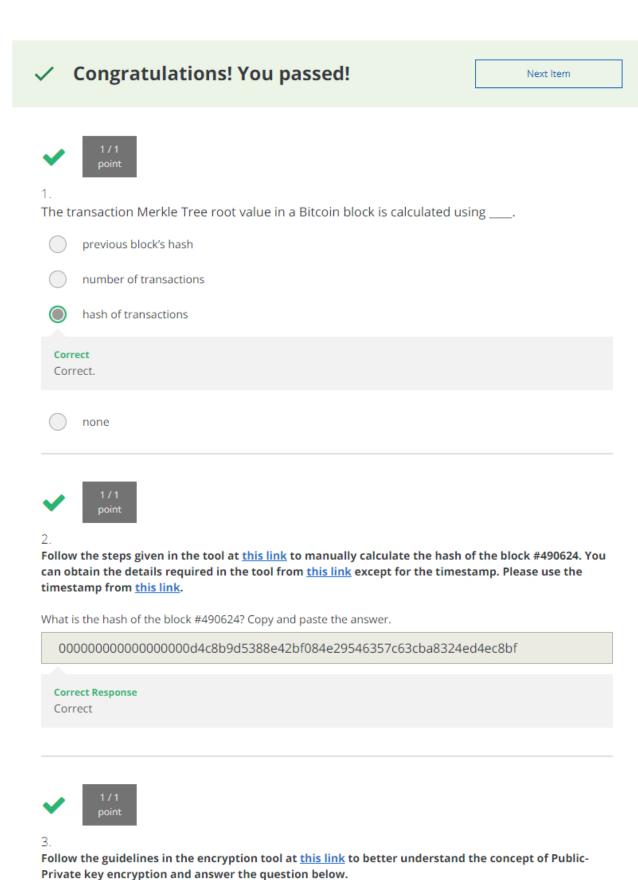
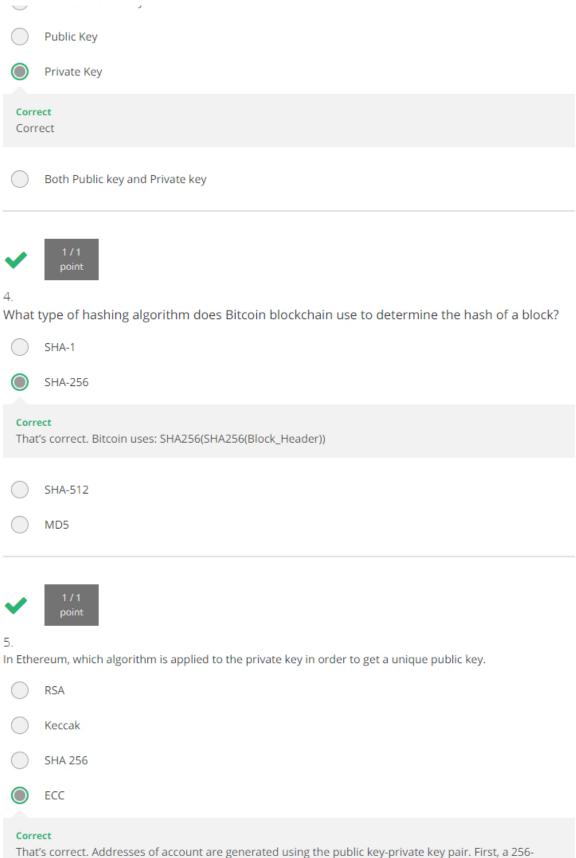


Quiz, 10 questions



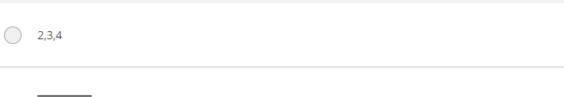
When encrypting a message with the public key, which key is required to decrypt the message?

Inverted Public Kev



That's correct. Addresses of account are generated using the public key-private key pair. First, a 256-bit random number is generated and designated as a private key, kept secure and locked using a passphrase. Then an ECC algorithm is applied to the private key to get a unique public key.

6. Which of the following methods can be used to obtain the original message from its generated hash message using SHA-256?						
Hashing the generated hash again						
Hashing the generated hash again, twice						
Hashing the reverse of generated hash						
Original message cannot be retrieved						
Correct That's correct. SHA-256 is a one-way hash function, that is a function which is infeasible to invert.						
✓ 1/1						
7. In Ethereum, hashing functions are used for which of the following?						
1. Generating state hash.						
2. Generating account addresses.						
3. Decrypting senders message.						
4. Generating block header hash.						
1,2,3						
1,3,4						
1,2,4						
Correct That's correct. In Ethereum, hashing functions are used for generating account addresses, digital signatures, transaction hash, state hash, receipt hash, and block header hash.						





What is the purpose of using a digital signature?

None of the above.

It supports both user authentication and integrity of messages

Correct

That's correct. A valid digital signature gives a recipient reason to believe that the message was

and	that the message was not altered in transit (integrity).					
\bigcirc	It supports user authentication					
	It supports the integrity of messages					
• 9.	1/1 point					
Encryption of a message provides						
	nonrepudiation					
	authentication					
	integrity					
	security					
Correct.						
~	1/1 point					
10. A publ	ic key is derived from the					
	a different public key					
	private Key					
Corr						
0	hash of the first transaction by the account genesis block hash					

created by a known sender (authentication), that the sender cannot deny having sent the message,



