ECE8930 Blockchain
Homework 1

R. R. Brooks - rrb@clemson.edu

May 2020

Answer each question clearly and concisely. Each question is worth 20 points.

1. What security guarantees can the blockchain provide? Explain how the blockchain data structure enforces these guarantees.

2. *Data on the blockchain is secure and private.* Explain what is true in this statement. Explain what it not true in this statement.

3. We explained BTC P2PKH transactions.[1] Research Pay to Script Hash P2SH transactions [2]. Explain how they work. Give some positive and negative aspects of P2SH.

4. Explain how P2PKH works. Be specific about how P2PKH guarantees that payment goes only to the intended recipient.

5. I set up a BTC account by generating an EC public key and private key pair. Assuming that the software has no bugs, how likely is it that someone else could redeem my coins? Compare that likelihood to the likelihood of that person winning the powerball lottery, winning the powerball lottery twice, being hit by lightning, and being hit by lightning twice. Is that risk acceptable? Why or why not?

[1] http://royalforkblog.github.io/2014/11/20/txn-demo/

[2] https://en.bitcoin.it/wiki/Transaction#Pay-to-Script-Hash