zkDocs

A way to not reveal your personal data, while e-signing legal documents and contracts in the web2 world!

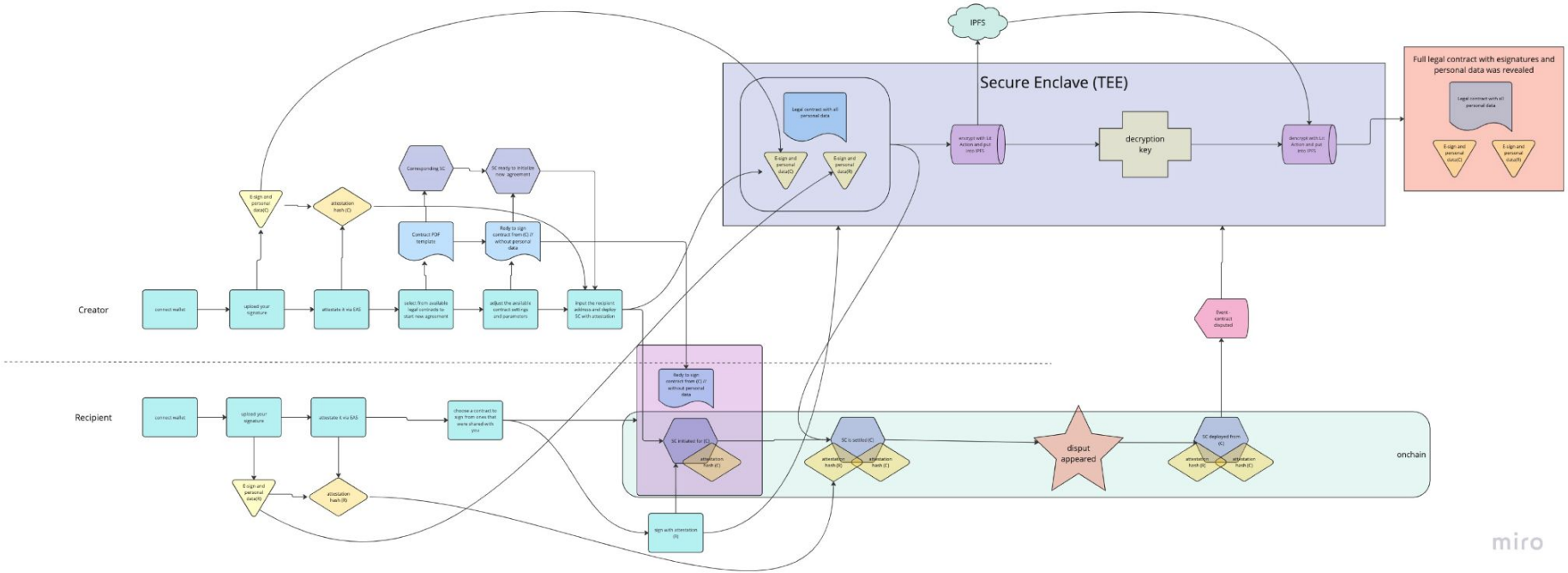
About project

Our aim is to increase people’s privacy in the legal agreements with the help of blockchain technologies!

A lot of the time there is no need in so much personal data sharing between the counterparties. This is usually necessary, when you interact with the law and the government, and usually only when something is going against the agreement.

We can preserve all the personal data safely and privately before that moment!

