CSCI 251: Concepts of Parallel and Distributed Systems

Alvin Lin

November 29th, 2017

Distributed Systems

Outline:

- Bitcoin and blockchain
- No block, no chain - directed acyclic graph
- Distributed consensus algorithm: proof-of-stake, proof-of-space-and-time, proof-of-retrievability
- Smart contracts

How to Use Bitcoins

1. Download software to your computer or phone to set up a Bitcoin wallet. This gives you the basic facilities to send, receive, and store Bitcoins.
2. Your software will generate a unique sting of letters and numbers: your Bitcoin address. The address isn't tied to your name or any other personal data, but it identifies you to the Bitcoin network. Give this address to anyone who needs to pay you.
3. Buy Bitcoins with a standard offline currency, either from another user or through a dedicated Bitcoin exchange. Your new digital funds are added to your wallet.

4. The Bitcoin network authenticates transactions by recording them in the 'block chain' - the underlying code that preserves the integrity of the currency.

5. Use your software to send payments to other addresses. Divisions as small as 100,000,000th of a Bitcoin are possible - a unit called a 'Satoshi', after the currency's enigmatic inventor.

Problems of Digital Tokens

- Ownership: who owns the digital currency?
- Authorization: who authorizes a transaction?
- Double Spending: what prevents a token from being transferred to multiple owners by erasing a transaction?

The Bitcoin Transaction Life Cycle

1. Person A opens his bitcoin wallet, scans/copies Person B's address, and sends a specific amount in a transaction.
2. The wallet signs the transaction using Person A's private key.
3. The transaction is propagated and validated by the network nodes.
4. Miners include the transaction in the next block to be mined.
5. The miner who solves the Proof of Work propagates the new block to the network.
6. The nodes verify the result and propagate the block.
7. Person B sees the first confirmation.
8. New confirmations appear with each new block that is created.

Key Elements

- Cryptographic Techniques: hash function (SHA256), public and private keys; the hash of the private key is the address for receiving money; pseudo-identity; digital signature/certificate

- Data structure to record "logs"
- Consensus algorithms: proof-of-work

Proof of Work

A nonce is appended to the previous hash to produce a new hash. A miner that guesses the correct nonce can broadcast the new block to the chain.

Reminders

Work on Project 2.
Professor Mohan Kumar:
`mjkvcs@rit.edu`
`https://cs.rit.edu/~mjk`

Rahul Dashora (TA):
`rd5476@mail.rit.edu`

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech