Quiz

Your Name: _____

For this quiz, you should **work alone**. You may use your course notes, but no other resources. Answer all the questions as well as you can. Good answers will be clear, consise, and correct.

1. What properties are *necessary* for something to work as a currency?

2. Alice owns coin X and has public/private key pair (KU_A, KR_A); Bob has public/private key pair (KU_B, KR_B) for the strong asymmetric cryptosystem E (the notation $E_K(m)$ denotes the encryption of input m with key K). Everyone agrees that H is a strong cryptographic hash function. What message should Alice send to the public ledger to transfer X to Bob?

3. Explain in a way that would be understandable to a non-computer scientist who wants to use bitcoin why it is important to wait several minutes (or longer) before accepting a bitcoin transfer.

The final two questions ask you to speculate on capabilities that might enable one to "break" bitcoin. You should answer them from the perspective of someone with no ethical concerns who what to either enrich herself or disrupt the bitcoin economy as mush as possible.

4. Suppose you are given a mysterious box Q that can produce fraudulent ECDSA signatures for the bitcoin curve. Given KU_x, a public key, and m, a message of your choosing, $Q(KU_x, m)$ outputs a valid signed message corresponding to m signed with the private key corresponding to KU_x. You can run Q on any input you want, but other than obtaining the output do not learn anything else about Q (that is, you cannot open it and see anything about how Q works). Would you be able to use Q to "break" bitcoin? Explain what you could do, or argue why Q by itself would not be enough to do serious damage.

5. Suppose you are given a mysterious box B that can compute SHA-256 pre-images. That is, given x as input, $B(x)$ outputs z such that SHA-256$(z) = x$. You can run B on any input you want, but other than obtaining the output do not learn anything else about B (that is, you cannot open it and see anything about how B works). Would you be able to use B to "break" bitcoin? Explain what you would do, or argue why B by itself would not be enough to do serious damage.

