7CCSMDLC: Distributed Ledgers & Cryptocurrencies

Lecture 3: Mining

Peter McBurney
Professor of Computer Science
Department of Informatics
King's College London

Email: peter.mcburney@kcl.ac.uk
Bush House Central Block North – Office 7.15

2021

Outline

Operation of the Bitcoin Blockchain

- Transactions
- Mining and Proof-of-Work
- Reaching Consensus over blocks

Operation of the Bitcoin Blockchain

Transactions

Transaction Outputs

For most transaction, there are two parts:

- An amount of Bitcoin (denominated in satoshis)
- A locking script (an “encumbrance”)
  - The amount is locked unless specific conditions are met

The intended recipient has to provide something to redeem the payment

- Typically they provide their signature (which encodes their private key) and a hash of their public key (their Bitcoin address)
- They may also provide their signature (which encodes their private key) and a hash of a script (a program written in the Bitcoin language Script).
- Some transactions require multiple parties to provide something before the locking script is unlocked.

UTXO

- **Unspent Transaction Output (UTXO)** is the output of a transaction which may be spent as an input in a subsequent transaction.
- “Sending” a recipient some bitcoin is done by creating some UTXO registered to their address
  - Encumbered to their public key hash or to a script
- All the UTXO of the system is known by every node
  - It is held in a database called the **UTXO set** or **UTXO pool**.
- It is locked to a specific address and may be scattered.
- A wallet will aggregate the UTXO belonging to a single address.

The 5 Standard Transactions

These are based on what is needed to redeem the payment
(ie, to satisfy the encumbrance)

- Pay-to-Public-Key-Hash (P2PKH)
  - A hash of a specific public key (a Bitcoin address) is needed to redeem
- Pay-to-Public-Key
  - Mostly used in coinbase transactions
- Multi-sig (multiple-signature)
  - Limited to 15 keys
  - M of N schemes (ie, M signatures of N total signatures are needed, eg 2/3).
- Pay-to-Script-Hash (P2SH)
- Data Output
  - 40 bytes of non-payment data to a Transaction output.

Mining & Consensus

Four parts of decentralized consensus

Step A Independent verification of each transaction, by every full node

Step B Independent aggregation of those transactions into new blocks by mining nodes, together with demonstrated computation through a Proof-of-Work algorithm

Step C Independent verification of the new blocks by every node and assembly into a chain

Step D Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work.

A: Independent verification of transactions

Each node checks against the following list of criteria:

- The transaction's syntax and data structure is correct.
- Neither lists of inputs or outputs are empty.
- The transaction size in bytes is less than MAX_BLOCK_SIZE.
- Each output value, as well as the total, is within the allowed range of values
- None of the inputs have hash=0, N=–1 (coinbase transactions should not be relayed)
- nLocktime is equal to INT_MAX, or nLocktime and nSequence values are satisfied according to MedianTimePast.
- The transaction size in bytes is greater than or equal to 100.
- The number of signature operations (SIGOPS) contained in the transaction is less than the signature operation limit.
- The unlocking script can only push numbers on the stack, and the locking script must match isStandard forms.
- A matching transaction in the pool, or in a block in the main branch, must exist.
- For each input, if the referenced output exists in any other transaction in the pool, the transaction is rejected.
- For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions pool, if a matching transaction is not already in the pool.
- For each input, if the referenced output transaction is a coinbase output, it must have at least COINBASE_MATURITY confirmations.
- For each input, the referenced output must exist and cannot already be spent.
- Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in the allowed range of values (less than 21m coins, more than 0).
- Reject if the sum of input values is less than sum of output values.
- Reject if transaction fee would be too low (minRelayTxFee) to get into an empty block.
- The unlocking scripts for each input must validate against the corresponding output locking scripts.

B: Aggregation TXs into Blocks & Mining

Mining new bitcoin

- New bitcoin are created during the creation of each block at a fixed and diminishing rate, approx. every 10 minutes.

- Every 210,000 blocks (ca. four years), the currency issuance rate is decreased by 50%
  - 2009-2012: 50 new bitcoin earnt per block
  - November 2012: 25 new bitcoin per block
  - July 2016: 12.5 bitcoin per block
  - May 2020: 6.25 bitcoin per block at block 630,000
  - ca. 2137: 1 satoshi per block (block 6,720,000) (99% of all BTC)
  - ca. 2140: After 6.93 million blocks a total of almost 2,099,999,997,690,000 satoshis (almost 21 million bitcoin).

- After that, payment to miners will only be via transaction fees.

- See Block 630,000 here:

  https://blockchair.com/bitcoin/block/630000

Bitcoin / Block / 629999 — Block

https://blockchair.com/bitcoin/block/629999

BLOCKCHAIR

Search in 17 blockchains (BTC/ETH/XRP/LTC/BCH/ADA/XLM/BSV/EOS/XMR/XTZ/DASH/ZEC/DOGE/BCHA/XIN/...

