1. Bitcoin in general
    a. It's a currency
    b. Purely digital
    c. Invented 2008/2009, Satoshi Nakamoto
        i. Has since handed it off
    d. Difficult to research
        i. If I contradict myself, please point it out
        ii. A lot of my sources were contradictory, so I'll try to elaborate/clarify, but I may not be able to
2. Who accepts Bitcoin?
    a. Individual businesses choose whether to accept it
    b. Many do
        i. Amazon
        ii. Target
        iii. Home Depot
        iv. Food trucks
3. How to purchase something
    a. Often Bitcoin is run off of your phone
        i. QR codes used for purchases
    b. Digital/physical Bitcoin "wallets"
4. Because it's purely digital, what problems?
    a. Double-spending
        i. Spending the same money to two different people
5. So how does this system work
    a. Network of computers, "miners" running software to power the system
    b. Note that the Bitcoin system uses no encryption, just hashes and digital signatures
    c. The system is massively distributed and redundant
        i. What this means is that everyone does everything
    d. So, transactions
        i. "Payer X sends Y bitcoins to payee Z"
            1. Signed with digital signature private key
        ii. Transactions are cherry-picked and clumped into blocks
        iii. Blocks are hashed, hashing should take ~10 minutes
            1. So a difficulty target nonce is chosen low enough
            2. This is "mining," because new Bitcoins are awarded to the first person to hash the block
        iv. Every block has a hash of the previous block, which "chains" them together
            1. Any change to a block requires changes to every subsequent block
                a. But the system keeps progressing, and a malicious attacker can't keep up
        v. Because everyone has a copy of the block chain, no one can modify it without people noticing the changes

6. So I mentioned earlier how security was without encryption
    a. Everything is in the open
    b. Mass agreement ensures that no one can change the past
    c. Building up the chain ensures that nothing in the past can be changed
        i. Hashes are hard to find due to difficulty target nonce
            1. Pointless work, done simply to be “hard”
            2. But easy to check because they’re hashes
        ii. Digital signatures ensure that no one but you can authorize spending your bitcoins
            1. ECDSA
                a. Elliptic Curve Digital Signature Algorithm
                b. By NIST (National Institute for Standards and Technology)
            2. Lose your key, lose your bitcoins
    d. Attackers would have to have more than half the computing power of the entire network to keep ahead of new blocks being created
        i. Hence incentivizing the “mining” process
        ii. Not financially viable