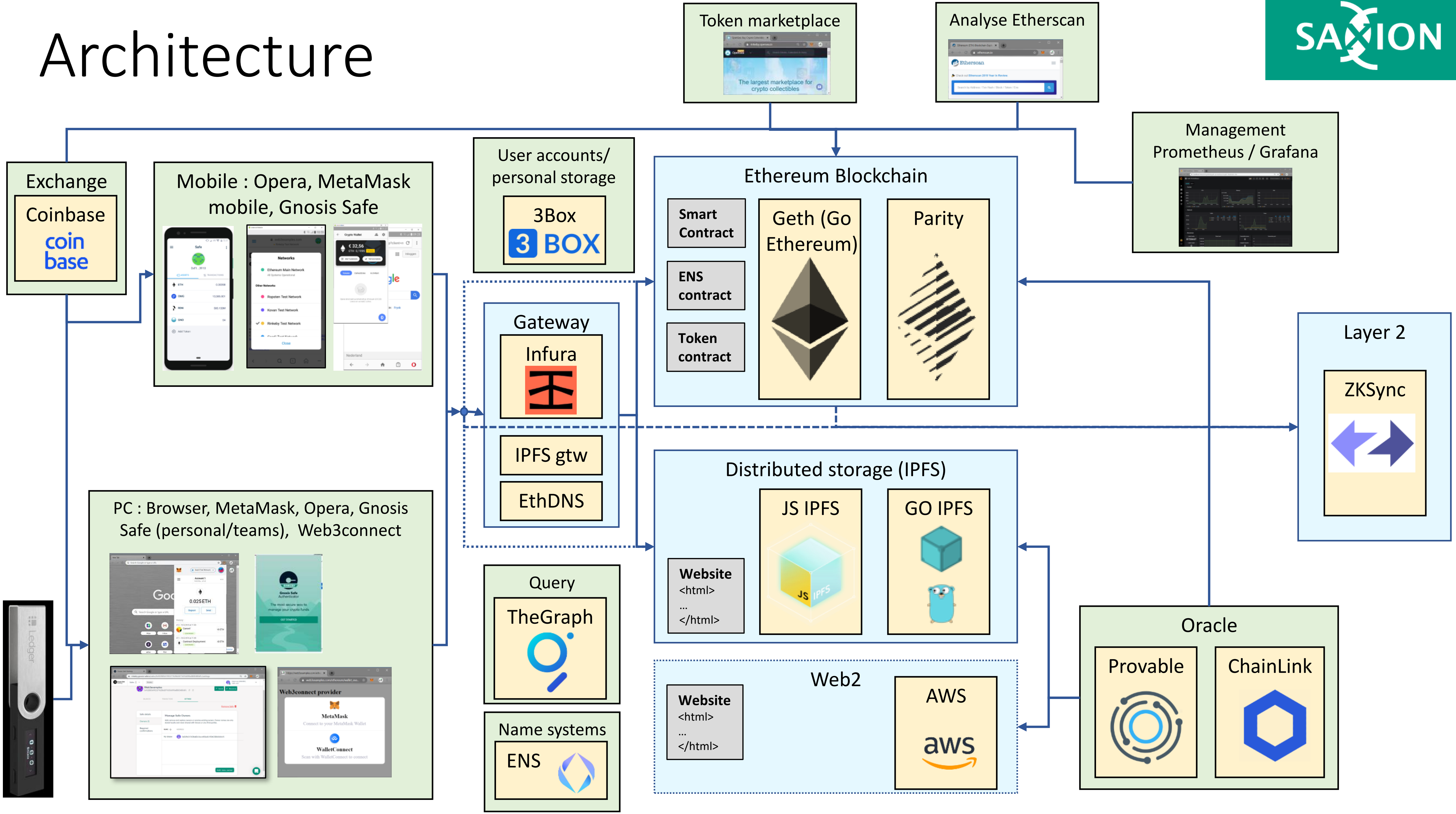
Workshop Ethereum

Oracles / The Graph / Layer2

Sheets
https://web3examples.com/Saxion

Architecture



Token marketplace

The largest marketplace for crypto collectibles

Analyse Etherscan

Management Prometheus / Grafana

Exchange

Coinbase

Mobile : Opera, MetaMask mobile, Gnosis Safe

User accounts/ personal storage

3Box

Ethereum Blockchain

Smart Contract

ENS contract

Token contract

Geth (Go Ethereum)

Parity

Gateway

Infura

IPFS gtw

EthDNS

Layer 2

ZKSync

PC : Browser, MetaMask, Opera, Gnosis Safe (personal/teams), Web3connect

Web3connect provider

MetaMask

WalletConnect

Distributed storage (IPFS)

