Lecture 4: Peer to Peer Network, Block Producers and the Fee Market

Total de pontos 19/22

✓ What is the current duty of a peer on the network? * 2/2

- [x] Propagate messages ✓
- [ ] Alert network fo a bad peer
- [x] Serve a copy of the blockchain ✓
- [ ] Try to connect to as many peers as possible

Feedback

A peer will simply disconnect from another peer if they consider them bad. It is a local policy for when to decide "good" or "bad" peers.

The p2p network's goal is to be a mesh network. You only need a number of transactions to ensure you have good visibility. By connecting with everyone, you exhaust available connections that others could have. Remember - every connected peer increases bandwidth consumption.

✓ Is it a requirement for a peer on the network to serve a full copy of the blockchain? *1/1

- ○ Yes
- ◉ No ✓

Feedback

Only full nodes or archival nodes will provide a copy of the blockchain to new peers.

You can run a "pruned" node, fully validate the network, and of course propagate messages across the blockchain.

But there is a more fundamental truth - the idea of fetching a copy of the blockchain from a peer on the network is mostly out of laziness / convenience.

The only thing the peer to peer network guarantees is that the new block is propagated widely, not that previous blocks can be fetched.

✓ is the DNS seed trustless or trusted? * 1/1

- ○ Trustless
- ◉ Trusted ✓

Feedback

We must trust that:
- One DNS seed will return an honest peer
- Node can connect with the honest peer

It is a trusted setup and there has never been a good solution for discovery of new peers.

✓ What message is propagated across the network when advertising a new transaction? *1/1

- (●) Transaction hash (inv) ✓
- ( ) Transaction data (tx)

Feedback

It is possible that a node will receive the same advertisement from multiple peers. The transaction hash is sent and the node can decide to fetch the transaction from one of their peers. This is a bandwidth-efficient approach.

✗ What storage assists with flooding attacks? * 0/1

- (●) Blockchain ✗
- ( ) Account database
- ( ) Memory pool

Resposta correta

- (●) Memory pool

Feedback

A node keeps track of recently propagated transactions. If they receive a copy of the same transaction, they can simply not propagate it onwards or request its data.

✓ What is a 0-confirmation transaction? * 1/1

- ○ The intended receiver of the payment has not yet confirmed the transaction on their website.
- ○ The transaction is in a block, but the tip of the chain is not yet stable.
- ◉ The transaction is not yet included in a block, but propagated across the network. ✓

Feedback

We say a transaction is "confirmed" when it is in a block and the "number of confirmations" is really the depth of the block in the blockchain.

For example, if a transaction has 1 confirmation, then it is included at the chain's tip. If it has 100 confirmations, then its respective block has had 100 more blocks extend it in the chain.

Thus, if a transaction has 0-confirmations, then it is not yet included in a block.

✗ Which approaches can undermine 0-confirmation transactions? * 0/2

- [ ] Merchant may decide not to update their website and pretend the transaction is not confirmed
- [x] The transaction signer can replace the content of a pending transaction by bumping its fee. ✓
- [ ] The transaction signer can simply send a replacement transaction directly to the miner.

Resposta correta

- [x] The transaction signer can replace the content of a pending transaction by bumping its fee.
- [x] The transaction signer can simply send a replacement transaction directly to the miner.

Feedback

It is very easy for the signer to replace the content of a transaction before it is finally confirmed on the network. Never trust a pending transaction.

✓ What is an archival node? * 1/1

- ( ) A node that validates the blockchain, but only keeps around recent blocks.
- ( ) A node that validates the blockchain and keeps a few snapshots of the latest database.
- (•) A node that validates the blockchain and records a snapshot of the database for every block. ✓
- ( ) A node that does not keep a copy of the database or blockchain, but only the chain of block headers.

✓ Is a "full node" and an "archival node" the same thing? * 1/1

- ○ Yes
- ◉ No ✓

Feedback

NO NO NO NO NO NO NO NO NO

✓ What is headers-first sync? * 1/1

- ○ Fetch the blocks and the relevant data in chronological order
- ○ Download a block header and its data together, and process each block in chronological
- ◉ Download all block headers first and then download the corresponding block data ✓
- ○ Download all block headers, but not the block data.

Feedback

Headers-first sync was implemented to help nodes find the longest and heaviest chain before they download the actual block data.

This is because block headers are significantly smaller than blocks. For example, a block header in Bitcoin is 80 bytes vs 1 MB block.

