Bitcoin Presentation Notes

1 Introduction

- Commerce on the Internet relies almost exclusively on financial institutions serving as trusted third parties to process electronic payments.
- Problem: TODO

2 Digital Signatures

- Scenario: Alice wants to send a message to Bob over a network. How can Bob verify that the message he received was from Alice? Alice needs to sign her message.
- Desired property of signature: cannot be forged on a different message.
- Both Alice and Bob each generate a public/private key pair for themselves. Each key is some string of bits. Private keys are kept secret.
- Producing a signature: $\mathsf{sign}(\mathsf{message}, \mathsf{privateKey}) = \mathsf{signature}$.
- Verifying a signature: $\mathsf{verify}(\mathsf{message}, \mathsf{signature}, \mathsf{publicKey}) = \mathsf{true}/\mathsf{false}$.
- Only the owner of the private key can produce the signature.
- No one can copy the signature and forge it on another message.
- Signature is a 256 bit value. Hard to find a valid signature if you don't know the secret key. There is no strategy better than guessing and checking if random signatures are valid using the public key. There are 2^{256} signatures to check; this is a very large number.

3 Transactions

- Electronic coin: a chain of digital signatures.
- Alice transfers a coin to Bob:
  1. Alice computes the hash of previous transaction and Bob's public key.

2. Alice signs the hash using her private key.
3. Alice adds her signature to the end of the coin.
4. Bob verifies that Alice transferred a coin to him using Alice's public key.

- Problem: how to verify that Alice did not double-spend the coin?