Website
<html>
…
</html>

JS IPFS

GO IPFS

Query

TheGraph

Name systems

ENS

Web2

Website
<html>
…
</html>

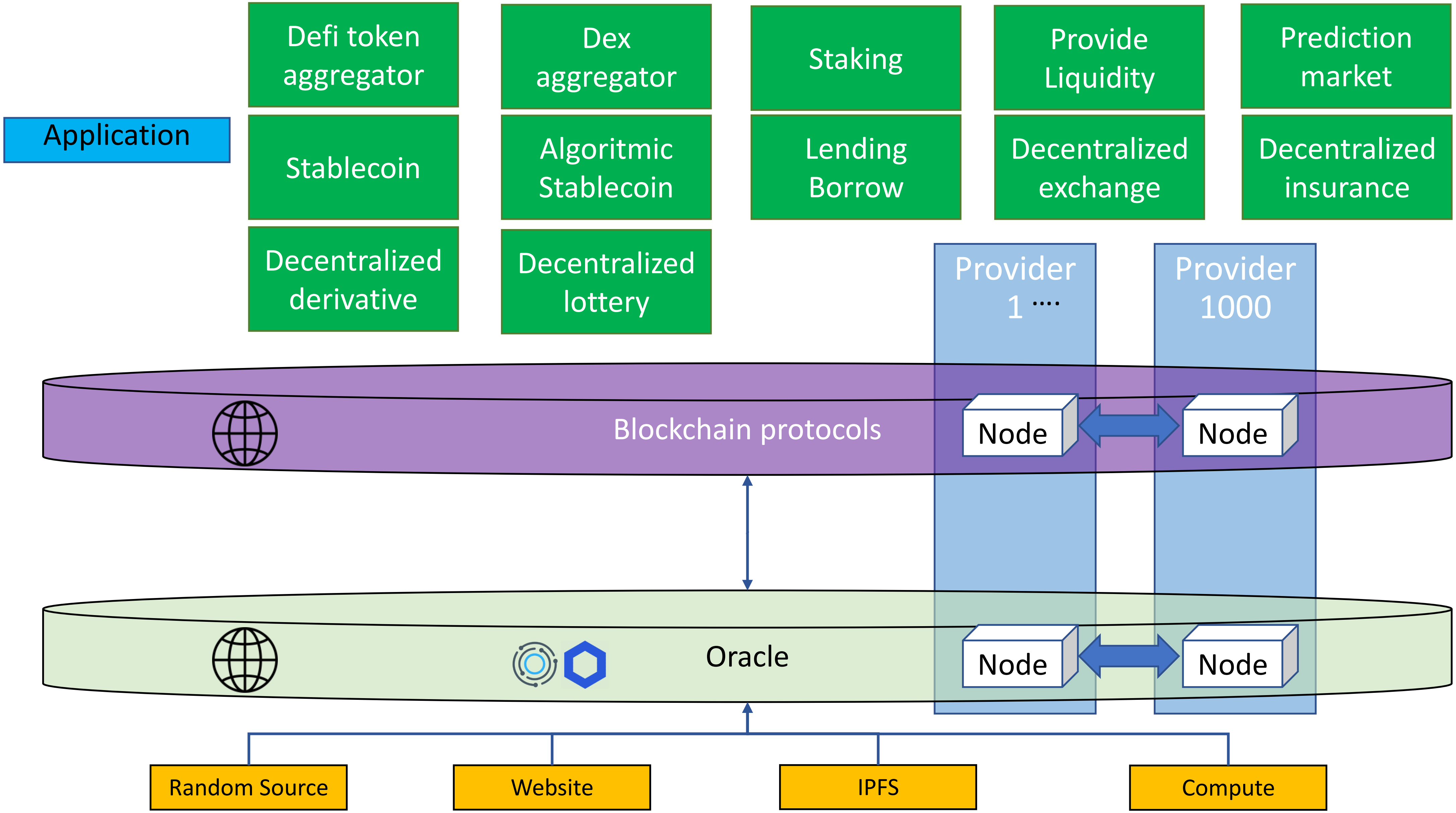
AWS

Oracle

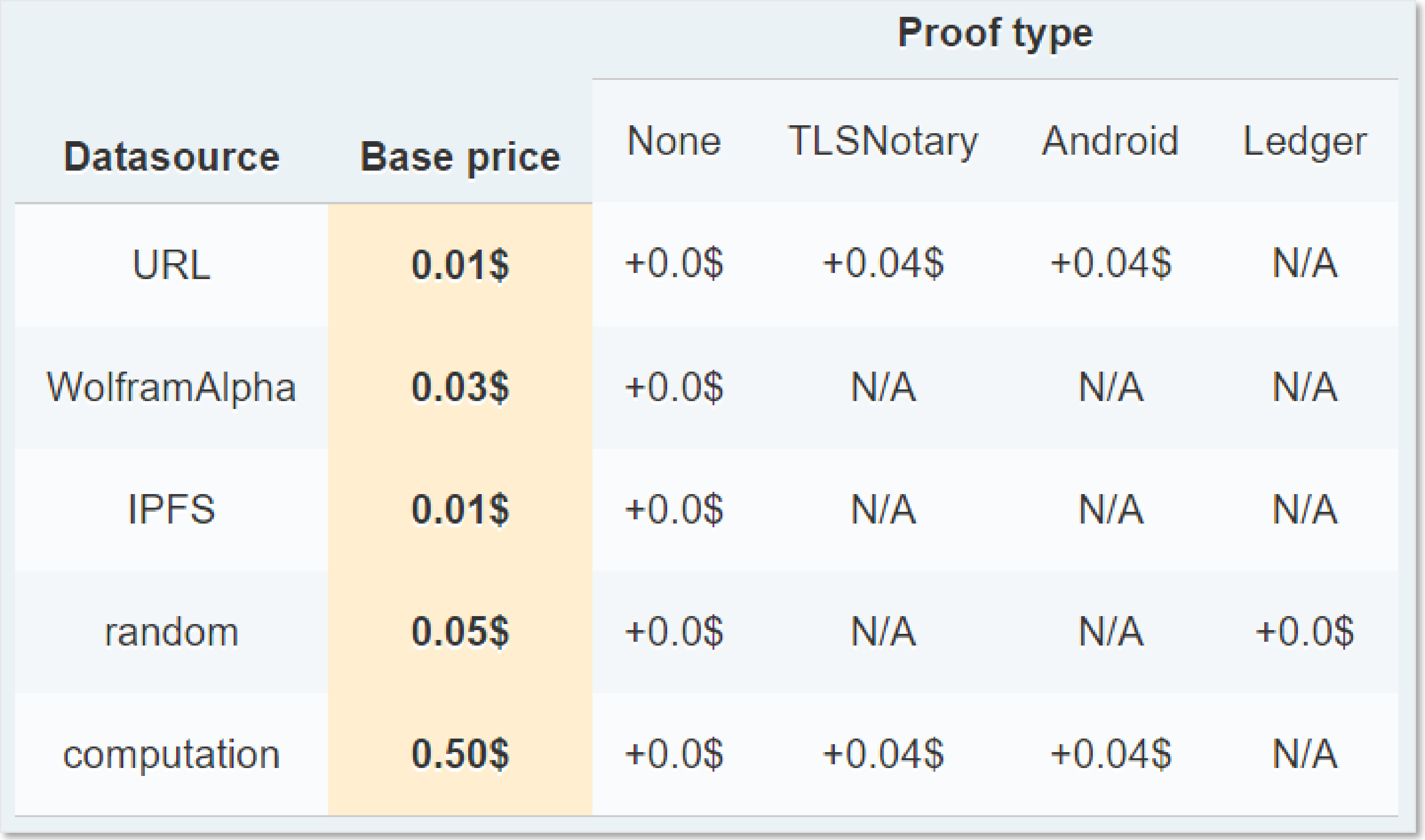
Provable

ChainLink

Oracle architecture



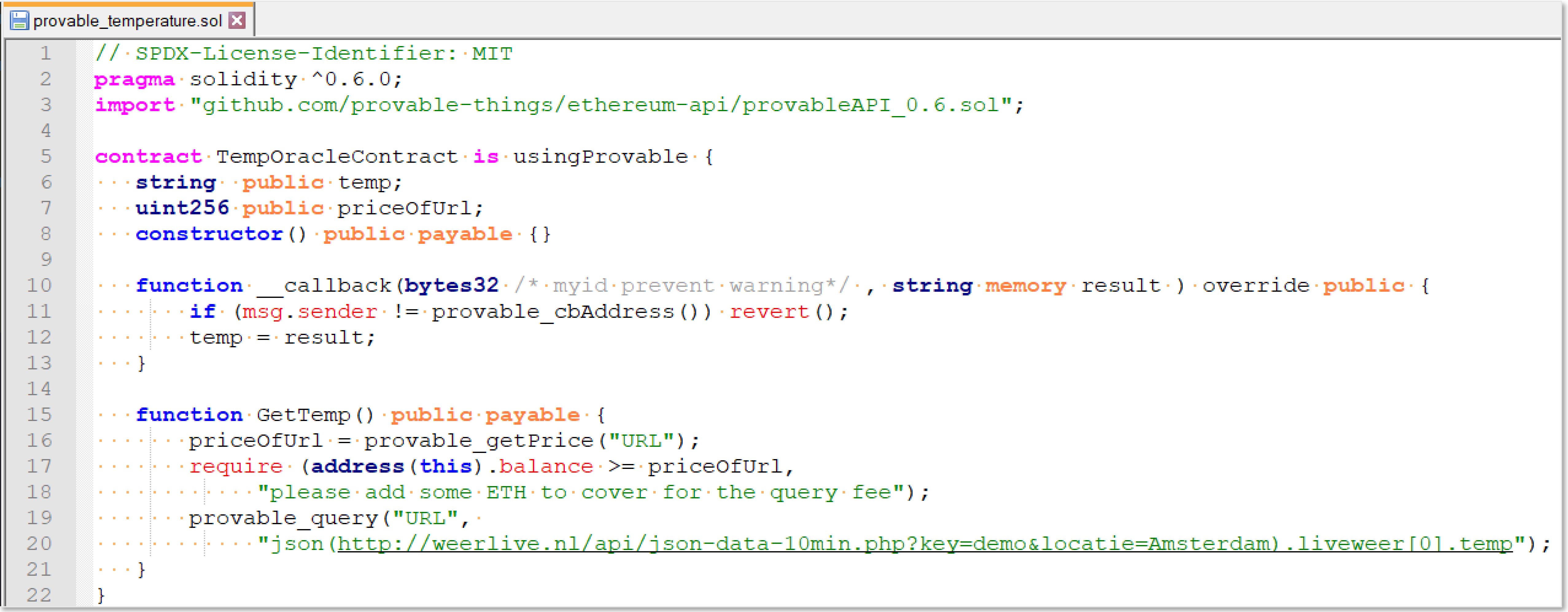
Pricing



		Proof type			
Datasource	**Base price**	None	TLSNotary	Android	Ledger
URL	**0.01$**	+0.0$	+0.04$	+0.04$	N/A
WolframAlpha	**0.03$**	+0.0$	N/A	N/A	N/A
IPFS	**0.01$**	+0.0$	N/A	N/A	N/A
random	**0.05$**	+0.0$	N/A	N/A	+0.0$
computation	**0.50$**	+0.0$	+0.04$	+0.04$	N/A