English

Bitcoin > Block > 629999

Get 100 Spins | Buy Crypto | Catch your luck | Earn Crypto

General info

629998 — **629999** — 630000

Hash	0000000000000000000d656be18bb095db1b23bd797266b0ac3ba720b1962b1e
Mined on	2020-05-11 19:23 (9 months ago)
Miner	F2Pool
Coinbase data	NYTimes 09/Apr/2020 With $2.3T Injection, Fed's Plan Far Exceeds

USD BTC

Transaction count	2,481	Fee per kB	0.00074808 BTC
Witness tx count	1,528	Fee per kWU	0.00026740 BTC
Input count	6,286	Output count	8,214
Input total	11,358.76469643 BTC	Output total	11,371.26469643 BTC
Fee total	1.06876397 BTC	Coindays destroyed	653,689.02
Generation	12.50000000 BTC	Reward	13.56876397 BTC

Technical details

Difficulty	16104807485529
Size	1,429,136
Weight (weight units)	3,998,681
Stripped size	856,515
Version	671080448_{10} $27ffe000_{16}$
Version [bits]	$10011111111111111000000000000000_2$
Median time	2020-05-11 18:16:54
Merkle root	f4 … 0f
For developers	API docs
Alternative explorers	

Click to see more

Transactions included in this block

Type here to search

ENG 20:55 28/01/2021

Bitcoin / Block / 630000 — Block

https://blockchair.com/bitcoin/block/630000

BLOCKCHAIR

Search in 17 blockchains (BTC/ETH/XRP/LTC/BCH/ADA/XLM/BSV/EOS/XMR/XTZ/DASH/ZEC/DOGE/BCHA/XIN/...

English

Bitcoin > Block > 630000

Get 100 Spins | Buy Crypto | Catch your luck | Earn Crypto

General info

629999 — **630000** — 630001

Hash	0000000000000000000024bead8df69990852c202db0e0097c1a12ea637d7e96d		
Mined on	2020-05-11 19:23 (9 months ago)	Miner	AntPool
Coinbase data	??? ?Mined by AntPool119⊕o		

USD BTC

Transaction count	3,134	Fee per kB	0.00076666 BTC
Witness tx count	720	Fee per kWU	0.00022789 BTC
Input count	5,494	Output count	7,160
Input total	3,312.53112406 BTC	Output total	3,318.78112406 BTC
Fee total	0.90968084 BTC	Coindays destroyed	6,836.56
Generation	6.25000000 BTC	Reward	7.15968084 BTC

Technical details

Difficulty	16104807485529
Size	1,186,930
Weight (weight units)	3,993,250
Stripped size	935,440
Version	536870912_{10} 20000000_{16}
Version [bits]	$10000000000000000000000000000000_{2}$
Median time	2020-05-11 18:28:39
Merkle root	b1 0d
For developers	API docs
Alternative explorers	

Click to see more

Transactions included in this block

Type here to search

ENG 20:56 28/01/2021

Reward for mining is new Bitcoin

The Generation Transaction (Coinbase reward)

- The bitcoin earnt by mining are awarded via the first transaction of each new block
  - The Generation (or Coinbase) transaction

- There are no UTXO inputs for these transactions

- Generation transactions do not have an unlocking script (since there is no UTXO). So the field can have arbitrary content:
  - Eg, Satoshi Nakamoto on 03-01-2009 added to the genesis block:

  “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”.

  See the Bitcoin Genesis Block (Block #0) here:

  https://blockchair.com/bitcoin/block/0

Bitcoin / Block / 0 — Blockchair

https://blockchair.com/bitcoin/block/0

BLOCKCHAIR

Search in 17 blockchains (BTC/ETH/XRP/LTC/BCH/ADA/XLM/BSV/EOS/XMR/XTZ/DASH/ZEC/DOGE/BCHA/XIN/...

English

Bitcoin > Block > 0

Get 100 Spins | Buy Crypto | Catch your luck | Earn Crypto

General info

0

1

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Mined on	2009-01-03 18:15 (12 years ago)
Miner	Unknown
Coinbase data	??????EThe Times 03/Jan/2009 Chancellor on brink of second bailout for

USD BTC

Transaction count	1	Fee per kB	0.00000000 BTC
Witness tx count	0	Fee per kWU	0.00000000 BTC
Input count	1	Output count	1
Input total	0.00000000 BTC	Output total	50.00000000 BTC
Fee total	0.00000000 BTC	Coindays destroyed	0.00
Generation	50.00000000 BTC	Reward	50.00000000 BTC

Technical details

Difficulty	1
Size	285
Weight (weight units)	1,140
Stripped size	285
Version	1_{10} 1_{16}
Version [bits]	$00000000000000000000000000001_2$
Median time	2009-01-03 18:15:05
Merkle root	4a 3b
For developers	API docs
Alternative explorers	BTC

Click to see more

Transactions included in this block

Type here to search

ENG 12:52 28/01/2021

Format for the Block Header

Size	Field	Description
4 bytes	Version	Software/protocol version
32 bytes	Previous Block Hash	Reference to previous (parent) block
32 bytes	Merkle Root	Hash of root of merkle tree of the transactions in this block
4 bytes	Timestamp	Creation time of block (seconds from Unix Epoch)
4 bytes	Target	Proof-of-Work algorithm target for this block
4 bytes	Nonce	Counter used for Proof-of-Work algorithm

Mining problem

- Proof-of-Work is designed to create a hurdle to mining
  - Otherwise, nodes would spin-up multiple sock-puppet nodes to win the reward
  - A form of Sybil attack
- The problems get harder over time
  - To ensure that a new block is created and accepted about every 10 minutes.
- Problem: Find the hash a specified object with a nonce parameter which is less than sum pre-specified total.
  - Problem designed to be hard to do and easy to check.
  - Can only be solved by trial and error.

