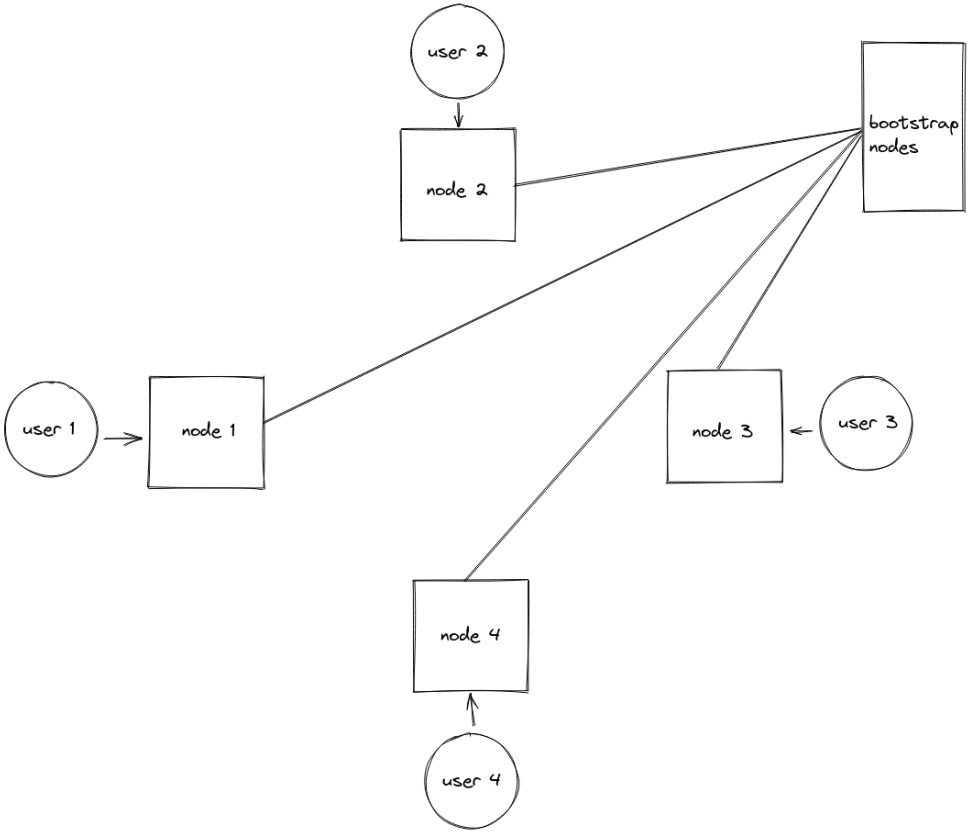
BlockCert Progress Report 1

By Kunal Bhat & Utkarsh Gupta

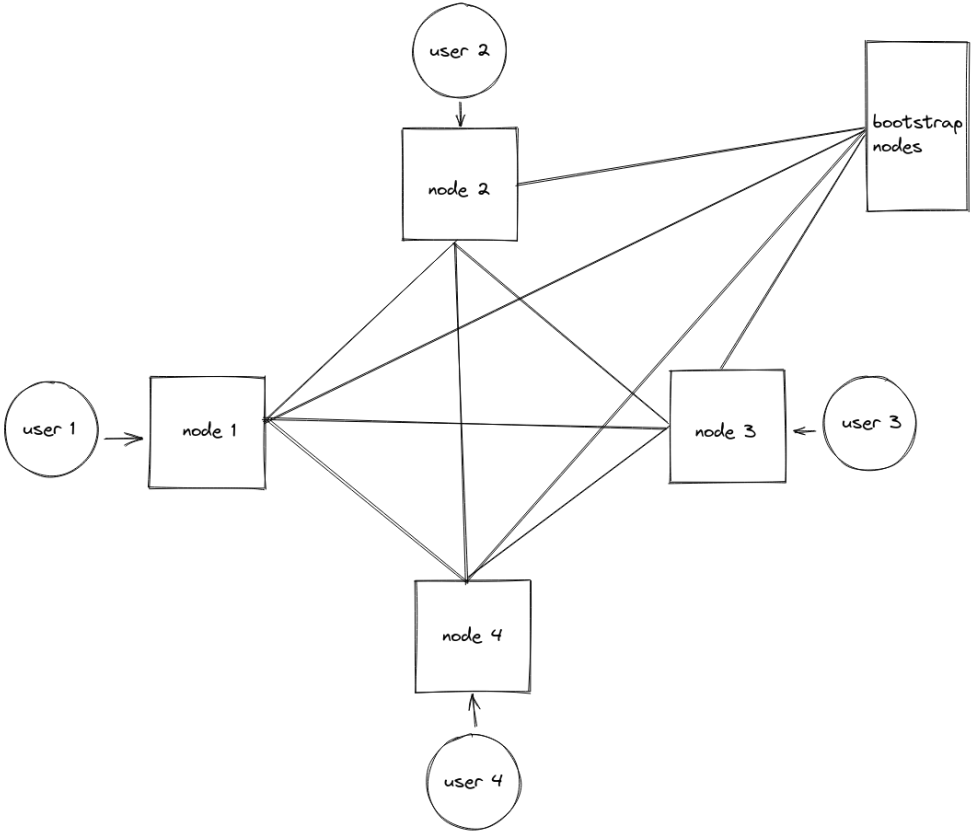
Current Implementation

- Generate an RSA Private and public key in order to sign files.
- Blockchain network that stores file certificates. Stores hash data of files as well as a signature created using the file owner’s private RSA key.
- Users can check the file certificates using the file owner’s public RSA key.
- A simple debug shell for testing functions.