https://docs.provable.xyz/#pricing-advanced-datasources-call-fee

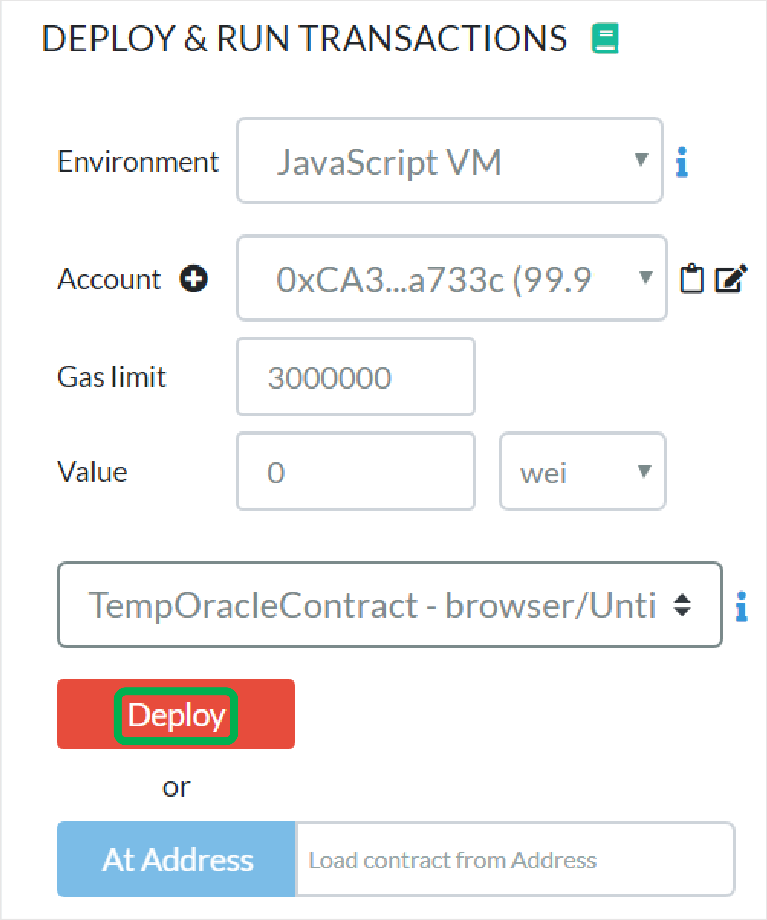
Temperature (url) oracle with Provable



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.6.0;
import "github.com/provable-things/ethereum-api/provableAPI_0.6.sol";

contract TempOracleContract is usingProvable {
   string  public temp;
   uint256 public priceOfUrl;
   constructor() public payable {}

   function  __callback(bytes32 /* myid prevent warning*/ , string memory result ) override public {
        if (msg.sender != provable_cbAddress()) revert();
        temp = result;
   }

