Network Keys

Network Encryption Key

Each Fhenix instance uses its own Encryption Key. This key is special, and allows users to encrypt their data in such a way that will match the encryption of all the other data on the network.

Did You Know? The public key we refer to here is aglobal key that is used to encrypt data being sent to the network. It is not the same as thetransactional public key that is used by fhenix.js to unseal data! If you're using fhenix.js you don't need to worry about this, as the public key fetching is already done automatically by the library.

Fetching the Public Key Manually

However, if you're using interfacing with Fhenix directly, you'll need to fetch the public key from the network you're connecting to. This can be done by calling thegetPublicKey function on the network you're connecting to.

The Public Key is constant for the lifetime of the network, but still has to be fetched once by the user to be able to encrypt data. To do this, we use a special precompiled function that can be accessed programmatically in the following way:

- ethers.js
- Web3.js

```
let result =

await provider . call ( { to :

"0x0000000000000000000000000000000000000080" , } ) ; let result =

await web3 . eth . call ( { to :

"0x0000000000000000000000000000000000000080" } ) ;
```

Edit this page

Previous End-to-End Example Next Catching Errors