بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۱۴

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان

Blockchain

Non-Miners

- Users do not have to be miners
- Non-miner just wants blockchain
  - Needed to know how much § others have
- Also, non-miner sends out transactions for others to make blocks (and mine)
- User might see conflicting blockchains
  - What to do in such cases???
- More work is "more better"!

More Work

- If conflicting blockchains, how to know which represents more work?
- Each block is a fixed amount of work
  - In terms of expected number of hashes
- So, longer block chain is more work
- Thus, ***longer*** block chain always wins
  - If it's a tie, wait until one is longer

Summary of Protocol

1. New transactions broadcast
2. Miners collect transactions into blocks
3. Miners race to find valid block hash
4. When miner finds hash, broadcast it
5. Block accepted if all transactions signed, no overdraft, & block hash valid
6. New block extends the blockchain
   - Miners use hash of new block in next block

Attack Scenario

- Suppose Trudy makes a block B that includes transaction
  - [Trudy pays Alice § 100]$_{Trudy}$
  - Trudy sends B to Alice ***only***, nobody else
- **Q**: Why would Trudy do this?
- ***A***: So she can spend that § 100 again
  - Trudy likes double spending!
  - It's free money!

Double Spending

- For Trudy's double spending attack to work, she must compute valid hash
  - That is, find R, so that $h(Y,B,R) < 2^n$
- And send chain with block B to *Alice*
- But, nobody else knows about B, or the chain that contains it
  - All other miners working on other chains
  - Those other chains can (and will) grow
  - Trudy is in a race with ***all other miners***

Double Spending Attack

- Assuming she waits, Alice will reject Trudy's chain if longer chain appears
- Trudy would need majority of compute power in network to win consistently
  - Trudy needs to win a lot!
- Or, miners must collude with Trudy
  - But is it in their interest to do so?

Blockchain

- From users perspective…
  - Transaction in last block might not be entirely trustworthy
  - Possibility of double spending attack
  - But, the more blocks that follow, the more certain that a transaction is valid
- Just wait until a few more blocks are added before accepting a transaction

Refinements

- Number of hashes can change so that winning hash takes constant time
  - Computing power in network can increase
  - In Bitcoin, new block every 10 minutes
- Can decrease mining reward so money supply does not grow forever
  - E.g., maximum of 21,000,000 bitcoins
  - Then what will be incentive for miners?

Refinements

- Merkle tree can be used to reduce storage requirements
  - Transactions in a block hashed in a tree, only the root is needed in block hash
- Simplified payment verification
  - In effect, rely on others to verify for you
- Combining and splitting value
  - Transaction can have multiple input/output

Privacy?

- Can use pseudonym in public key
- But, can still connect transactions to a specific public key
  - Might be able to tie public key to an individual based on transactions
  - We'll see examples like this later…
- Not a super-strong form of anonymity
- Bitcoin is said to be "pseudonymous"

Future of Blockchain?

- Blockchain can be viewed as a way to implement a distributed ledger
- Useful for cryptocurrency, but many other possible applications too
- Blockchain said to be a "foundational" and/or "disruptive" technology
- Perhaps, but your skeptical author is not completely convinced…