   function GetTemp() public payable {
        priceOfUrl = provable_getPrice("URL");
        require (address(this).balance >= priceOfUrl,
                "please add some ETH to cover for the query fee");
        provable_query("URL", 
                "json(http://weerlive.nl/api/json-data-10min.php?key=demo&locatie=Amsterdam).liveweer[0].temp");
   }
}
```

https://github.com/web3examples/ethereum/blob/master/oracle_examples/provable_temperature.sol

Temperature (url) oracle with Provable


DEPLOY & RUN TRANSACTIONS

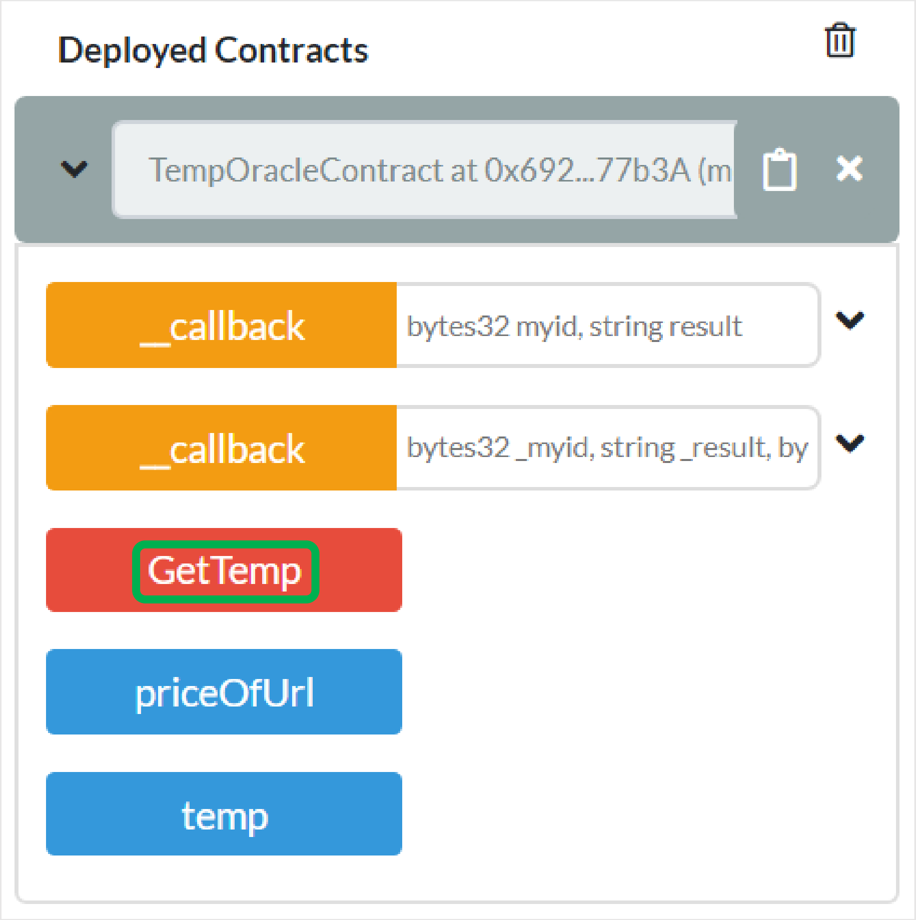
Environment: JavaScript VM

