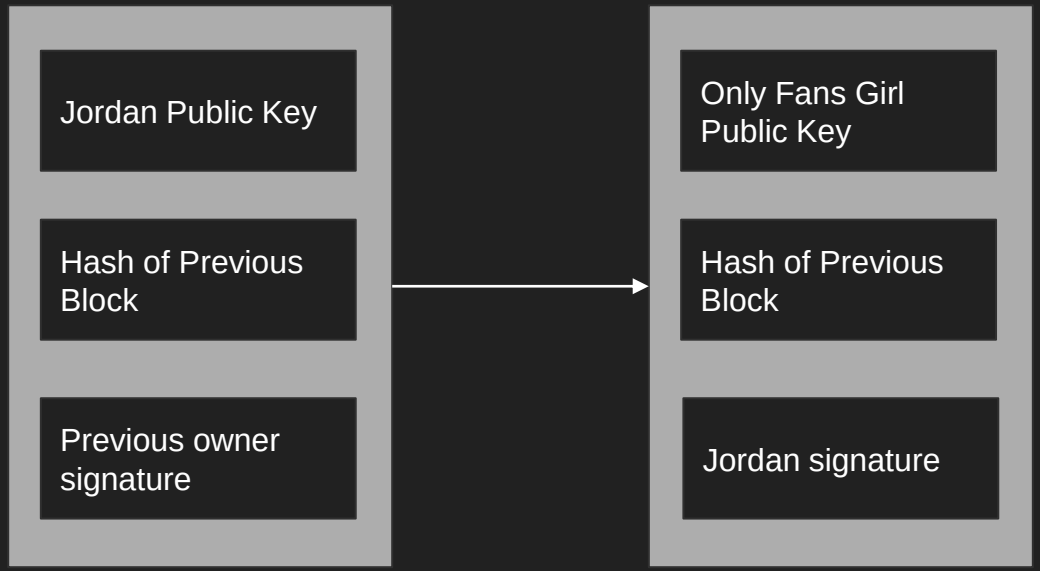
Bitcoin Design

Background

Originally, the motivation behind Bitcoin was to act as a decentralized currency, to eliminate the need for all transactions to be approved and monitored by a third party. However, with a decentralized currency comes potentially many malicious actors that may want to trick others into believing that they have more money than they really do. Bitcoin leverages the use of its blockchain, along with cryptographic proofs to ensure that this does not happen.

Coins

Coins are comprised of a chain of transaction records of every transfer of the coin. The latest record in the chain shows the public key of the current owner.



Only fans girl can use Jordan’s public key to ensure that he was the one who signed the block (with his private key), because when decrypted the message should be the same as the hash of the previous block!

Double Spending

While the previous design is useful for tracking the ownership of a coin, there is nothing to stop a coin's owner from creating two transaction blocks double spending the same coin.

However, if we were to have a publicly visible ordered log of all transactions, the user on the receiving end of the transaction could see that the coin was previously spent, and reject the payment. This is challenging because typically ordering events requires some sort of central server!

Blockchain

A set of blocks, acting as a public ledger (record of transactions) for all coins in the network, where each block contains:

- A hash of the previous block in the chain
- Some transactions
- A nonce (used to prove validity of the block)

Each node keeps a copy of the blockchain, and every time a node wants to add a block it must broadcast it to all the other nodes. Since all transactions will be in the blockchain, we can ensure that nobody will be able to double spend.

Adding a Block

- Peer (node in network) receives new transactions and adds them into block
- To add a block to the blockchain the peer must mine the block
  - Use some amount of CPU power to determine the nonce (proof of work)
  - Find x such that hash(list_of_transactions, previous_block_hash, x) starts with n leading zeros
    - Parameter n can be adjusted over time to keep the rate of mined blocks relatively constant
- After nonce is found block is broadcast to other peers

Validating Blocks

Once peers receive a block, they need to make sure it is valid:

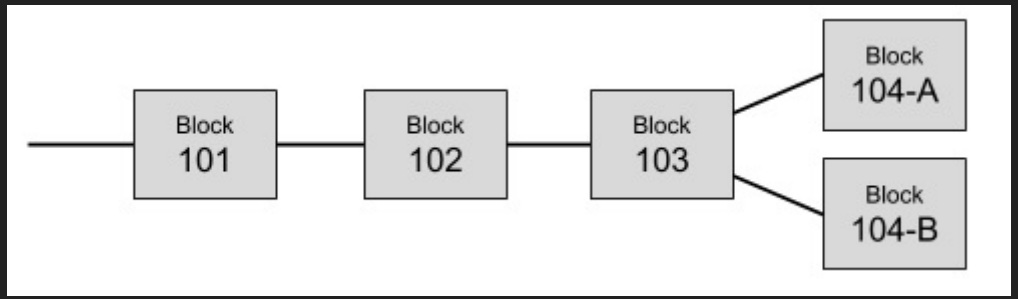
- Hash of the new block has the proper number of leading zeros
- Previous block hash points to existing block in chain
- Transactions in the block are valid
  - No other record for the coin has the same hash of a previous transaction
  - Valid transaction signature

Peers show that they have accepted a block by adding it to their blockchain and creating a new block which references this block as the previous one

Forks in the Blockchain

Sometimes, there are times where forks may arrive in the blockchain:

- Two peers find the nonce of a block at the same time and so some nodes process them in different orders than others
- One malicious peer sends a block to a subset of nodes and a different block to another subset



Resolving Conflicts

Peers will continue to add blocks to whichever branch of the fork that they received first. However, if it sees that another branch has gotten longer it will abandon its current shorter branch and use the end of the other branch as the previous block for any new blocks it creates.

Double spending is technically possible during this time. However, most parties that accept bitcoin will wait until a few blocks have been processed after the one holding a given transaction in order to ensure that it is likely the transaction will stay in the blockchain.

Conclusion

Bitcoin is an extremely interesting culmination of a lot of concepts that we have studied, such as building ordered logs, using hashes, and resolving conflicts. However, it has its downsides as well. Bitcoin is extremely slow due to its insistence on only mining a block once per ten minutes, and additionally extremely resource intensive (wasteful) due to causing computers to use a bunch of CPU cycles to not accomplish anything. As a result, many alternative blockchain implementations have sprung up trying to fix these problems, as well as add new features to the blockchain to support items beyond just cryptocurrency.