What I learned from building my own blockchain

Outline

1. Quick overview
2. Double spend problem
3. Payment verification on smartphones
4. Bitcoin is slow!
5. How can I get my transaction into the blockchain?

1. Quick overview -- What is a blockchain?

A blockchain is a distributed ledger

Blocks contain data and are linked by including the hash of the previous block in the current blocks header

2. The double spend problem -- and a solution

Why not just spend my money 100 times?

- proof of work requirement

How does a node know a transaction is valid?

- list of 18 criteria
- the transaction’s syntax and data structure must be correct
- reject if transaction fee would be too low to get into an empty block
- the referenced output must exist and cannot already be spent

3. Payment verification on mobile nodes (i.e. wallet application)

Problem: Most smartphones can't download the whole blockchain (currently 142gb)

Solution: Simple Payment Verification (SPV)

4. Bitcoin is slow

By design, it takes ~10 min for a new block to be mined and a new transaction to be included in that block.

*When you want to buy something with bitcoin, do you have to wait **10 min** for your transactions to be included in the block?*

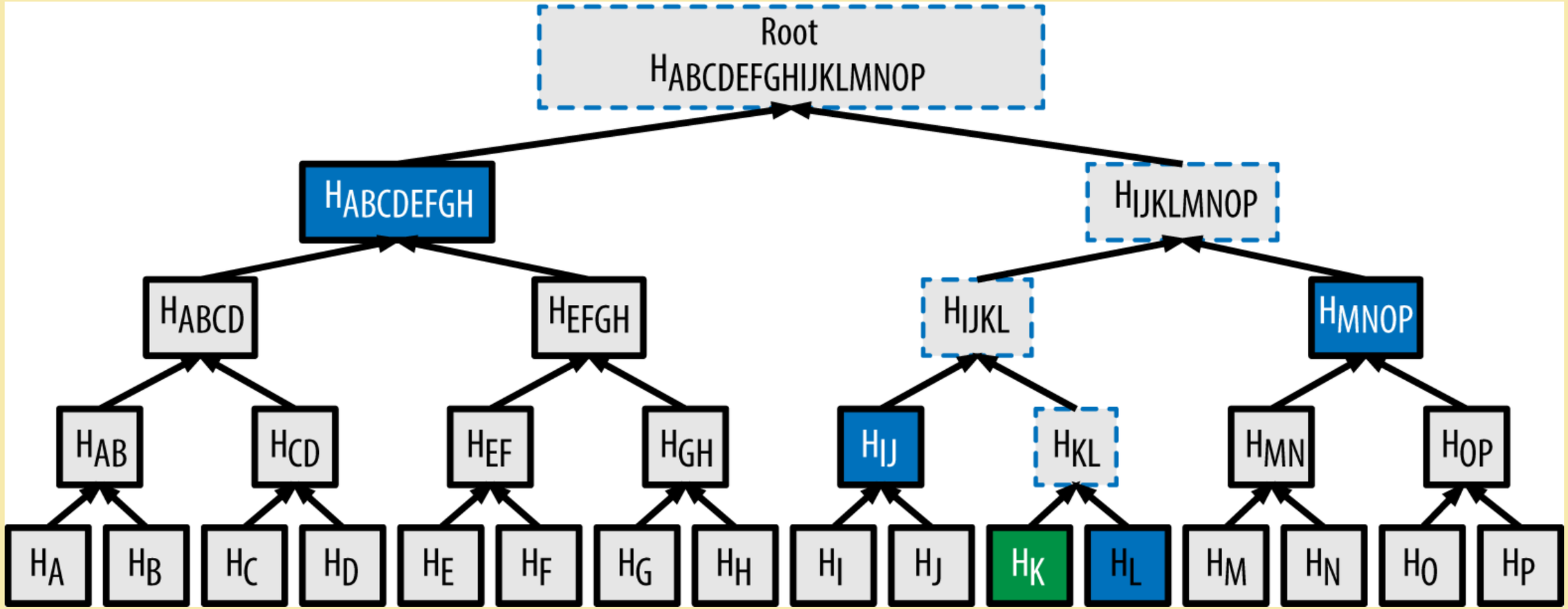
5. How can I get my transaction into the blockchain?

Why do the miners include transactions in the blockchain?

Open questions

- Why can't a node hog down a lucrative transaction?
- Can an SPV node be configured to connect to a full node it trusts or does it need to connect to random nodes?
- Do wallet applications on smartphones also route and validate and propagate transactions and blocks?
- How can the owner of bitcoins proof that they're authorized to spend the UTXO?
- How does a node get notified about a newer version of the blockchain (when another node has successfully mined a new block)?
- And many more...

Bonus slide: Merkle tree



Thank you ✌