Account: 0xCA3...a733c (99.9

Gas limit: 3000000

Value: 0 wei

TempOracleContract - browser/Unti


Deployed Contracts

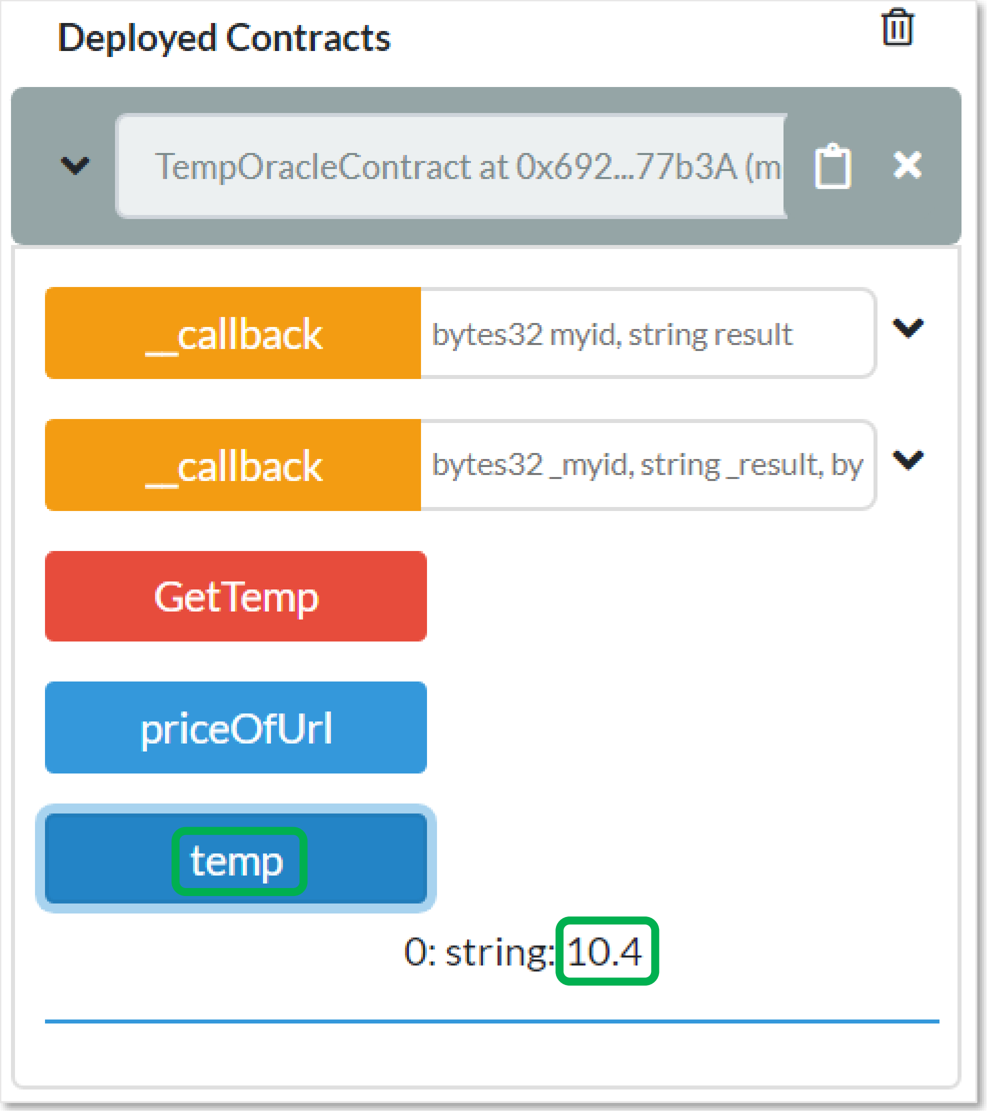
TempOracleContract at 0x692...77b3A (m

_callback: bytes32 myid, string result

_callback: bytes32 _myid, string _result, by

https://github.com/web3examples/ethereum/blob/master/oracle_examples/provable_temperature.sol

Result



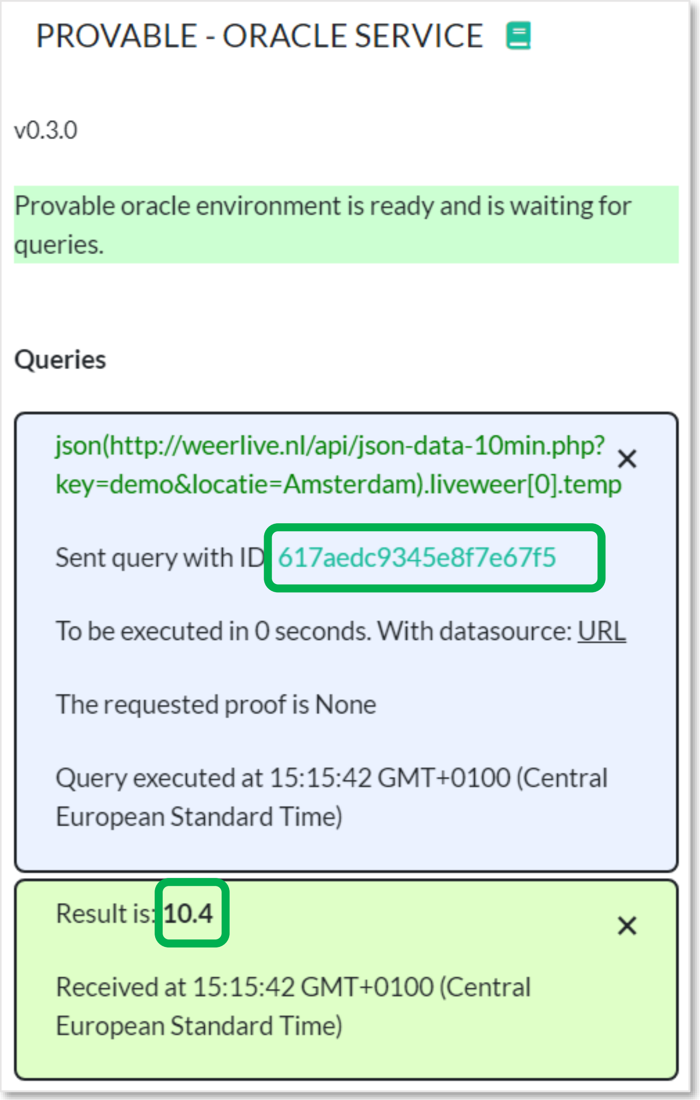
Deployed Contracts

TempOracleContract at 0x692...77b3A (m

_callback
bytes32 myid, string result
_callback
bytes32 _myid, string _result, by
GetTemp
priceOfUrl
temp