Two die example

When throwing two die (dices), how many possible outcomes are there when the total is less than a specified number?

- How many outcomes less than 12 in total
- How many outcomes less than 11 in total
- How many outcomes less than 10 in total

. . . . . .

- How many outcomes less than 3 in total?
- How many outcomes less than 2 in total?
- How many outcomes less than 1 in total?

Sum of two dice throws

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

How many outcomes less than 12 in total: 35 out of 36

How many outcomes less than 11 in total: 33 out of 36

How many outcomes less than 10 in total: 30 out of 36

How many outcomes less than 9 in total: 26 out of 36

. . . . .

How many outcomes less than 3 in total: 1 out of 36

Example of iterating nonce parameter

I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...

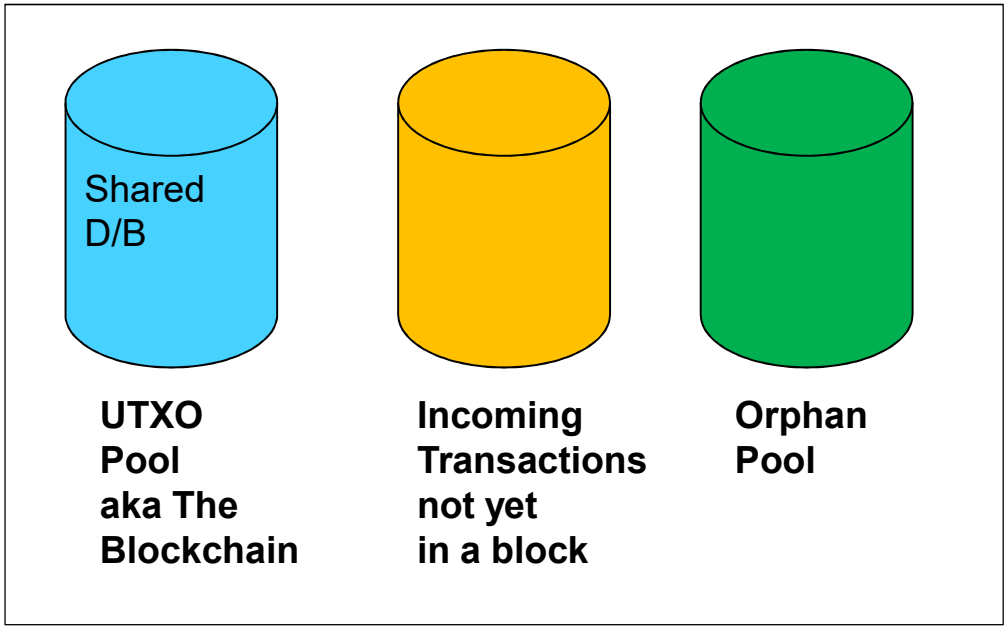
Intending miners

- When a new block arrives, miners tackle the next PoW problem
- Meanwhile, they assemble transactions that are not in a block into a candidate block
  - Prioritized by age (how many blocks since the UTXO was recorded) &
  - Size of transaction

- High priority:
  - 1 Bitcoin, aged 1 day

- As new blocks added, unused TXs increase in age

- When miner is restarted, its TX pool is wiped.



Four parts of decentalized consensus: C & D

Step C: Independent verification of the new blocks by every node and assembly into a chain

Step D: Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work.