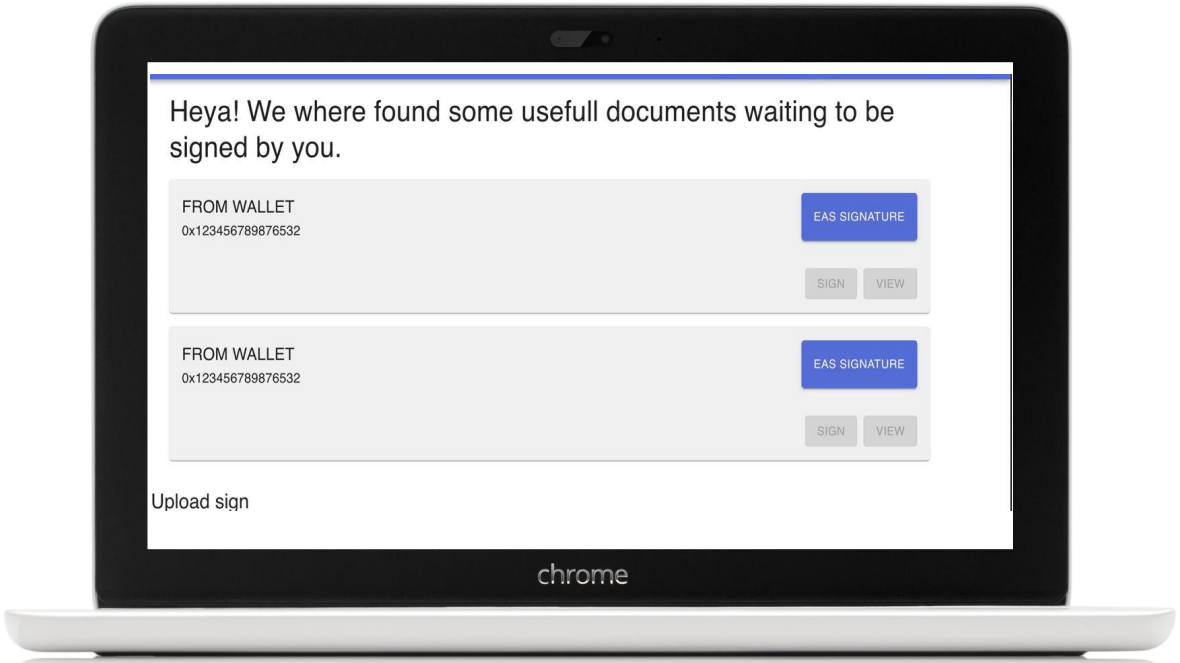
Project architecture



Technologies used

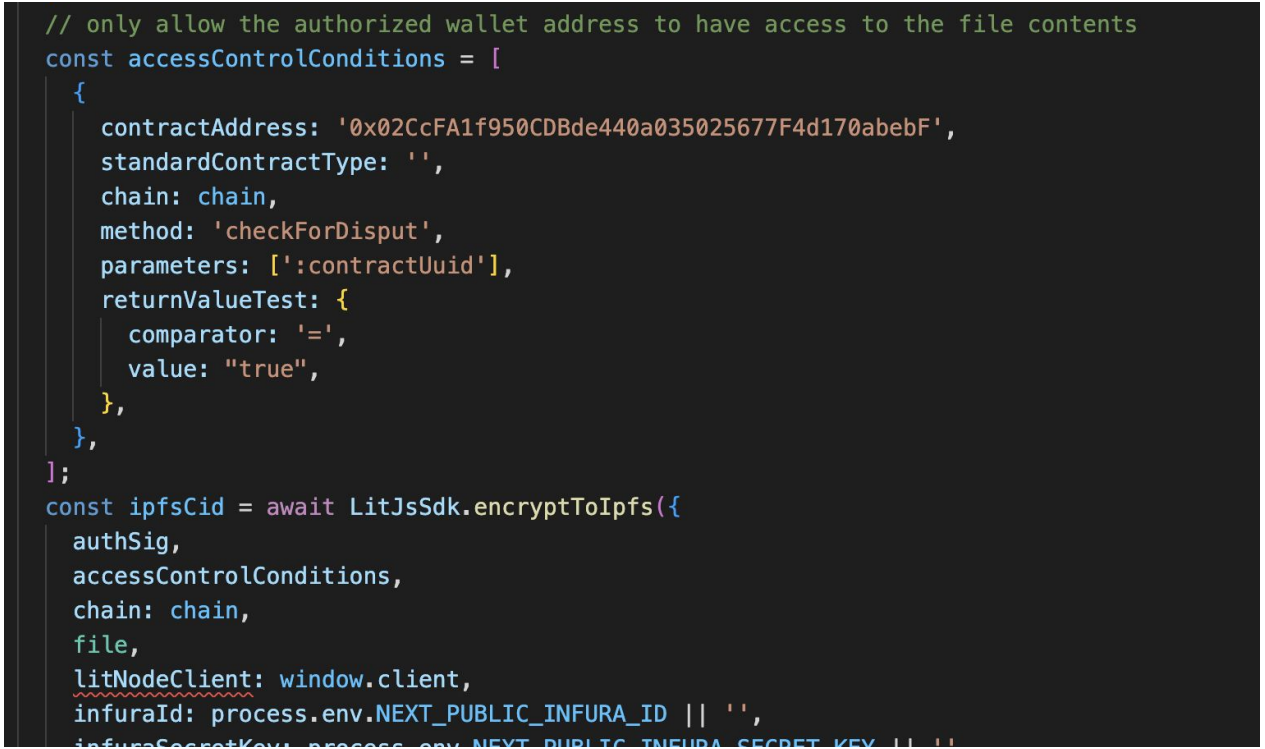
EAS

EAS enable users to create attestations for their eSignatures without revealing personal data. Data integrity then can be validated by comparing hashes of eSignature



LIT Protocol

LIT Actions enable users to remain their data secured unless certain condition on-chain are met. Legal contracts with sensitive data are encrypted but may be encrypted if counterparties agreement has been broken.

