Lecture 1: An Introduction to Cryptocurrency

Total de pontos   25/25

Email *

lalanda.alberto@gmail.com

✓ **What is the double-spending problem? ***   1/1

◯ Picking one out of multiple pending transactions to confirm.

⦿ Assuming two or more transactions are trying to spend the same coin, only one   ✓
transaction can be finalised.

✓ **Select one or more key insights by Satoshi Nakamoto to solve the**   2/2
problem which plagued all previous e-cash protocols? *

☑ Replacing human trust with programmable rules.   ✓

☐ Incorporating the US legal system in the block production process.

☑ Allowing anyone to participate as a broker.   ✓

☐ Relying solely on altruistic behaviour of participants

Feedback

Good work!

✓   **What is a Bitcoin address or Ethereum account? ***   1/1

- ⦿ A cryptographic hash of the public key such that A = H(P).   ✓

- ◯ An encryption of the public key.

✓   **What is trust engineering? ***   1/1

- ◯ Setting up a trusted party to protect the system

- ⦿ Defining and reducing trust in the system   ✓

✓   **What is a block producer not trusted to enforce in a cryptocurrency like**   5/5
    Bitcoin or Ethereum?

- ☑ Monetary policy   ✓

- ☑ Rules that dictate validity of a transaction   ✓

- ☑ An approve list of who can participate   ✓

- ☑ Not to reverse already confirmed transactions   ✓

- ☐ Deciding the order of execution for a list of transactions

- ☑ Picking the next leader for producing blocks   ✓

✓ **What does an attacker need to forge a signature from your public key?**   1/1

- ⦿ Private key   ✓
- ○ Previous digital signatures
- ○ Address/account
- ○ Screenshot of your metamask wallet

✓ **Who pays for a transaction? ***   1/1

- ⦿ User   ✓
- ○ Node
- ○ Block producer
- ○ No fee

Feedback

Typically, the user pays the network fee. Someone may pay it on their behalf, but it is ultimately a user.

✓   **Is a block producer also a node on the network?** *   1/1

(●)   Yes   ✓

( )   No

Feedback

A block producer runs a node to collect transactions from the peer to peer network. It is important to run a node to ensure that all transactions are valid before packing it into their block.

✓   **What is a block?** *   1/1

( )   An unordered list of transactions

(●)   An ordered list of transactions   ✓

( )   A full copy of the database at a given time

Feedback

A block is just an ordered list of transactions. All transactions are executed against the current state of the database. It is basically a batch update.

✓   **Does proof of work help scale transactions on the network?** *   1/1

( )   Yes

(●)   No   ✓

✓   **Why do we need a leader election?**   2/2

☐   Satoshi appointed a large set of participants in advance and we need to pick amongst them just in case some go offline.

☑   There is no trusted authority who can pick a leader to run the system.   ✓

☑   Protect liveness of the system as anyone can participate.   ✓

☐   Democratic elections are a way to secure the system.

☐   By knowing the leaders, we can rapidly scale transaction throughput.

✓   **What properties can we find in proof of work?** *   3/3

☐   Popular on TV

☑   Time consuming to solve   ✓

☐   Time consuming to verify solution

☐   Only one solution for the same challenge

☐   Quick to solve

☑   Quick to verify solution   ✓

☑   Multiple solutions to same challenge   ✓

☐   Puzzle is subjective

☐   Puzzle is set by a leader

✓   **What is a fork in the chain's tip?** *   1/1

◉   Competing blocks at the tip of the blockchain   ✓

○   A special reward to the block producer

✓ Why do we need a fork choice rule? *   1/1

○ It is not needed. Block producers can just extend all competing blocks.

◉ To decide which chain of blocks should be considered part of the blockchain.   ✓

✓ Can a transaction get dropped (reversed) after it is confirmed?   1/1

◉ Yes   ✓

○ No

✓ What is the recommended number of confirmations to wait for a Bitcoin   1/1
transaction? *

○ 1

○ 2

○ 3

○ 4

○ 5

◉ 6   ✓

✓ How are new coins issued on a network like Bitcoin or Ethereum?   1/1

○ All coins existed and allocated when the network was formed.

◉ Every new block issues new coins to the block producer.   ✓

○ Every new block issues new coins to all users of the network.

Este conteúdo não foi criado nem aprovado pela Google. - Termos de Utilização - Política de privacidade

Google Formulários