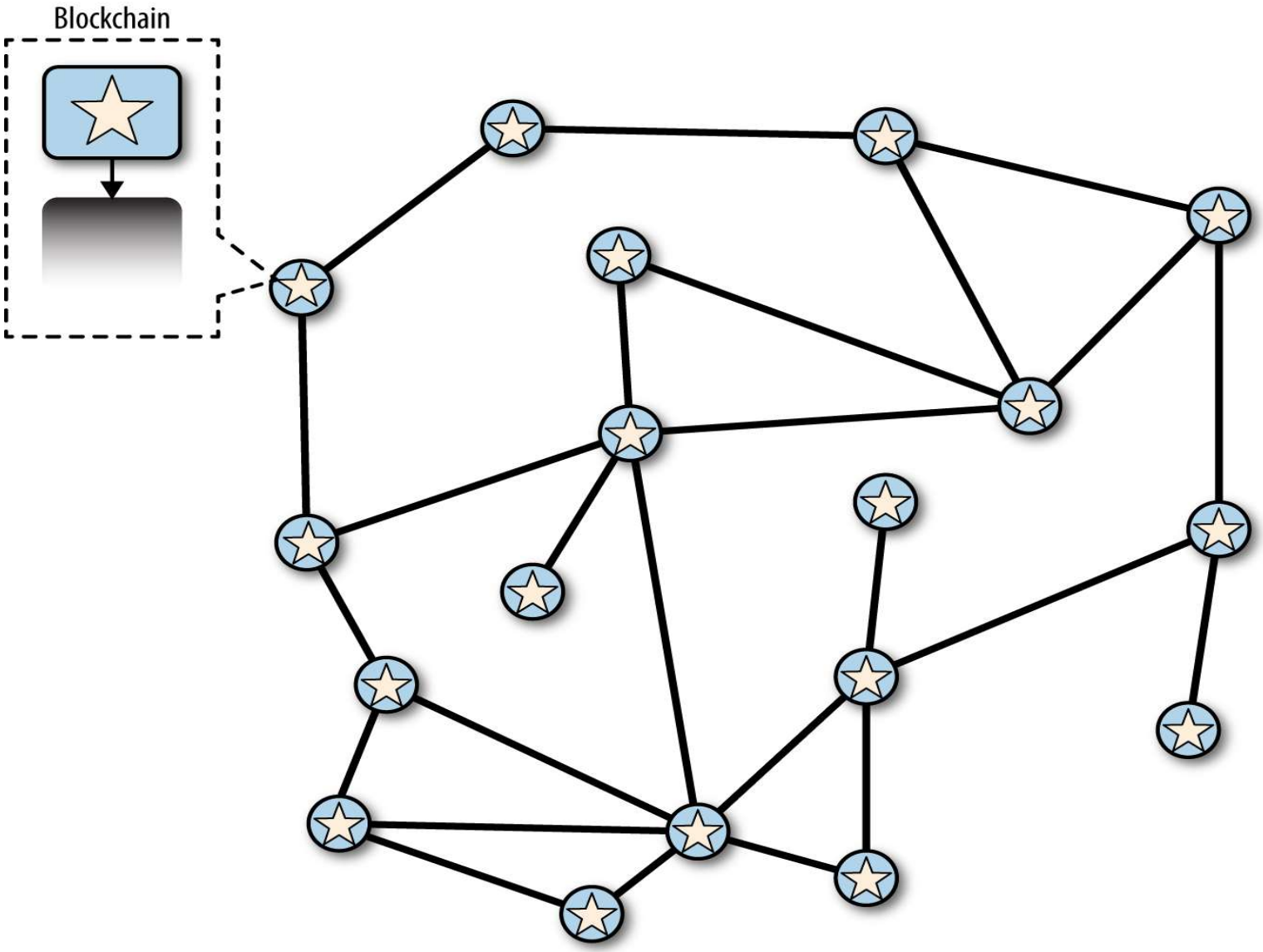
- We can reference blocks by their height (currently about 669,000), or the hash of their header.
  - Block height may not be unique (if there is a fork).
- Block hash is not stored within the block
  - It is calculated by each node as the block is received.

Validating a new block

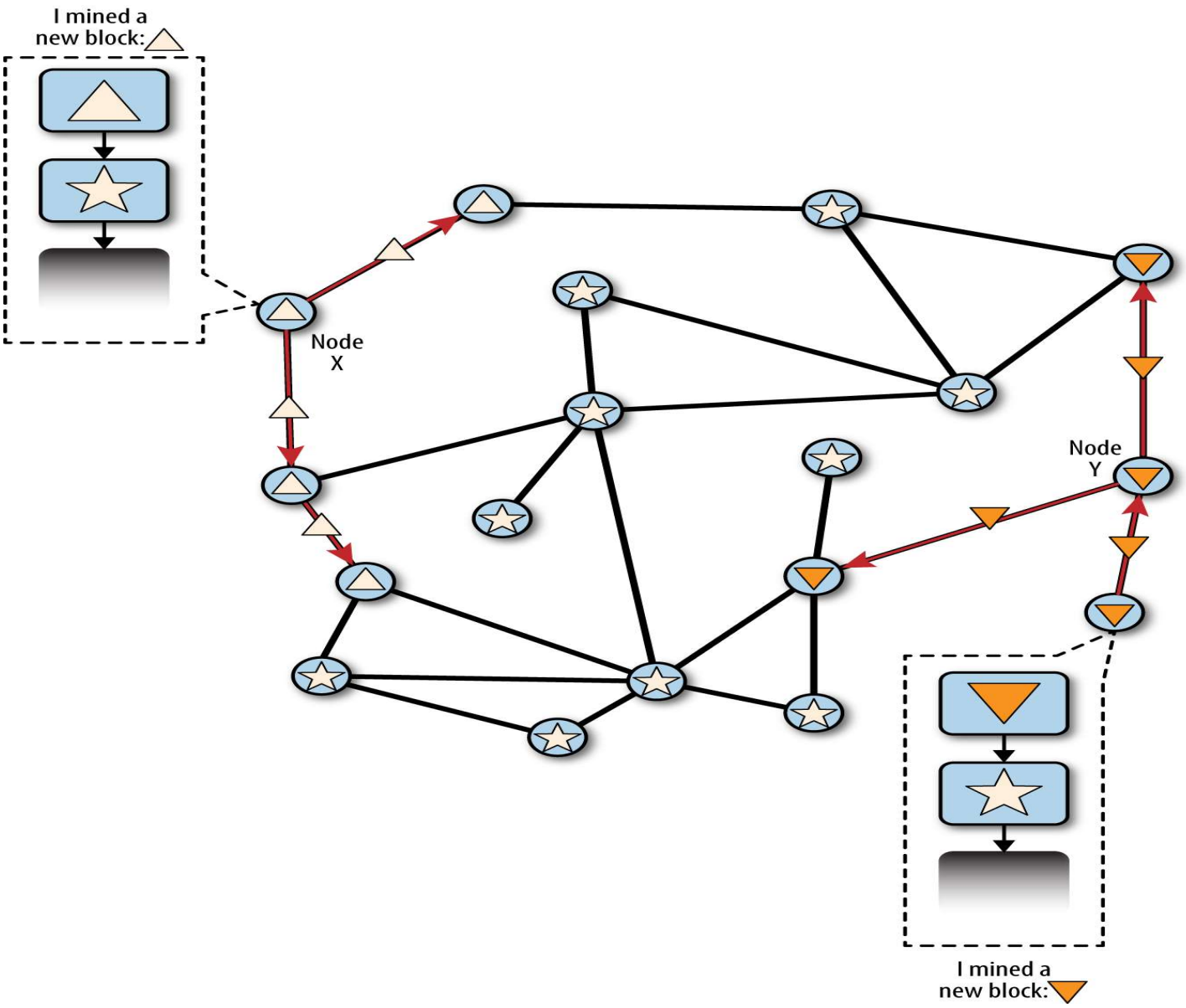
Criteria for validation include:

- The block data structure is syntactically valid (ie, format is correct)
- The block header hash is less than the target (enforces Proof-of-Work)
- The block timestamp is less than two hours in the future (allowing for time errors)
- The block size is within acceptable limits
- The first transaction (and only the first) is a coinbase transaction
- All transactions within the block are valid using the transaction checklist for Independent Verification of Transactions.

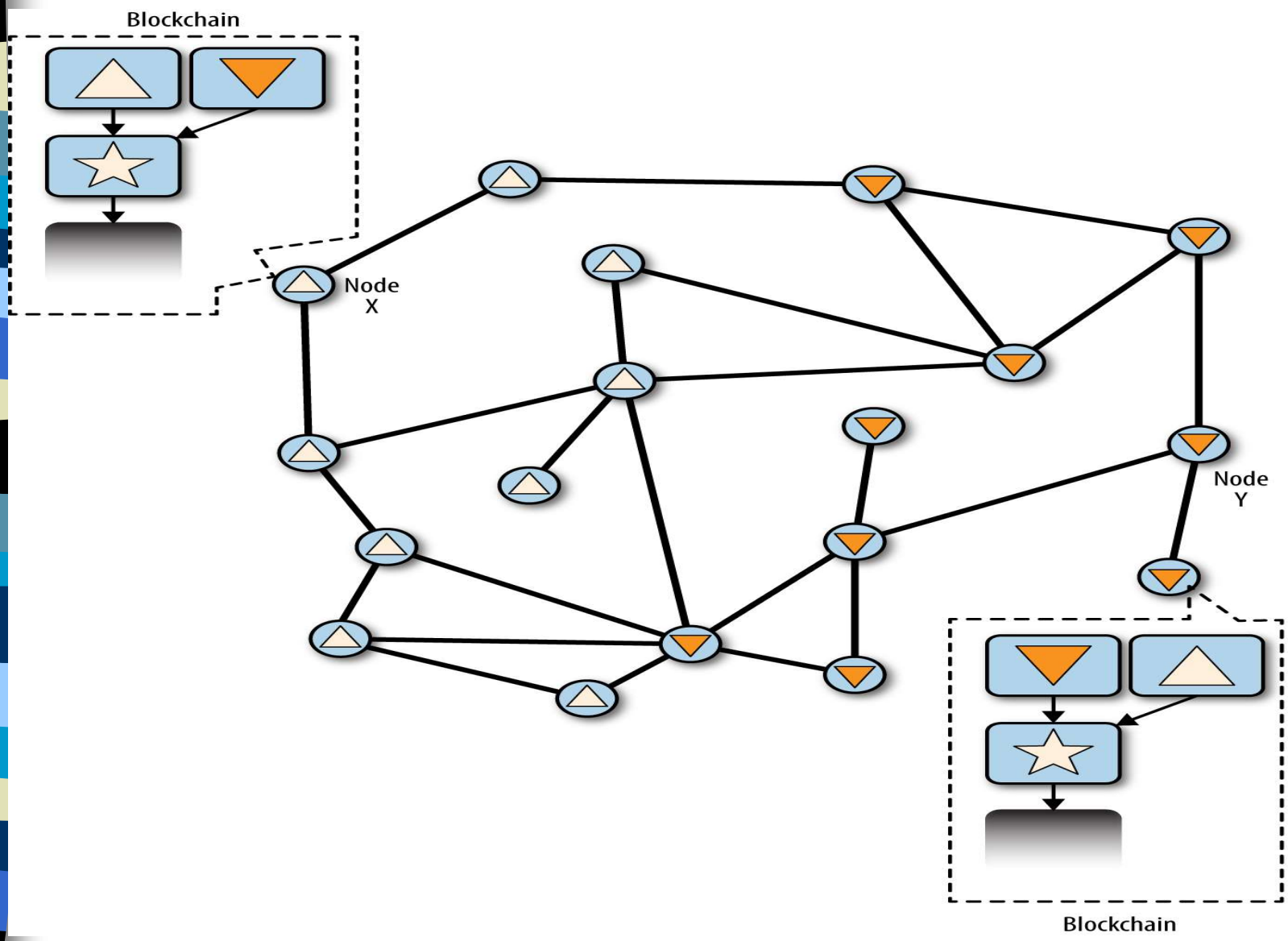
Blockchain assumes a peer-to-peer (P2P) network
No one is in control.



