Improving Bitcoin light clients with Floresta

What we’ll see today

→ Why running a node?

→ What are the problems

- → Why so much disk space?
- → Why does it take so long to start??
- → Two machines? Multiple programs???

→ Lightweight clientes and their advantages disadvantages

→ Reclaiming space with utreexo a pruning

→ Skipping IBD

→ Keeping track of our balance, privately

→ Embedded node

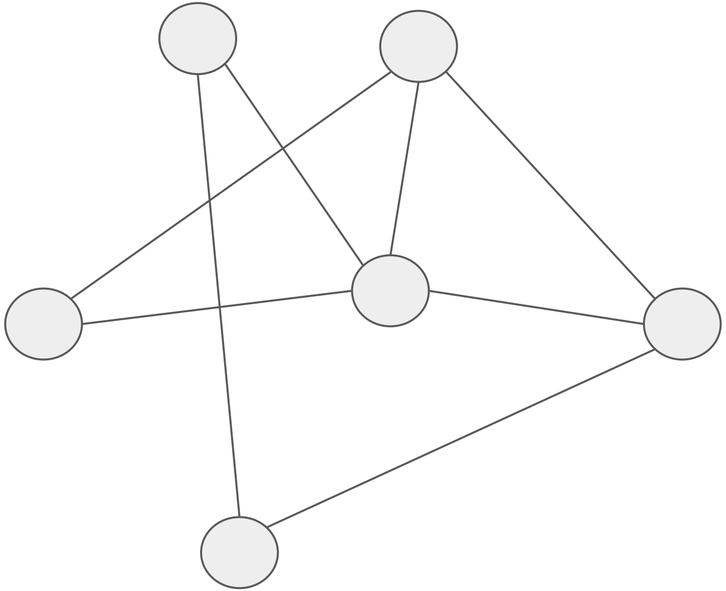
Why running a node?

→ The bitcoin network is a p2p network

→ No servers

→ No trusted third parties

→ Nodes are the backbone of this network



Why running a node?

→ Better privacy

→ Trustlessness

→ No single point of failure

Why running a node?

→ Better privacy

→ Trustlessness

→ No single point of failure

→ But it can be quite challenging to run one!

Why does it takes so much space tho?

There’s two things that eats-up space in a node:

Why does it takes so much space tho?

There’s two things that eats-up space in a node:

Block data

→ the changelog of all transactions that happened in bitcoin’s history

→ We use them to serve other peers and do some processing

Why does it takes so much space tho?

There’s two things that eats-up space in a node:

Block data

→ the changelog of all transactions that happened in bitcoin’s history

→ we use them to serve other peers and do some processing

→ but we don’t really need it

UTXO set

→ all unspent transaction outputs in Bitcoin’s history

→ we need this to validate blocks and transactions as they come

Why do it takes so long??

→ Initial Block Download

→ Download and validate every single block in Bitcoin’s history

→ Costly and time-consuming!

→ Required for new nodes to learn the network state

Two machines? Multiple programs???

→ If you want to use a mobile wallet, you need to have a node at home

→ Very inconvenient

→ what if your node dies while you’re outside??

→ You need to install core + electrum server + tor ….

→ What if everything was in a single program?

Lightweight clients

→ Only require downloading the block headers (80 bytes per block)

→ Assume that the majority of the hash rate is hones

→ Needs external servers to find transactions (privacy problems!)

Meet Floresta!

→ Floresta tries to build better lightweight clients

Meet Floresta!

→ Floresta tries to solve all those problems, making reasonable trade-offs

→ To solve the disk problem, we use pruning and utreexo

Meet Floresta!

→ Floresta tries to solve all those problems, making reasonable trade-offs

- → To solve the disk problem, we use pruning and utreexo
- → We skip IBD using Softchains

Meet Floresta!

→ Floresta tries to solve all those problems, making reasonable trade-offs

→ To solve the disk problem, we use pruning and utreexo

→ We skip IBD using Softchains

→ and finally, Floresta is a library that can be embedded in your favorite wallet

Possible use-cases

→ All-in-one mobile wallets

→ Self contained, low-cost point-of-sale

→ A lighter version of a node distribution

→ and more…

More information about it

→ The source code: github.com/Davidson-Souza/Floresta

→ Technical write-ups on my blog: blog.dlsouza.lol

Thank you!