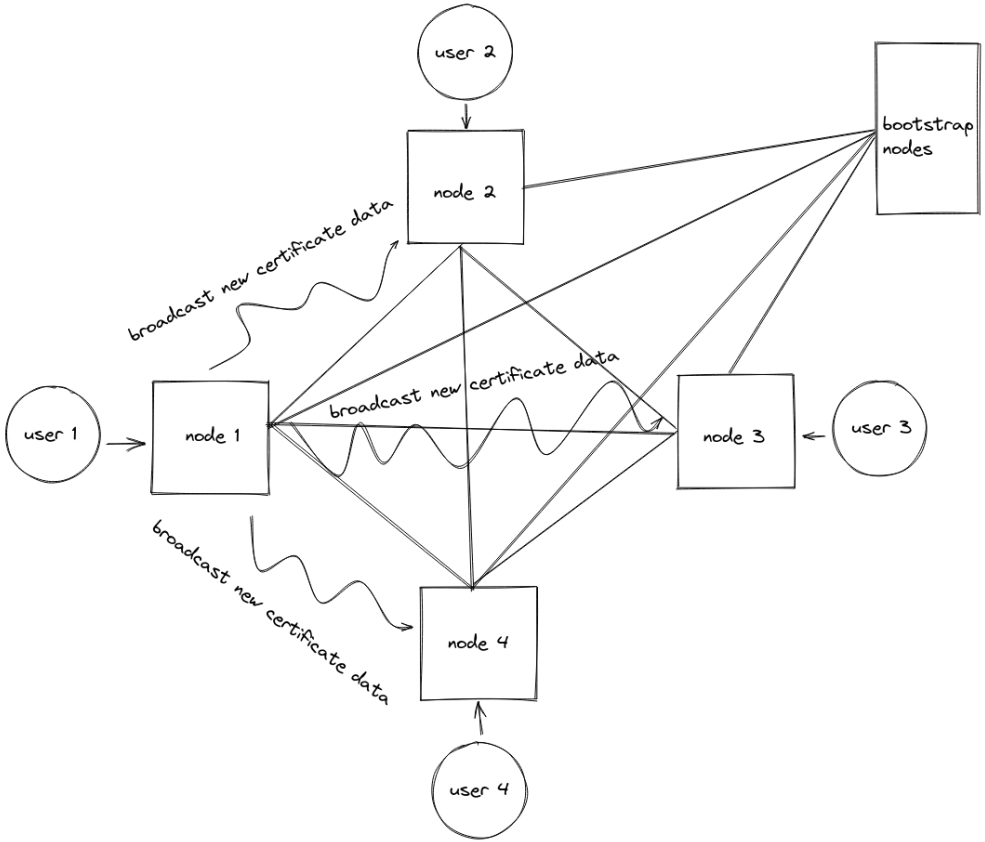
Connecting to IPFS Bootstrap nodes



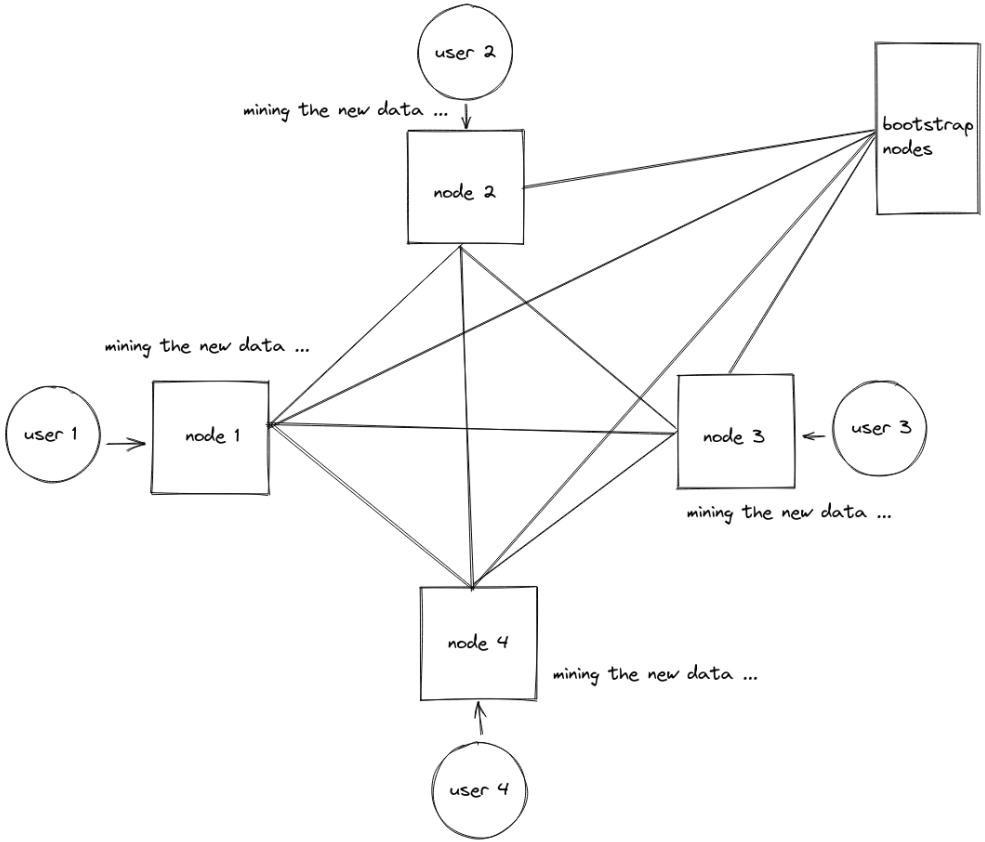
Connecting to Peers in the blockchain network



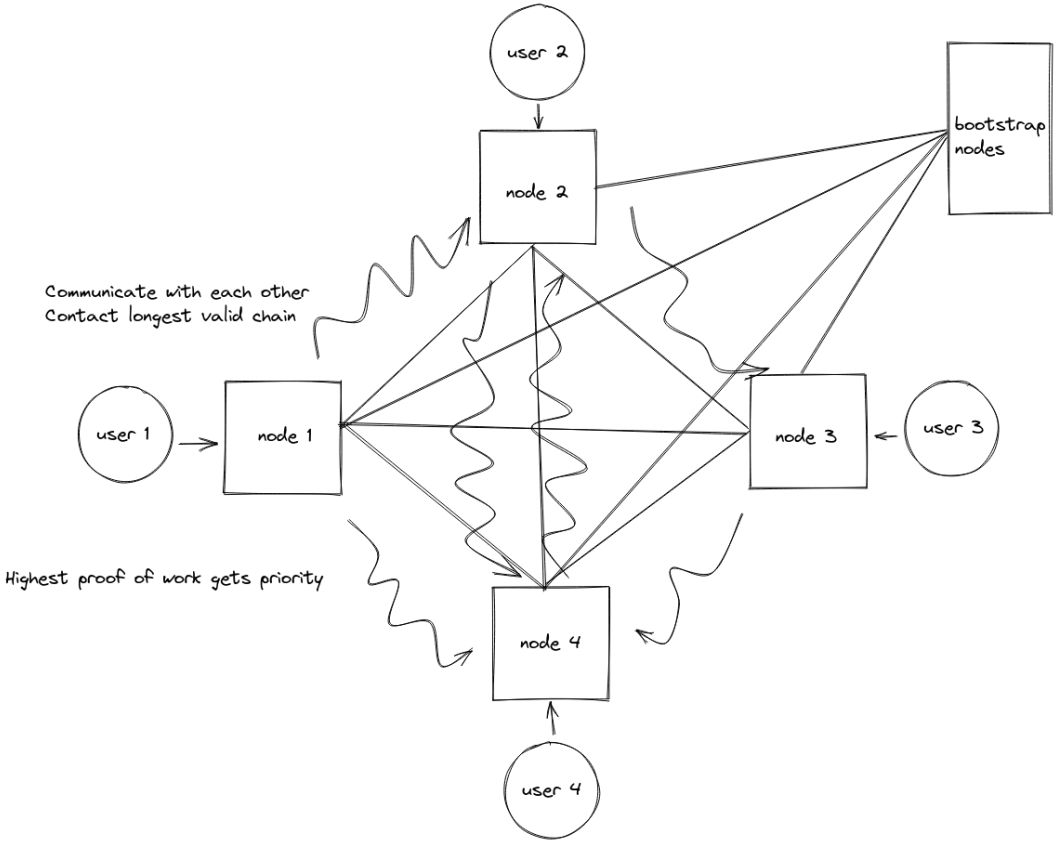
Broadcasting data when a new certificate is issued



Data mined in every single node



Communication between nodes



Next steps

- WIP REST API to communicate with the front-end.
- WIP Flutter front-end with a simple UX that can be used by anyone.
- Better conflict resolution in the blockchain network. Right now it only replaces it with the largest valid chain, which isn’t ideal.

Queries

- Anything else we can do to improve the certificates. Right now it only uses file hashes, maybe adding more metadata?
- How can we improve conflict resolutions in the network?