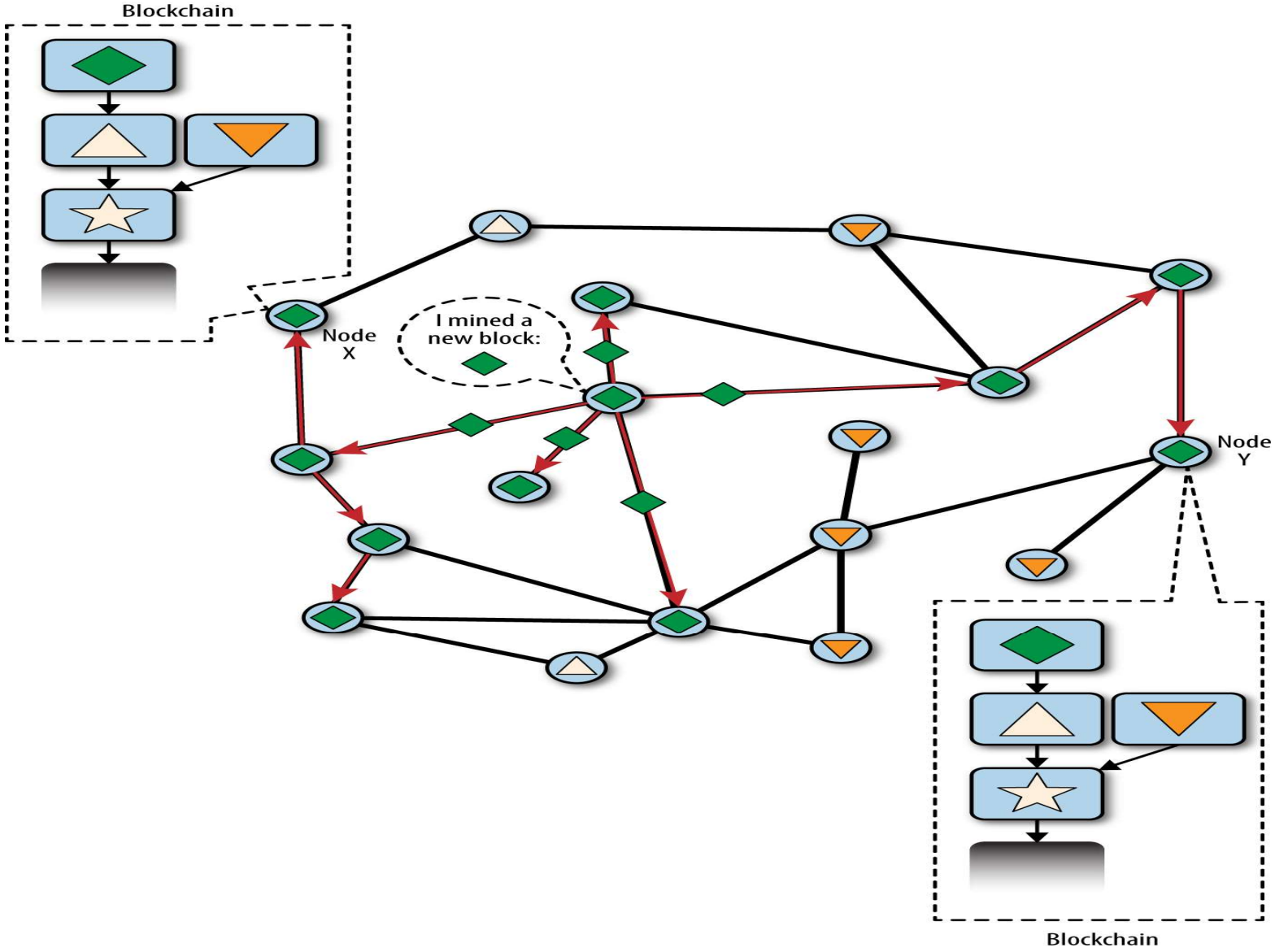
Nodes mine blocks and propagate them locally



