

Puzzle #2: Light the Way

As you know, the design of Bitcoin depends heavily on cryptographic protocols. Two of my closest friends, Alice and Bob used their deep knowledge of cryptography to help me invent Bitcoin. Prove you are as knowledgeable as they are if you want Bob to send you your next clue:

1. Alice wants to send Bob a secret message using asymmetric key encryption. What does she need from Bob in order to do so?

P U B L I C K E Y

2. Alice wants to make sure that she has Bob's public key, and not the public key of an imposter. What can she use to verify the authenticity of Bob's public key?

D I G I T A L C E R T I F I C A T E

3. Alice uses Bob's public key to send him a shared secret, "blockchain7". Use this public key and tinyurl.com/satoshisymmetric to encrypt a secret message, "protect satoshi's bitcoin". Write the first six characters of the ciphertext below:

8 f c a z d

4. What can Bob use to verify that Alice is the only person who could have possibly sent this message?

D I G I T A L S I G N A T U R E

bobBCFDE@gmail.com