```
0: string: 10.4
```

Provable status in remix



PROVABLE - ORACLE SERVICE

v0.3.0

Provable oracle environment is ready and is waiting for queries.

Queries

json(http://weerlive.nl/api/json-data-10min.php?key=demo&locatie=Amsterdam).liveweer[0].temp

Sent query with ID 617aedc9345e8f7e67f5

To be executed in 0 seconds. With datasource: URL

The requested proof is None

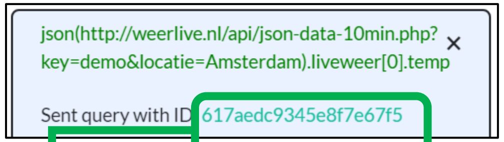
Query executed at 15:15:42 GMT+0100 (Central European Standard Time)

Result is: **10.4**

Received at 15:15:42 GMT+0100 (Central European Standard Time)

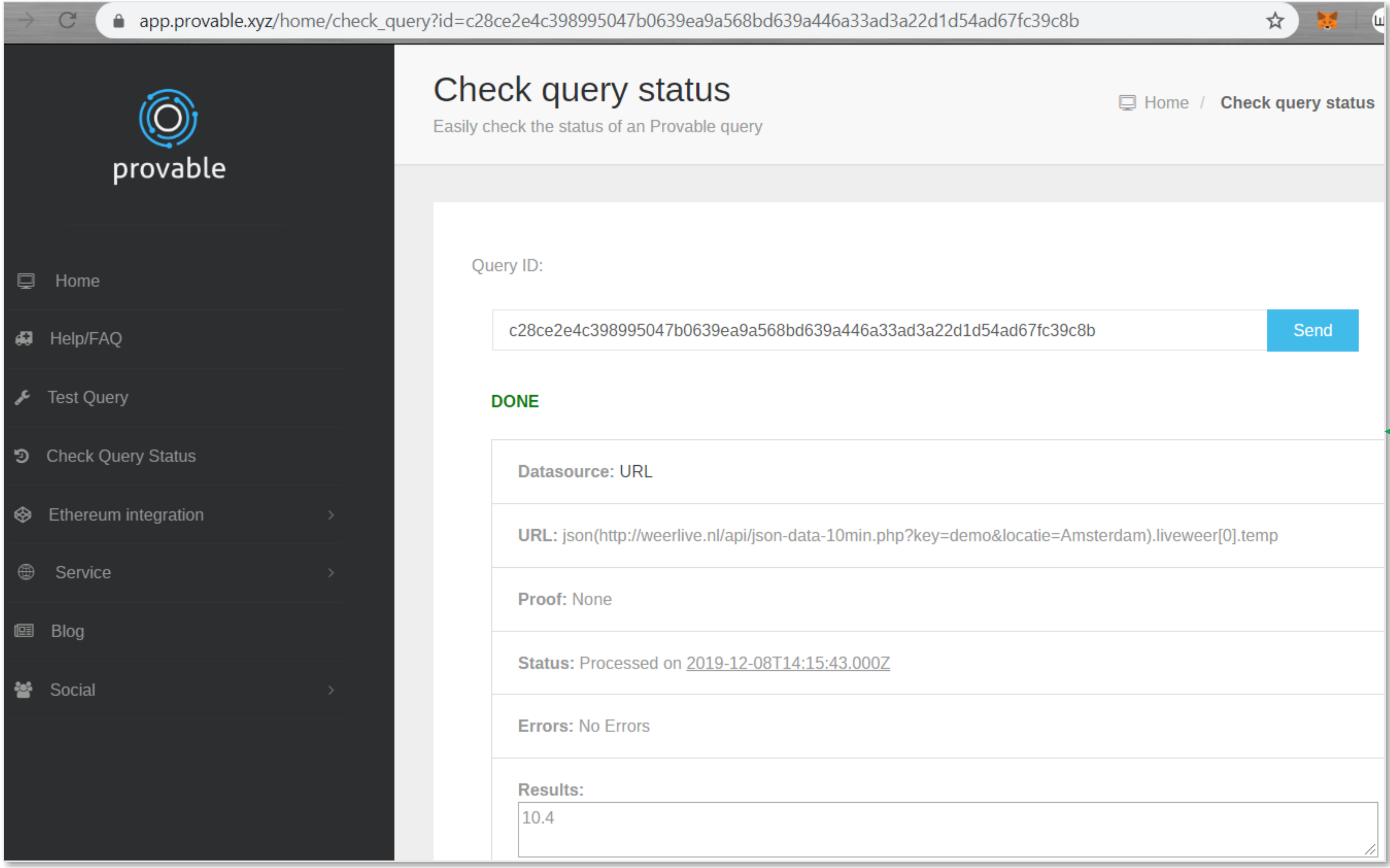
Check status

Go to Provable query with ID: 0x617aedc9345e8f7e67f590fc4abfe60c54cb520e7a41737385e32d283e426398



json(http://weerlive.nl/api/json-data-10min.php?key=demo&locatie=Amsterdam).liveweer[0].temp

Sent query with ID 617aedc9345e8f7e67f5



app.provable.xyz/home/check_query?id=c28ce2e4c398995047b0639ea9a568bd639a446a33ad3a22d1d54ad67fc39c8b
provable
Home
Help/FAQ
Test Query
Check Query Status
Ethereum integration
Service
Blog
Social
Home / Check query status