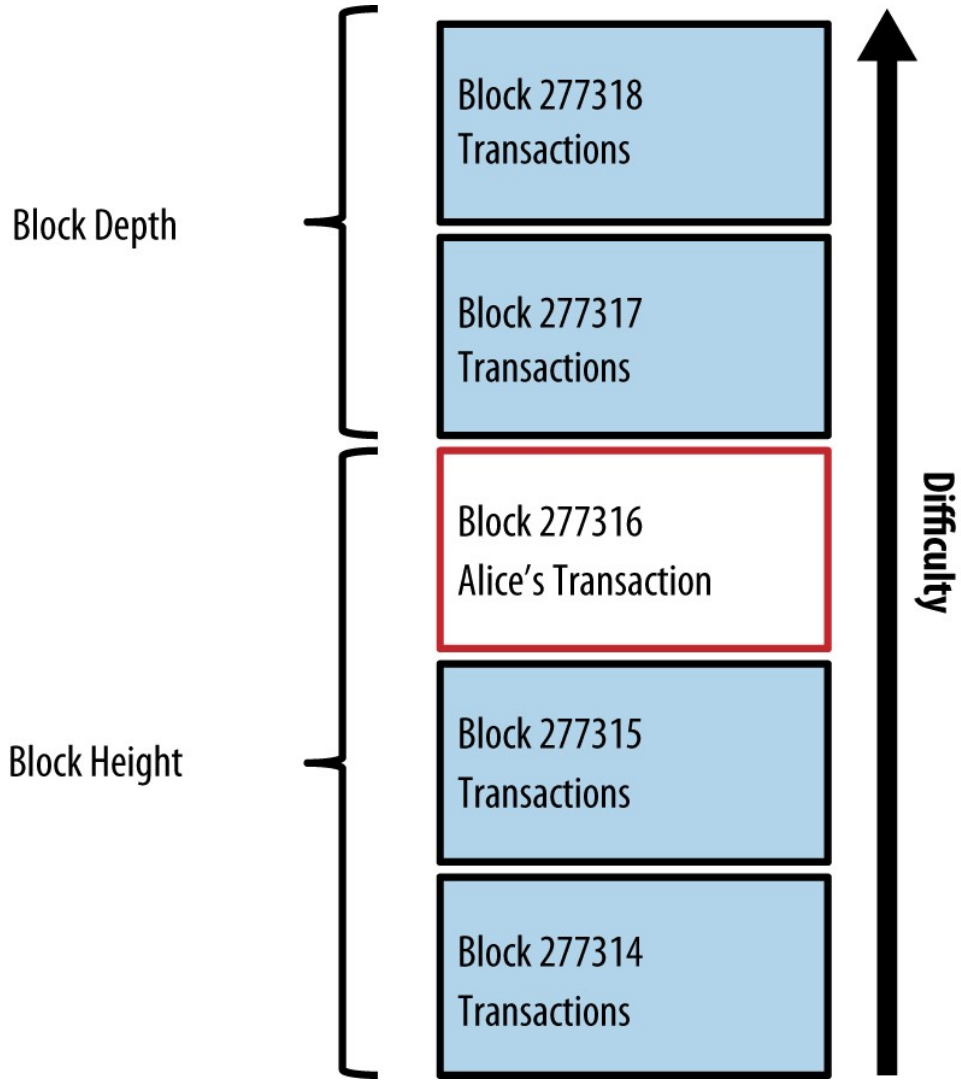
Competing new blocks from different miners



Which chain is “longer” (contains more work)?



Block height currently is about 669,000



https://blockchain.info/q/getblockcount

Bitcoin / Block / 668042 — Block | New tab

https://blockchair.com/bitcoin/block/668042

BLOCKCHAIR | Search in 17 blockchains (BTC/ETH/XRP/LTC/BCH/ADA/XLM/BSV/EOS/XMR/XTZ/DASH/ZEC/DOGE/BCHA/XIN/... | English

Bitcoin > Block > 668042

Get 100 Spins | Buy Crypto | Catch your luck | Earn Crypto

General info

668041 — **668042** — 668043

Hash	0000000000000000000006f1ff3092d43c50db0316686155b049b6aef785d5885f
Mined on	2021-01-28 12:42 (20 minutes ago)
Miner	Bitdeer
Coinbase data	⍰⍰1⍰ ⍰⍰`bj/Bitdeer/⍰qz⍰⍰⍰

USD BTC

Transaction count	2,122	Fee per kB	0.00018353 BTC
Witness tx count	461	Fee per kWU	0.00005391 BTC
Input count	5,896	Output count	5,080
Input total	2,169.27789065 BTC	Output total	2,175.52789065 BTC
Fee total	0.21520995 BTC	Coindays destroyed	5,798.78
Generation	6.25000000 BTC	Reward	6.46520995 BTC

Technical details

Difficulty	20823531150112
Size	1,172,929
Weight (weight units)	3,993,073
Stripped size	940,048
Version	549453824_{10} $20c00000_{16}$
Version [bits]	$10000011000000000000000000000000_2$
Median time	2021-01-28 12:21:03
Merkle root	5d f9
For developers	API docs
Alternative explorers	

Click to see more

Transactions included in this block

Type here to search | ENG | 13:02 28/01/2021

Bitcoin / Block / 668042 — Block | New tab

https://blockchair.com/bitcoin/block/668042

Input total	2,169.27789065 BTC	Output total	2,175.52789065 BTC
Fee total	0.21520995 BTC	Coindays destroyed	5,798.78
Generation	6.25000000 BTC	Reward	6.46520995 BTC

Alternative explorers

Click to see more

Transactions included in this block

Block #	Hash	Inputs #	Outputs #	Coindays destroyed	Output (BTC)	Output (USD)	Transaction fee (BTC)	Transaction fee (USD)	Fee/kB (BTC)	Size (kB)
668042	4f…7b	1	3	0.00	6.46520995	194,454.00	0.00000000	0.00	0.00000000	0.247
668042	90…7a	9	12	1,629.36	1,407.29027588	42,327,100.00	0.00363000	109.18	0.00117704	3.084
668042	f9…1b	1	4	0.07	4.77249091	143,542.00	0.00054000	16.24	0.00188153	0.287
668042	85…a7	2	1	0.00	0.00469994	141.36	0.00043482	13.08	0.00127513	0.341
668042	d4…4e	1	2	0.00	0.08270061	2,487.39	0.00040320	12.13	0.00161928	0.249
668042	f5…57	1	2	0.01	4.40783554	132,574.00	0.00039840	11.98	0.00161296	0.247
668042	f9…5f	1	2	0.03	16.34465500	491,598.00	0.00039840	11.98	0.00161296	0.247
668042	72…ea	1	2	0.33	3.75875904	113,052.00	0.00039840	11.98	0.00160645	0.248
668042	77…a5	4	1	0.00	0.03894625	1,171.39	0.00084847	25.52	0.00116229	0.730
668042	49…8e	3	1	0.07	0.03890000	1,170.00	0.00100799	30.32	0.00207833	0.485