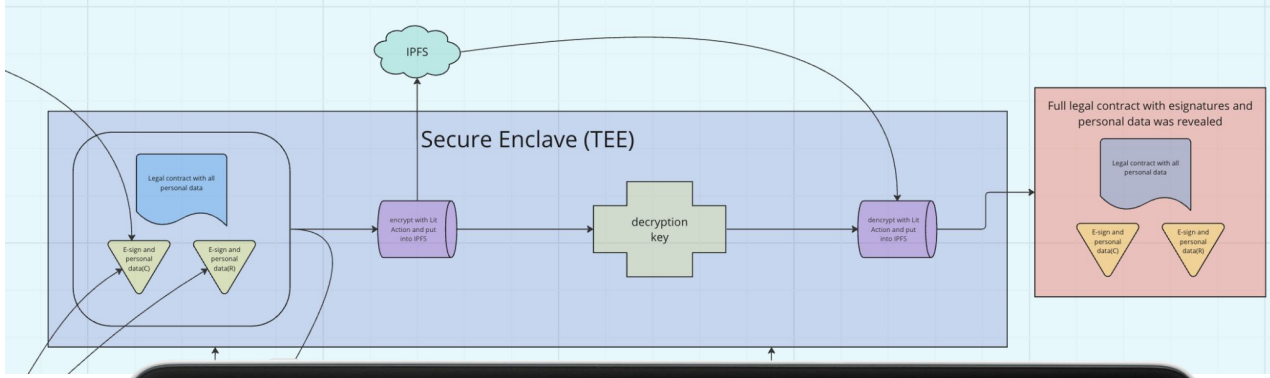


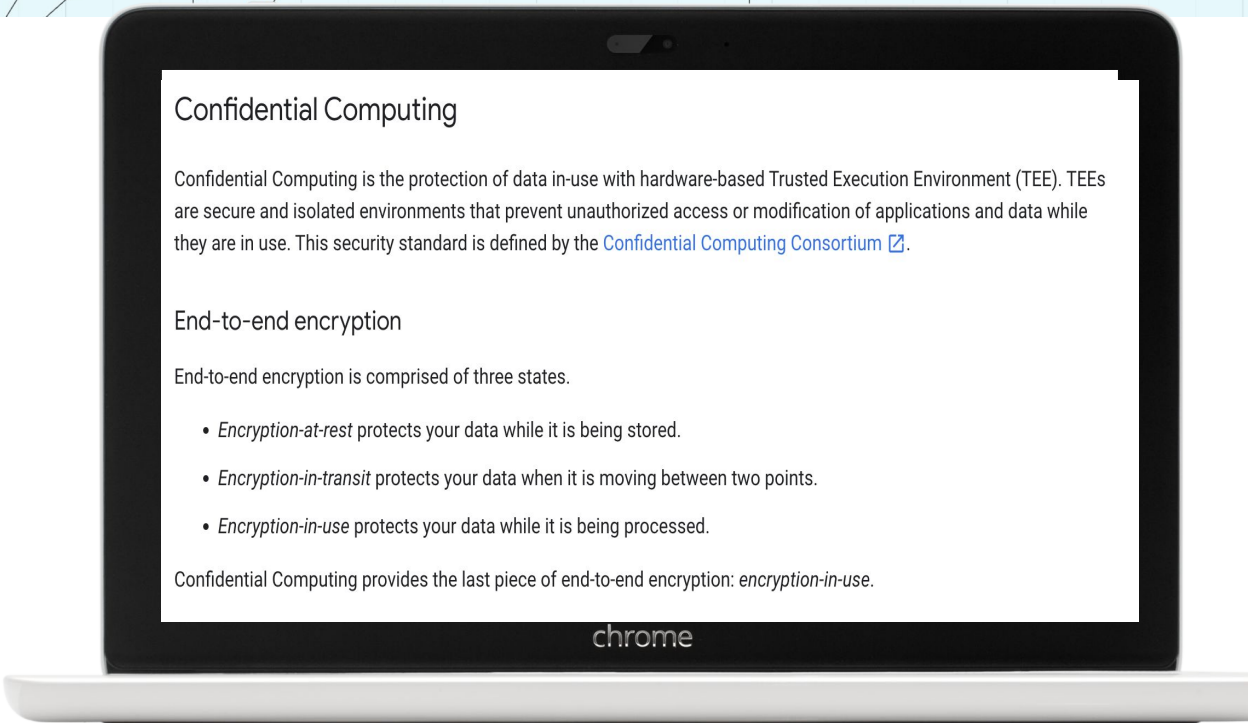
```
// only allow the authorized wallet address to have access to the file contents
const accessControlConditions = [
  {
    contractAddress: '0x02CcFA1f950CDBde440a035025677F4d170abebF',
    standardContractType: '',
    chain: chain,
    method: 'checkForDisput',
    parameters: [':contractUuid'],
    returnValueTest: {
      comparator: '=',
      value: "true",
    },
  },
];
const ipfsCid = await LitJsSdk.encryptToIpfs({
  authSig,
  accessControlConditions,
  chain: chain,
  file,
  litNodeClient: window.client,
  infuraId: process.env.NEXT_PUBLIC_INFURA_ID || '',
```

Confidential Computing (TEE from Google)

For the hackathon POC, we've used the Confidential Computing by Google. It allowed us to easily use trusted environments to protect and interact with our sensitive data - esignatures and personal data on legal contract.

Our secure enclave encrypts the data and stores it to IPFS and only keeps decryption key for the case if some dispute will appear and counterparties will need to reveal the legal agreement with all of the personal data.





Chains Deployed

Chains

```
