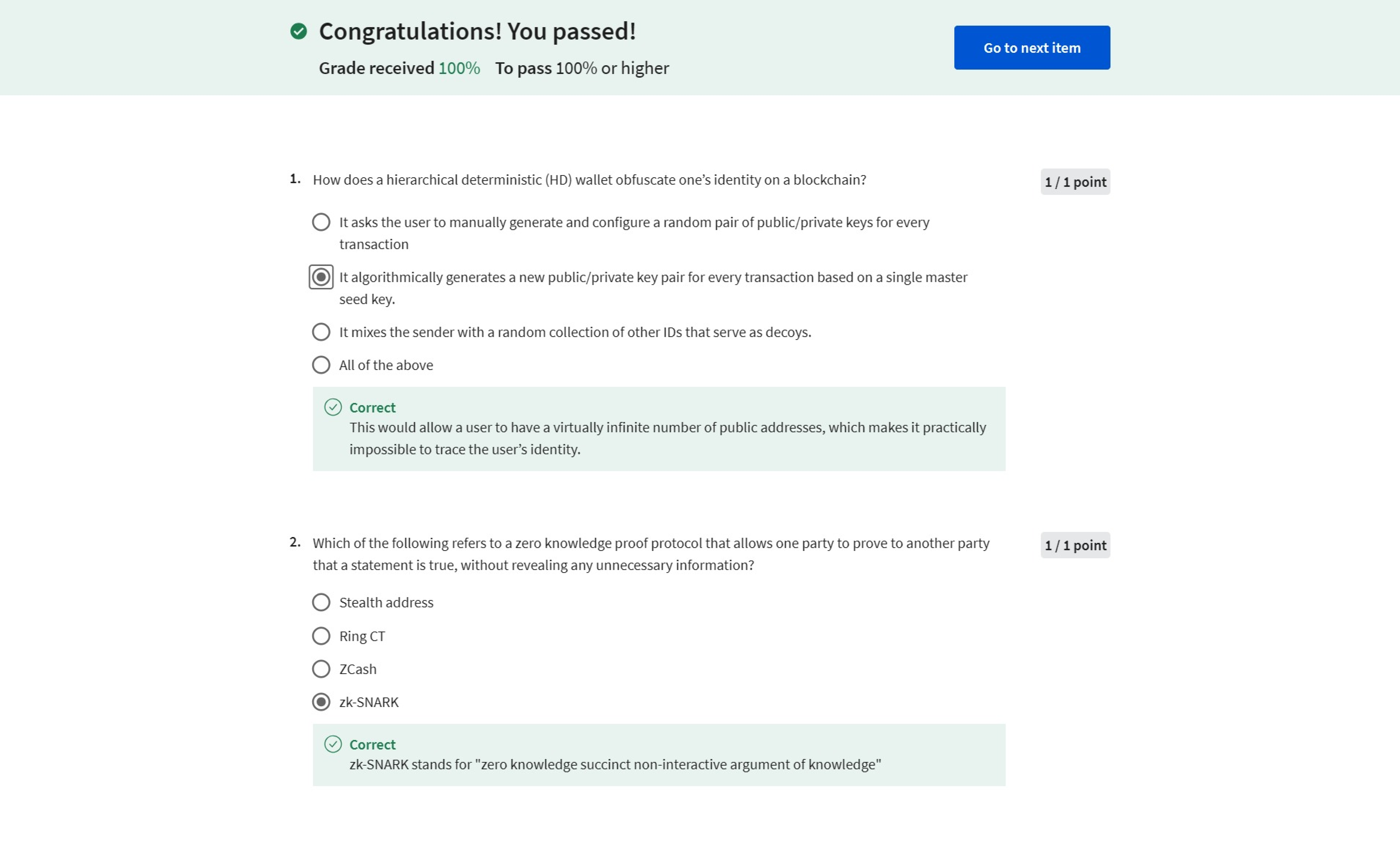

Congratulations! You passed!

Grade received 100% **To pass** 100% or higher

1. How does a hierarchical deterministic (HD) wallet obfuscate one's identity on a blockchain?

1 / 1 point

○ It asks the user to manually generate and configure a random pair of public/private keys for every transaction

● It algorithmically generates a new public/private key pair for every transaction based on a single master seed key.

○ It mixes the sender with a random collection of other IDs that serve as decoys.

○ All of the above

Correct
This would allow a user to have a virtually infinite number of public addresses, which makes it practically impossible to trace the user's identity.

2. Which of the following refers to a zero knowledge proof protocol that allows one party to prove to another party that a statement is true, without revealing any unnecessary information?

1 / 1 point

○ Stealth address

○ Ring CT

○ ZCash

● zk-SNARK

Correct
zk-SNARK stands for "zero knowledge succinct non-interactive argument of knowledge"