Dean Makovsky (dem2dw)
Cryptocurrency Problem Set 1

1. Answer the following questions about the transaction where you received the bitcoin.
   Link to transaction:
   https://blockchain.info/tx/1487e03aa6c26e03cf07124caf1a2feb56cf4a9108c16a3ceb82a956c664a99f
   a. Transaction ID: 1487e03aa6c26e03cf07124caf1a2feb56cf4a9108c16a3ceb82a956c664a99f
   b. Transaction fee: 0.0001 BTC ~ $0.022
   c. Block 372136 transacted a total value of 1,111.13927457 BTC ~ $254,317.56
   d. The transaction was received at 2015-08-30 00:35:29
      and included in block 372136 at 2015-08-30 00:35:57
      and block 372139 was confirmed at 2015-08-30 01:24:17
      …so it took 48 minutes and 48 seconds to be confirmed 3 times.
2. How much can you figure out about the way bitcoin was transferred to students in the class?
   a. By tracing backwards, I found:
      1D6qsGhZqrRSKegqWT3e8TPR8gGczTxMLu
      1JHoF2bak7KCST3SzeR7e1AwqDm4tiLJjt
      1MtYZBtRw8XcnTgEY8qQphbddnwwFcoEXH
      which are probably other student's bitcoin addresses (all were given the same BTC amt.)
   b. I traced it back a lot, with a few odd transactions and addresses thrown in, but this seems to be the origin of your wallet:
      https://blockchain.info/address/14J6ep326owXDpc1waViGJNB1onSFy9eou
      I traced back very far and found some million dollar transfers, but didn't know how to associate these addresses with a bitcoin exchange.
   c. Did you use a proxy to Germany? Would a foreign proxy explain why I saw a small sum sent to a gambling site? Although blockchain.info clearly has a map showing Germany, an IP address location finder also resulted in Germany. …after doing more of the assignment I see this is not the case, but still unsure what the gambling thing is about.
3. Stealing bitcoin via malicious software
   a. A malicious developer could take a fee, say 1000 satoshi, every time you decide to send money with the wallet. Or they could open a connection to the outside world and send your (and everyone else's) private keys to their servers; then when they have enough keys they steal everyone's money at the same time and "go public" with the thieving. Or if it sees you make a lot of transactions, it could just add a

small one in every now and then to give themselves a few extra pennies. There are many possibilities.

   b. I’m pretty confident that my money is safe in Multibit HD. It’s listed on the main bitcoin website, so I assume those people have looked into the technology to verify its security. Furthermore, you recommended it too. If I was going to store all my money in a bitcoin wallet, I might consider changing to use bitcoin-core and use the CLI (though this could have similar problems).

4. Typing “2^256 - 2^32 - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 hex” into Wolfram Alpha yielded “fffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f” which is the same as the Go code.
5. The Operating System has good randomness; the library was written to handle randomness securely (whatever this means; which is more than calling Math.random() in Java); these keys remain local on your computer and not sent over network; no other process can view the output of this program and will transmit the data elsewhere; the btcd library is written to the bitcoin spec and is bug-free.
6. Er

```
func generateVanityAddress(pattern string) (*btcec.PublicKey,
                                                  *btcec.PrivateKey)  {
        for {
                pk, sk := generateKeyPair()
                temp := generateAddr(pk).String()
                // fmt.Printf(temp, "\n")
                boolean, garbage := regexp.MatchString(pattern, temp)
                if boolean {
                        return pk, sk
                } else if false {
                        fmt.Printf("temp", garbage)
                }

        }
}
```

7. This is a public key in hex:
   [02de7e161e6abed54102b9f22623d21f61a62a5ffcb67b3382efac98c8eba1a520]
   This is the associated Bitcoin address:
   [1BjGkTPSeEDLodean2es4xomvyW1mTR617]
8. The vanity address should have the same level of security as a regularly generated address. This is because a good hash function makes it infeasible to find some key, x, such that H(x) = *vanity*.
9. Link to transaction (and transaction id):
   https://blockchain.info/tx-index/e33371daca889afb1e8ca21d0a8392dd386ee5b3d01a798d3c73fef91825499a This is weird though...the received time is 2015-09-15 05:27:02 but

the “included in block” time is 2015-09-15 05:26:36, which doesn't make sense.

10. Link to transaction: https://blockchain.info/tx/48f5fb7a657f825d68af2bc000c1da8a5c37ec87e10513509bc9aeb41b9645ac