Send

Check query status

Easily check the status of an Provable query

Query ID:

c28ce2e4c398995047b0639ea9a568bd639a446a33ad3a22d1d54ad67fc39c8b

DONE

Datasource: URL

URL: json(http://weerlive.nl/api/json-data-10min.php?key=demo&locatie=Amsterdam).liveweer[0].temp

Proof: None

Status: Processed on 2019-12-08T14:15:43.000Z

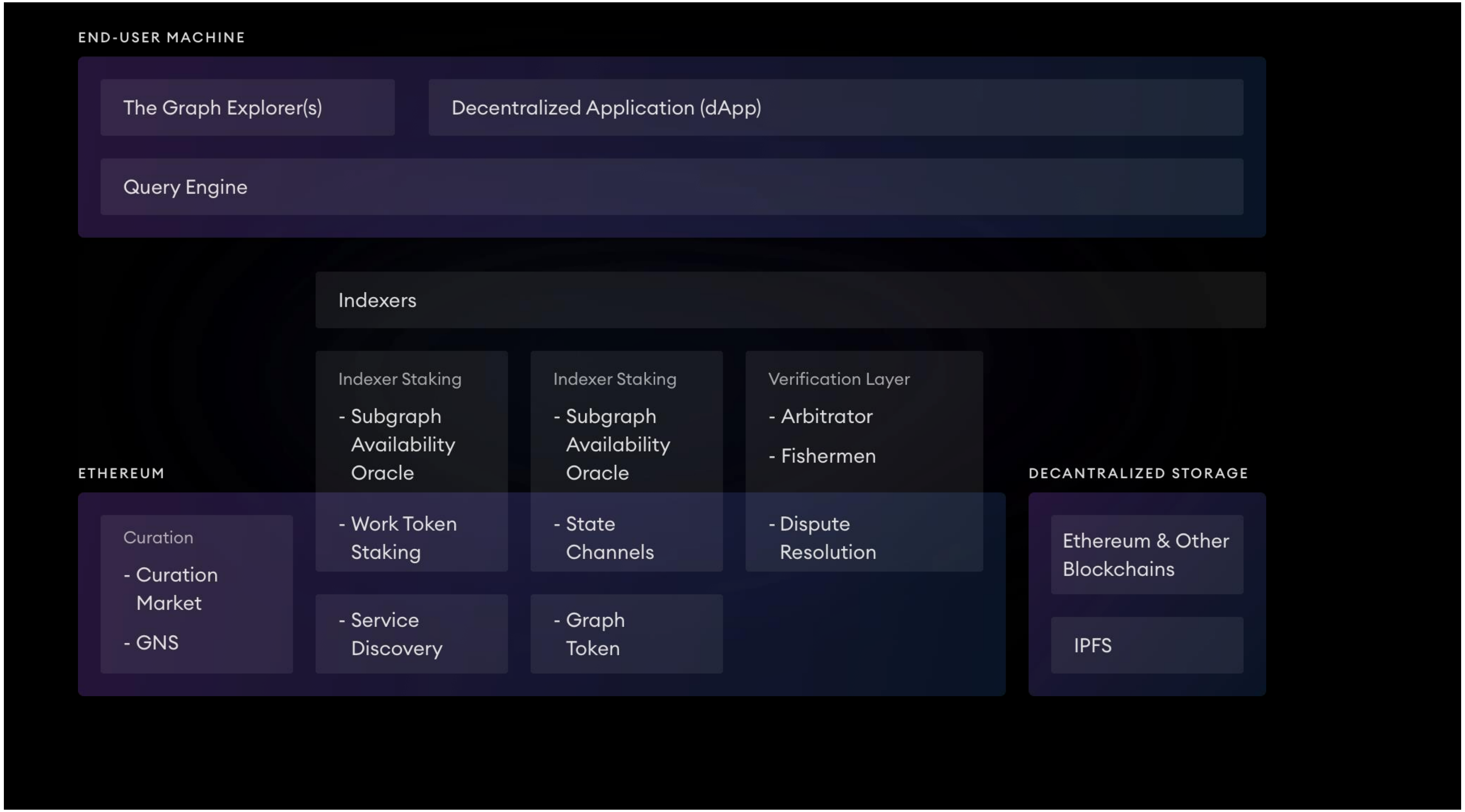
Errors: No Errors

Results:

10.4

https://app.provable.xyz/home/check_query?id=c28ce2e4c398995047b0639ea9a568bd639a446a33ad3a22d1d54ad67fc39c8b

TheGraph



END-USER MACHINE

The Graph Explorer(s)

Decentralized Application (dApp)

Query Engine

Indexers

Indexer Staking

- Subgraph Availability Oracle
- Work Token Staking
- Service Discovery

Indexer Staking

- Subgraph Availability Oracle
- State Channels
- Graph Token

Verification Layer

- Arbitrator
- Fishermen
- Dispute Resolution

ETHEREUM

Curation

- Curation Market
- GNS

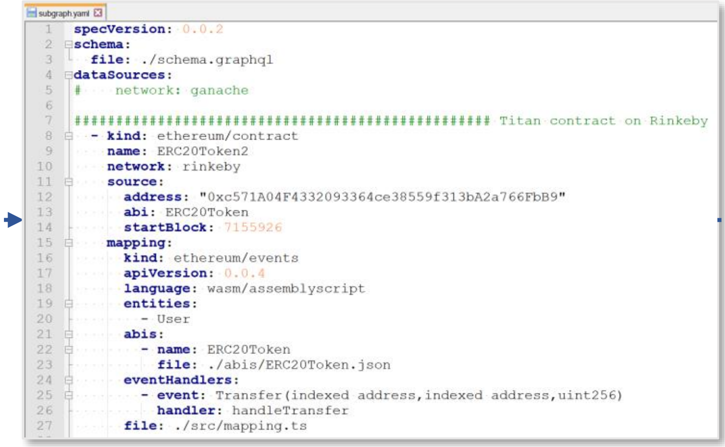
DECANTRALIZED STORAGE

Ethereum & Other Blockchains

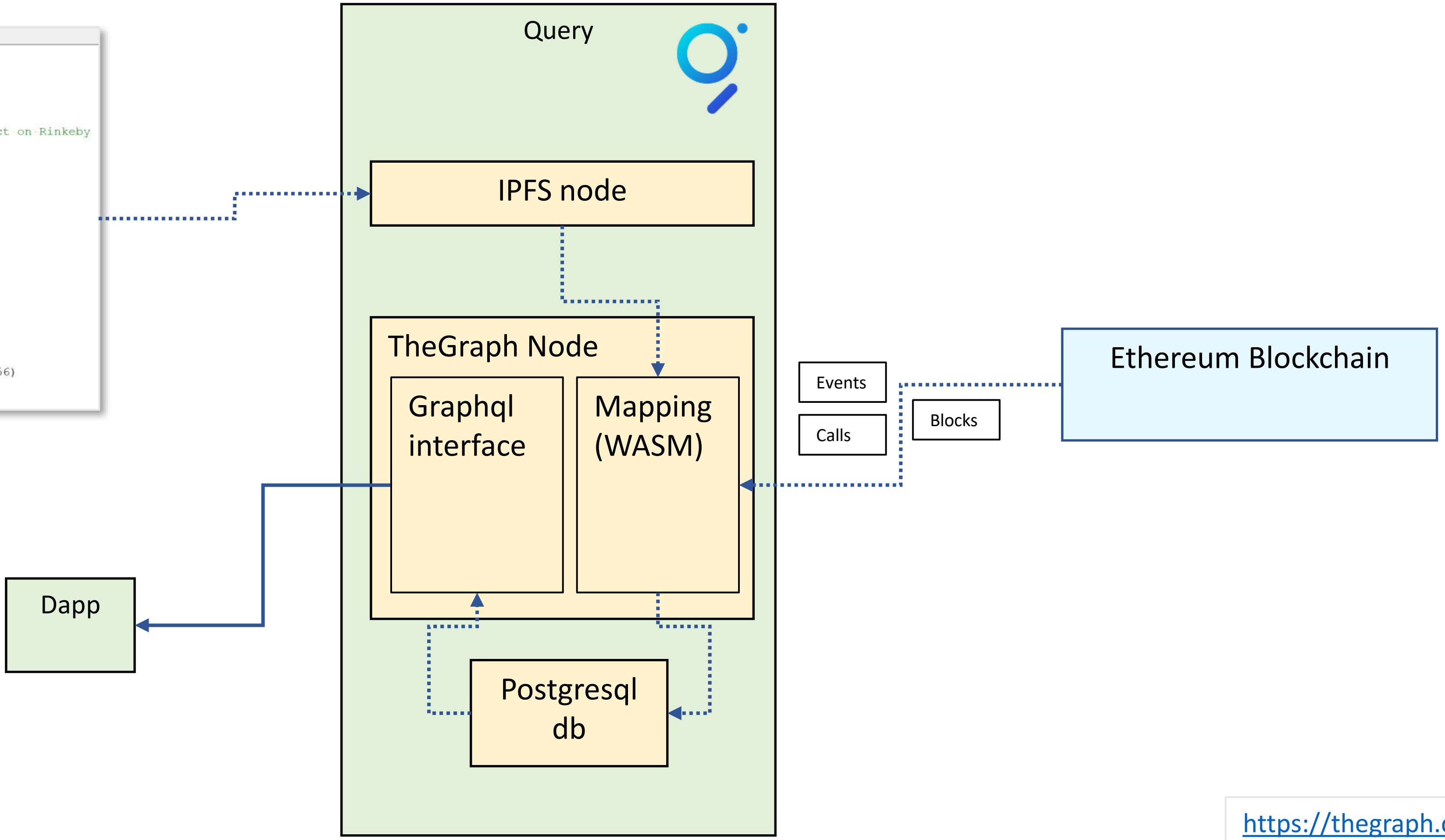
IPFS

The Graph Architecture

Solidity files



