6.857 Recitation 3: Bitcoin

Heeyoon Kim

1 Administrivia

- Pset 1 due on Gradescope Mon. 2/27
- Pset 2 out 2/27
- Post project idea on Piazza with group members or individually by Wed. 3/1 (can use this post to recruit group members)

2 Introduction

This recitation gives a high level description of electronic money and Bitcoin. We will go more in depth during lecture next Monday. We'll start by covering the thoughts that went into creating Bitcoin, then dive into how Bitcoin actually works, and the properties of the system.

3 Properties of Money

Before we discuss how to make electronic money, we must first understand what money is. Money:

- Stores values
- Very important to keep track of who has what amount
- Is tradeable
- Has backing
  - Government backing
  - People's belief in its worth
- Ancient days, kept financial records

4 Centralized Digital Money System

Now that we know the properties of real money, how do we approach making an electronic money system that works? We know that in ancient days, there were records kept that described who owed what amount. It'd be nice to have someone, like a bank, to keep such a record for everyone!
Could work as follows:

- Bank initially distributes some money to everyone
- Bank keeps track of who has what
- Bank must sign off transactions (digital signatures)
- Everyone only trusts the money or transaction if the bank signs it
- It's a simple solution, since only have to ask one entity to check the records.

The downsides of a centralized system are that:

- The bank sees all transactions $\rightarrow$ privacy issues
- May not trust the bank
- Bank can deny people transactions or even lie since central point of power

5 Public Ledger ("Magic book in the sky")

It seems that record keeping was a good idea, but having one person in control of it may lead to corruption. It'd be nice if we had a magical book in the sky that is always right, and everyone can use to keep records; that everyone can write to. In other words, keeping a public ledger in the cloud.
This is the idea behind Bitcoin, though note that the idea of a secure digital money system was thought about long before then by David Chaum (1983), who proposed ecash.

Properties of Ideal Public Ledger:

- Decentralized
- Double spending not allowed
  - E.g. Alice offers \$1000 to both Bob and Charlie for a \$1000 car at the same time. The public ledger will show Bob and Charlie that Alice has enough to buy the car. Need to be able to prevent Alice from spending the money twice.
- Consensus: everyone has to agree, or third party can verify who's right

- Updated each time a transaction happens
- Ideally, have a record of what each person has right now.

6 Bitcoin (Nakamoto, 2008)

6.1 Properties

Bitcoin has almost all of the above properties. It's decentralized, has a system preventing double spending and allowing concensus, and records transactions. In a bit, we'll see how some of these properties are enforced. Note that rather than storing the current amounts of everyone's account, Bitcoin stores the entire history of transactions. The downsides of this are that it's privacy violating since everyone can see this record (though identies are sort of anonymized), and that it's inefficient. However, note that it's good for doing taxes, record keeping for business, credit/loan, etc.

6.2 Protocol

- Each person needs an identity (may have multiple identities)
- Why can't one steal another's identity? Use (PK, SK) pair
- Public ledger where transfers between PK's are recorded
- Transactions are recorded only if sender's PK was signed by sender. This prevents double spending, since a sender would have to sign twice. Specifically, to append a transaction to the ledger, person must sign H(ledger data so far).
- Can't have everyone simply writing at once, since Internet is asynchronous $\rightarrow$ Need a serialization (ordering) mechanism

6.3 Proof of Work

What if many people sign at once? Bitcoin solves this by making it into a competition, so that it's harder for people to append so quickly. Must solve a puzzle to append the transaction. The puzzle should be hard to solve, but easy for anyone (i.e. Bitcoin) to verify.

- Enforces serialization, since must solve a puzzle in order to append to ledger
- Prevents spamming, since proof of work takes time

The Proof of Work problem that Bitcoin uses is to find r such that

$$H(ledger\_data|r) = 2^{256-D}$$

i.e. find a hash with D leading 0's. D = difficulty of PoW puzzle.
Solving by brute force takes $\theta(2^D)$ attempts, $\theta(1)$ space. D is automatically adjusted by system, and is a function of the amount of time that it takes people to mine coins, i.e. solve puzzles.

6.4 Blocks and Blockchains

Since it takes a long time to do proof of work, we should batch transactions. Each batch is called a block, and a chain of blocks is called the blockchain. There are miners verifying each block, i.e. solve proof of work. Every time a miner mines a block, get free money, i.e. brand new bitcoins given to PK of miner. (The amount of award is halved every time period, so it's not just limitless money.)
Note that it's still possible that two people solve the puzzle at the same time, leading to forks in the blockchain. To break ties and determine which record is correct, we simply take the longest chain, and the shorter one is ignored.
Any ties are likely to be broken within a few more blocks, since people choose to mine on the longest chain. However, since ties aren't broken immediately, this is the reason why people shouldn't have confidence in the block chain record until around 6 blocks later. In this sense, Bitcoin provides rough synchronization, which is usually enough.

7 Anonymity

Because Bitcoin stores the history of transactions publicly, there isn't a pure sense of anonymity. One can still track down patterns of transactions to, say, identify users. For example, it's been shown that if you keep track of individual transactions, and create a network graph using them, there will be clusters or other patterns that will form, that can reveal information about user patterns.
Z-cash is another digitcal currency system (layered on top of Bitcoin) that is really good at providing anonymity. It uses cryptographic proofs to reveal that Alice has enough money to pay Bob for something, but doesn't reveal any other info.