✓ From the perspective of the peer to peer network, what is the goal of decentralization? *1/1

- ○ A % of the world's population can afford to use the network
- ○ A % of the world's population can produce blocks
- ◉ A % of the world's population can verify the blockchain's integrity in real-time ✓

Feedback

We are really considering "who can run a node" aspect of cryptocurrency. It is the only type of network where the database is publicly available and anyone can independently verify its correctness. The more people who can run nodes, the greater likelihood that the economic-majority can continue to enforce the rules.

✓ What is Proof of X really proving? * 1/1

- ◉ Prove ownership of a scarce resource ✓
- ○ Prove ownership of X
- ○ Prove ownership of hardware
- ○ Prove ownership of an abundant resource

Feedback

Proof of X is a rate-limiting mechanism for restricting who can become a block producer. If "X" is abundant, then anyone could get the resource and become a block producer. Thus, "X" needs to be a scarce resource, like the ability to solve a computationally difficult resource or ownership of tokens.

✓ Does Proof of X impact the network's throughput? * 1/1

- ○ Yes
- ◉ No ✓

Feedback

It can have a "little" impact, but generally it is not the bottleneck for the network's throughput. As we will see, it is about compute/storage/bandwidth, not necessarily how we pick the next block producer.

✓ Has a single mining pool ever achieved more than 51% of Bitcoin's hashrate? *1/1

- ◉ Yes ✓
- ○ No

Feedback

GHash achieved 51% of the network's hashrate in 2014. The position was not abused and the miners shortly left the pool -- so much so that it no longer exists!

But it does demonstrate that it is indeed within the realm of possibility to get 51% of the network's hashrate. And we should consider it a long term threat.

✓ Should block producer's rely on the longterm upside of holding crypto coins as their business model? *1/1

- ○ Yes
- ◉ No ✓

Feedback

It should be expected that the price of crypto eventually stabilises and block producers can no longer expect 1000x within 5 years.

The "coin go up" economics was a good way to bootstrap the network, but long term it must rely on a profitable business venture.

✓ In Bitcoin, what is the auction mechanism for transaction bidding? * 1/1

- ○ Second priced auction
- ◉ First priced auction ✓
- ○ Sealed price auction

Feedback

All users bid for blockspace using their transaction fee. Miners pick the transactions based on the highest fee. This is a first-priced auction as all users will pay the price they proposed.

✓ It can be argued that the blockchain's tip in Bitcoin can become unstable when the block subsidy disappears. What is the argument for that? *1/1

- ○ The subsidy will never go away. It is not an argument.
- ◉ If the memory pool becomes empty, miners will create a fork at the tip and try to steal transaction fees from an already mined block ✓
- ○ Without a block subsidy, miners will have no income and simply stop mining altogether

Feedback

The dilemma is mostly, why mine a new block if there is no pending transactions and no income?

✓ What is the base fee in EIP-1559? * 1/1

- ○ A fee set by the user before they send their transaction
- ○ A constant value (10 gwei) that must be paid for all transactions
- ◉ A minimum fee that is computed for the transaction based on the network's current congestion ✓

Feedback

In EIP-1559, the base fee is increased / decreased based on usage of the Ethereum blockchain. If there is a sudden spike of traffic and people are willing to pay for it, then the fee will go up. If there is no traffic, the base fee will decrease.

✓ Why is it possible for Ethereum to become "deflationary"? * 1/1

- ○ People are losing their coins and can be considered lost for ever.
- ○ The block reward will go to zero and no new coins will be issued.
- ◉ The base fee is burnt and it is expected the total burnt fees will be greater than the total issuance of new coins. ✓
- ○ Ethereum will issue new coins forever and it will never be deflationary.

Feedback

There is a delicate balancing act:
- Burning coins via transaction fees
- Issuing coins via block subsidy

Long term, it is expected that more coins will be burnt (on average) than coins issued (on average).

✓ What is the idea behind minimal viable issuance? * 1/1

- ◉ We need to pay the bock producers the minimum necessary to secure the network. ✓
- ○ An ERC-20 token should issue coins over time and avoid the physical limit of a uint.
- ○ Ethereum has reduced the subsidy from 5 eth to 2 eth over time. It should eventually go to 0.

Feedback

The idea behind minimal viable issuance is to avoid overpaying the block producers more than is necessary to secure the network.

Remember - every time coins are issued and the total supply inflates - this hurts coin holders who are essentially paying a "tax" to secure the network.

We should avoid inflating the total supply as much as we can - so something like ETH can be considered a good store of value.