CSC 591 Cryptography 11/7/2018

Lecture Bitcoin

Lecturer: Alessandra Scafuro *Scribe: Ryan Mee*

Philosophy

What is the idea behind Bitcoin?

- Payments are made by updated the balances between the transacting parties.
- The recording and management of these balances has previously been maintained by a trusted 3rd Party: Banks
- Trust in banks is lost when banks fail, e.g. in the 2008 financial crisis. How can they be replaced?
- Trust Math instead! Use a cryptograpically secure public ledger maintained by democratic consensus: Bitcoin

Bitcoin

- Created by Satashi Nakamoto (pseudonym), whose real identity is unknown.
- Public Ledger: Every transaction and account is recorded and viewable to the public.
- Immutability: The ledger is appendable only, once a transaction is confirmed it cannot be erased or edited.
- Consensus: The verification and acceptance of transactions is achieved through democratic agreement.

Protocol

- Users are given a public key, and private key. An address is created by hashing the public key. These keys are used for the ECDSA signature scheme.
- Transaction: User A who knows the private key for an address with balance X can send Y s.t. Y <= X to another address, while the change, Z = X - Y, remains at A's address. A transaction is sent to every node in the network when broadcasted.
- Node: Collects and validates the transactions.
- Miners: A subset of Nodes that create blocks to add to the ledger.
- Blocks: A set of transactions to add to the blockchain along with the hash of the previous block and x, where x is the solution to H(B,x) = $0^k||*$ with k being some chosen difficulty parameter.

- Difficulty: The difficulty parameter k is chosen based on the total mining hash rate to ensure blocks are added in a reasonable time.
- Proof of Work: The above process of finding x is the miner's "proof of work", and the inclusion of a valid x to their block shows the network that they've followed the protocol and their block can be added.
- Hash Function: Bitcoin uses the SHA-256 hash function which is optimization-free (no better strategy than random), progress-free (no improvement from one puzzle to the next), and parameterable (difficulty can be chosen).
- Fork: Each block requires a number of confirmations by validators (nodes) before it is considered to be accepted. During this period, multiple blocks may be added with the assumption that they are all building off the same most recent block. This creates a fork where separate chains will begin being built. The more hashing power dedicated to a chain, the faster it will grow. Honest miners will always work on the longest chain. When one of the competing chains are confirmed, the other chain's blocks will become orphaned. Some of their transactions may have already been included in the longest chain, the others will need to be added to another block to be appended again.

Attacks

- 51% Attack: As honest miners work on the longest chain, so long as 51% of the network's hash power is controlled by honest miners, their chain will outpace any attacker's chain. If a group of adversaries gain more than 51% of the hash power, they can manipulate the future additions to that blockchain.
- Double Spend Attack: In this 51% attack, the adversarial miners build a chain in secret that conflicts with the chain being worked on by the honest miners. At some point after the honest chain has been confirmed, the adversaries broadcast their chain to the network. Since their chain is longer, the honest miners switch to it and their previously worked on chain is orphaned.
  - Adversary A has 10 bitcoin. They send 10 bitcoin to vendor B for pizza, and this is added to the honest chain. A works on a separate secret chain in which they send 10 bitcoin to vendor C for a book. After the honest chain confirms their transaction to vendor B, vendor B sends the pizza to A. At this point, A broadcasts their secret chain, which is longer than the honest chain, to the network. As its the longest chain, the honest miners switch to it and the previous chain is orphaned. The transaction from A to C is confirmed, and C sends the book to A. The transaction from A to B for the pizza becomes orphaned, and vendor B no longer has those 10 bitcoin associated with their private key. Adversary A has successfully spent their 10 bitcoin twice, once to B and once to C, double spending it.

Privacy

- All addresses and transactions are public. If your address is in any way tied or linked to your information, there is no anonymity.
- For more privacy, use Zero-Knowledge Proof based cryptocurrencies such as ZCash.
  - Hides the contents of the transaction.
  - Miners have no knowledge of the transactions, just check the given proof.