

- Namecoin

```
contract NameRegistry {  
    mapping(bytes32 => address) public registryTable;  
    function claimName(bytes32 name) {  
        if (msg.value < 10) {  
            throw;  
        }  
        if (registryTable[name] == 0) {  
            registryTable[name] = msg.sender;  
        }  
    }  
}
```

Figure 10.8: A simple Ethereum smart contract implementing a name registry.

Ethereum

- A contract: A program that lives on the blockchain
- Anybody can create an Ethereum contract, for a small fee,
 - by uploading its program code in a special transaction.
- This contract is
 - written in bytecode
 - executed by a special Ethereum-specific virtual machine: EVM
- Once uploaded, the contract will live on the blockchain.
 - It has its own balance of funds,
 - Other users can make procedure calls through API
 - The contract can send and receive money.

Ethereum

- Turing Completeness allows loops $\rightarrow \infty$ loops!
- Contracts may run forever!
- A way to check whether a program runs forever?
 - No! (the undecidability of the Halting Problem)
- How to prevent:
 - Define “GAS”
 - Each VM instruction runs for some fee (gas)

- Basic operations (addition, comparison): 1 gas,
- Computing a SHA-3 hash: 20 gas
- Writing a 256-bit word to storage: 100 gas
- Transaction: 21,000 gas
- These prices are fixed.
 - Modifying → Forking
- Like a cheap airline: You pay for everything ;)

- Gas
 - paid to execute contracts
 - paid to use “ether”, the currency
- Every transaction can specify how much gas
- Miners are free to choose any transaction
 - A free market
- Every call specifies how much gas to spend
 - When run out of gas, execution halts

- Each computation instruction costs some gas
- Not suitable for large computations
 - Use clouds instead; Amazon's Computing Cloud
- Suitable to implement security logic
 - Allows many parties to count on to behave
- Its security too complex, not as Bitcoin
 - Difficult to analyze
- Rewarding complex, not clear
 - It goes to who includes the transaction, not to miners

Chess in Ethereum

- Alice and Bob live in different countries
- Neither trusts each other to pay if they lose
- Ethereum can solve this!
- Alice
 - Writes a chess program, uploads to Ethereum
 - Bets some money (sends a contract with some ether)
- Bob
 - Should be sure that contract works
 - Bets money

Chess in Ethereum

- Once both bet, game starts
 - No one can take the money without winning
- Playing
 - Send transactions to the contract: Moves
- Contract must
 - ensure, play only in order,
 - check the rules for each move
 - End the game. Win, draw; send the ether

Chess in Ethereum

- What if the loser stops playing?
 - Contract gives the ether to other after some time
- Who moves first?
 - White more advantageous.
 - No randomness source
 - Randomness beacons?
 - Use some Hash? (Convince only A&B, not whole world)

Other Applications

- Chess is fun, but real life:
 - Smartcontracts
 - Escrowed payments
 - Micropayments
 - Mixing services
 - Auctions
- Ledger
 - Bitcoin: Transaction-based
 - Ethereum: Account-based