### Testnet
- [Sepolia Core](https://sepolia.etherscan.io/address/0x02CcFA1f950CDBde440a035025677F4d170abebF)
- [Sepolia Scheduler](https://sepolia.etherscan.io/address/0x02CcFA1f950CDBde440a035025677F4d170abebF)
- [Celo Core](https://alfajores.celoscan.io/address/0x32E2735553C54b19938907e387c47f36B7B89cC8)
- [Celo Scheduler](https://alfajores.celoscan.io/address/0xc7256041d9f92Ca126c1140b9359d63f8C4F703b)
- [Gnosis Core](https://gnosis-chiado.blockscout.com/address/0x02CcFA1f950CDBde440a035025677F4d170abebF)
- [Gnosis Scheduler](https://gnosis-chiado.blockscout.com/address/0x32E2735553C54b19938907e387c47f36B7B89cC8)
- [Polygon zkEVM Core](https://testnet-zkevm.polygonscan.com/address/0x32E2735553C54b19938907e387c47f36B7B89cC8)
- [Polygon zkEVM Scheduler](https://testnet-zkevm.polygonscan.com/address/0xc7256041d9f92Ca126c1140b9359d63f8C4F703b)
- [Linea Core](https://explorer.goerli.linea.build/address/0x32E2735553C54b19938907e387c47f36B7B89cC8)
- [Linea Scheduler](https://explorer.goerli.linea.build/address/0xc7256041d9f92Ca126c1140b9359d63f8C4F703b)
- [Mantle Core](https://explorer.testnet.mantle.xyz/address/0x32E2735553C54b19938907e387c47f36B7B89cC8)
- [Mantle Scheduler](https://explorer.testnet.mantle.xyz/address/0xc7256041d9f92Ca126c1140b9359d63f8C4F703b)
```