Explore this list (2,112 more rows) →

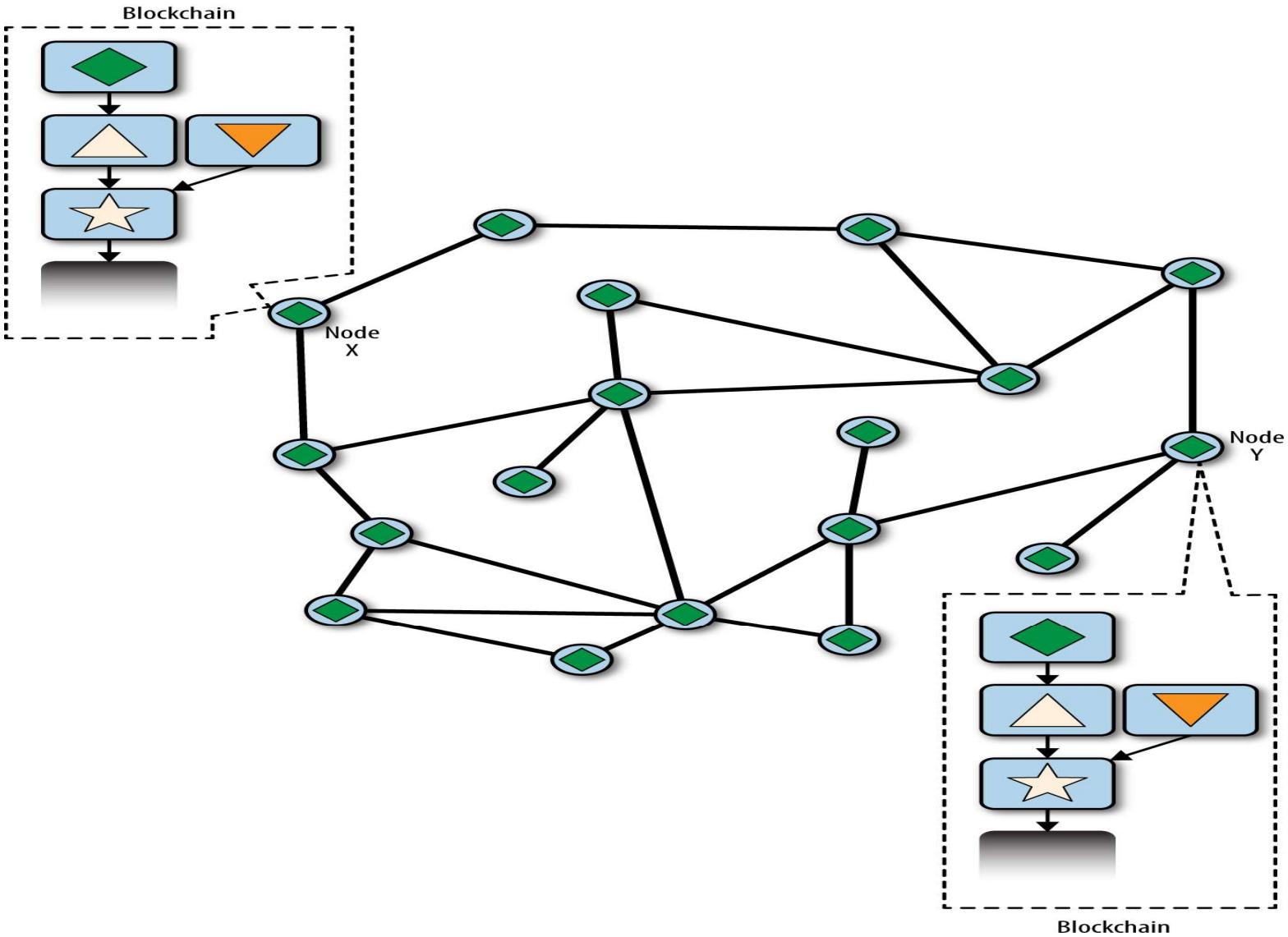
Type here to search

ENG 13:03 28/01/2021

How do nodes decide between competing blocks?

- Nodes keep three collections of blocks
  - Those on the main blockchain
  - Those that form branches off the main blockchain
  - Orphan blocks – those without a parent block
- The main chain is the chain with the most cumulative difficulty associated with it
  - Usually the chain with the most blocks
  - If two chains are equal length, then the main chain is the one with most PoW
- Forks usually resolved within 1 block
- 10 minutes for each block time is a compromise between
  - Fast confirmation times & the probability of a fork.

Eventually consensus is achieved



Thank you!

peter.mcburney@kcl.ac.uk