```yaml
specVersion: 0.0.2
schema:
  file: ./schema.graphql
dataSources:
#    network: ganache

################################################# Titan contract on Rinkeby
  - kind: ethereum/contract
    name: ERC20Token2
    network: rinkeby
    source:
      address: "0xc571A04F4332093364ce38559f313bA2a766FbB9"
      abi: ERC20Token
      startBlock: 7155926
    mapping:
      kind: ethereum/events
      apiVersion: 0.0.4
      language: wasm/assemblyscript
      entities:
        - User
      abis:
        - name: ERC20Token
          file: ./abis/ERC20Token.json
      eventHandlers:
        - event: Transfer(indexed address,indexed address,uint256)
          handler: handleTransfer
      file: ./src/mapping.ts
```

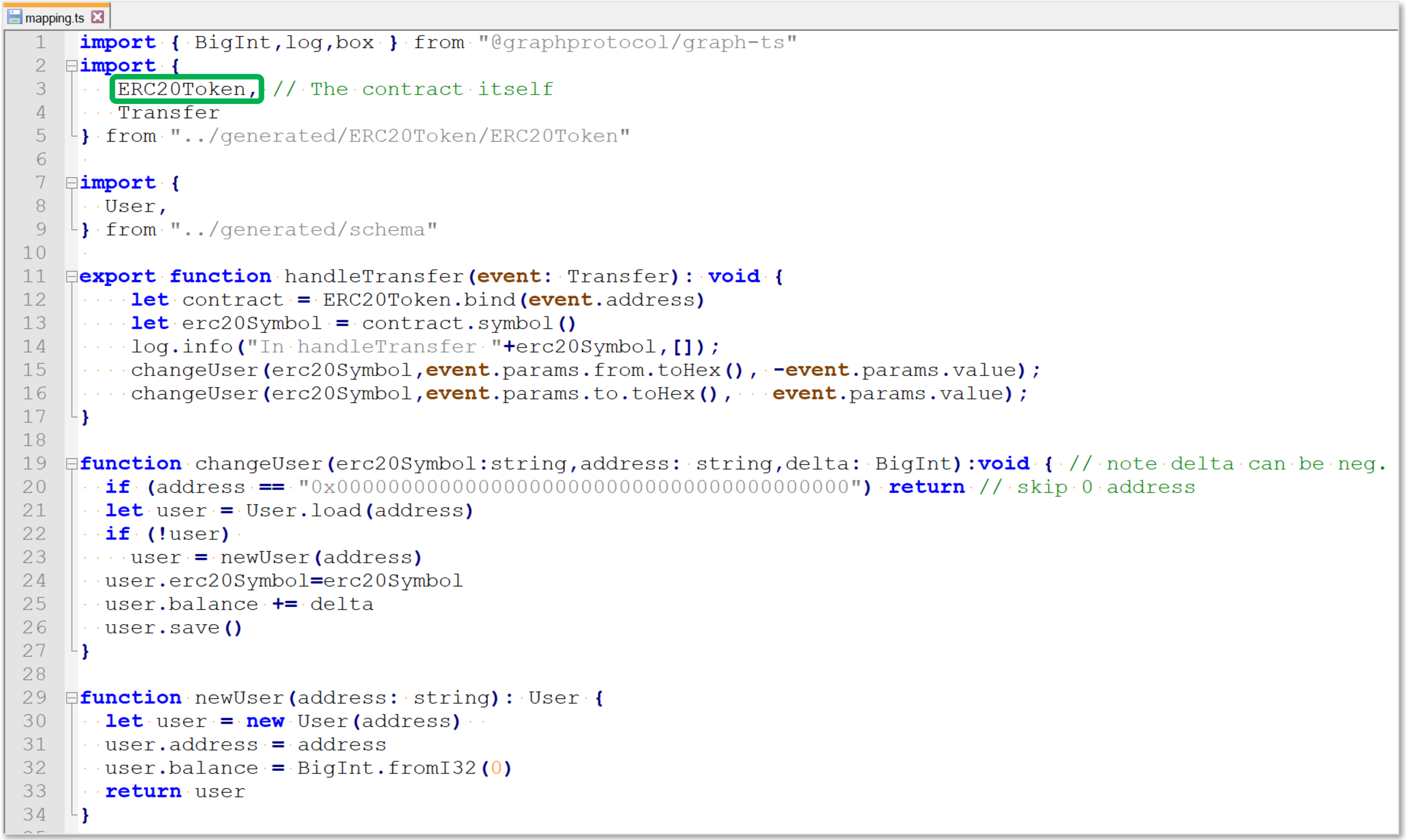


https://thegraph.com

https://thegraph.com/docs/define-a-subgraph

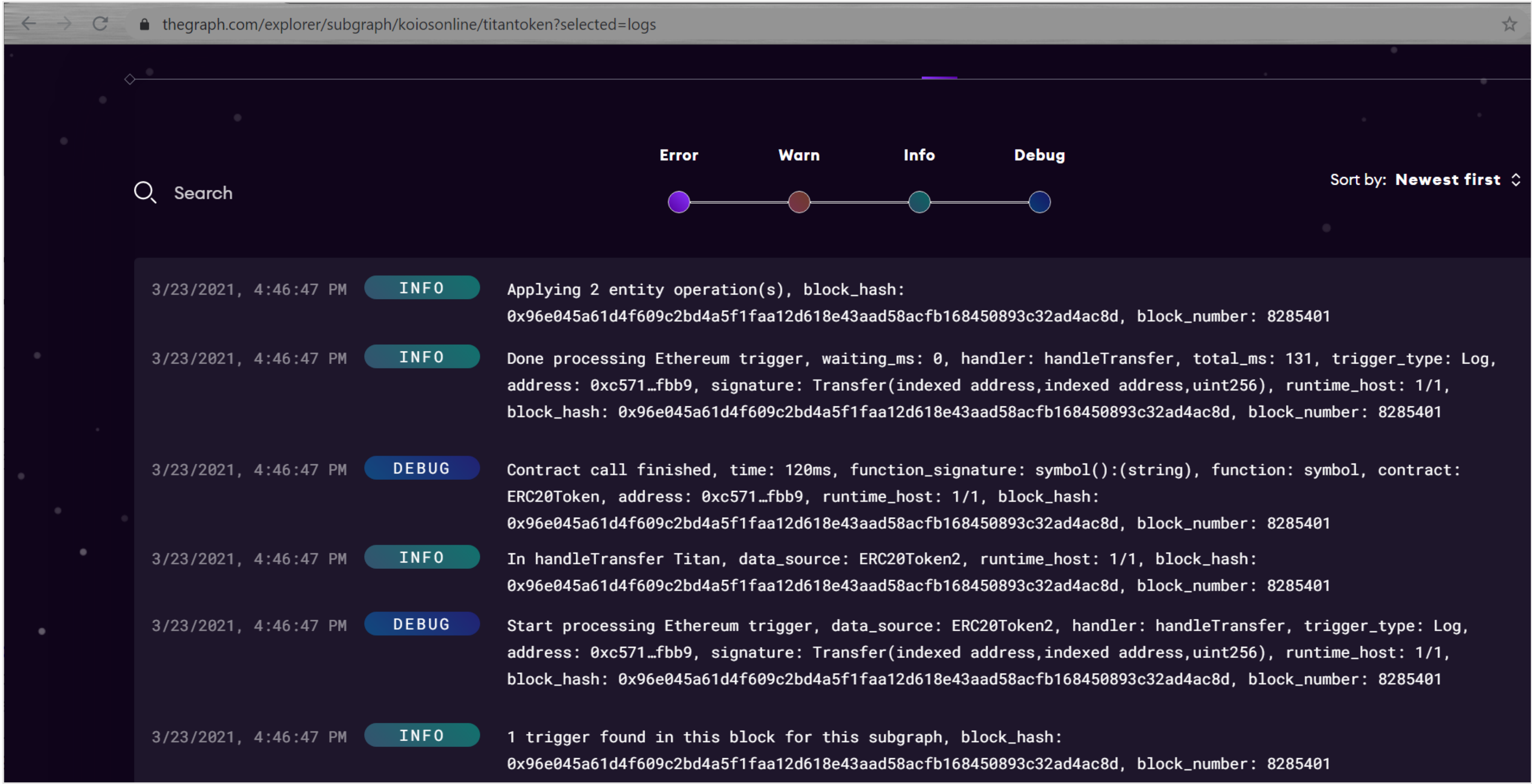
https://ethereumdev.io/how-to-access-indexed-ethereum-data-with-graph

Collect Graph data



```
import { BigInt,log,box } from "@graphprotocol/graph-ts"
import {
   ERC20Token, // The contract itself
   Transfer
} from "../generated/ERC20Token/ERC20Token"

import {
  User,
} from "../generated/schema"

export function handleTransfer(event: Transfer): void {
    let contract = ERC20Token.bind(event.address)
    let erc20Symbol = contract.symbol()
    log.info("In handleTransfer "+erc20Symbol,[]);
    changeUser(erc20Symbol,event.params.from.toHex(), -event.params.value);
    changeUser(erc20Symbol,event.params.to.toHex(),  event.params.value);
}

function changeUser(erc20Symbol:string,address: string,delta: BigInt):void { // note delta can be neg.
  if (address == "0x0000000000000000000000000000000000000000") return // skip 0 address
  let user = User.load(address)
  if (!user)
    user = newUser(address)
  user.erc20Symbol=erc20Symbol
  user.balance += delta
  user.save()
}

function newUser(address: string): User {
  let user = new User(address)
  user.address = address
  user.balance = BigInt.fromI32(0)
  return user
}
```

Processing by Indexer

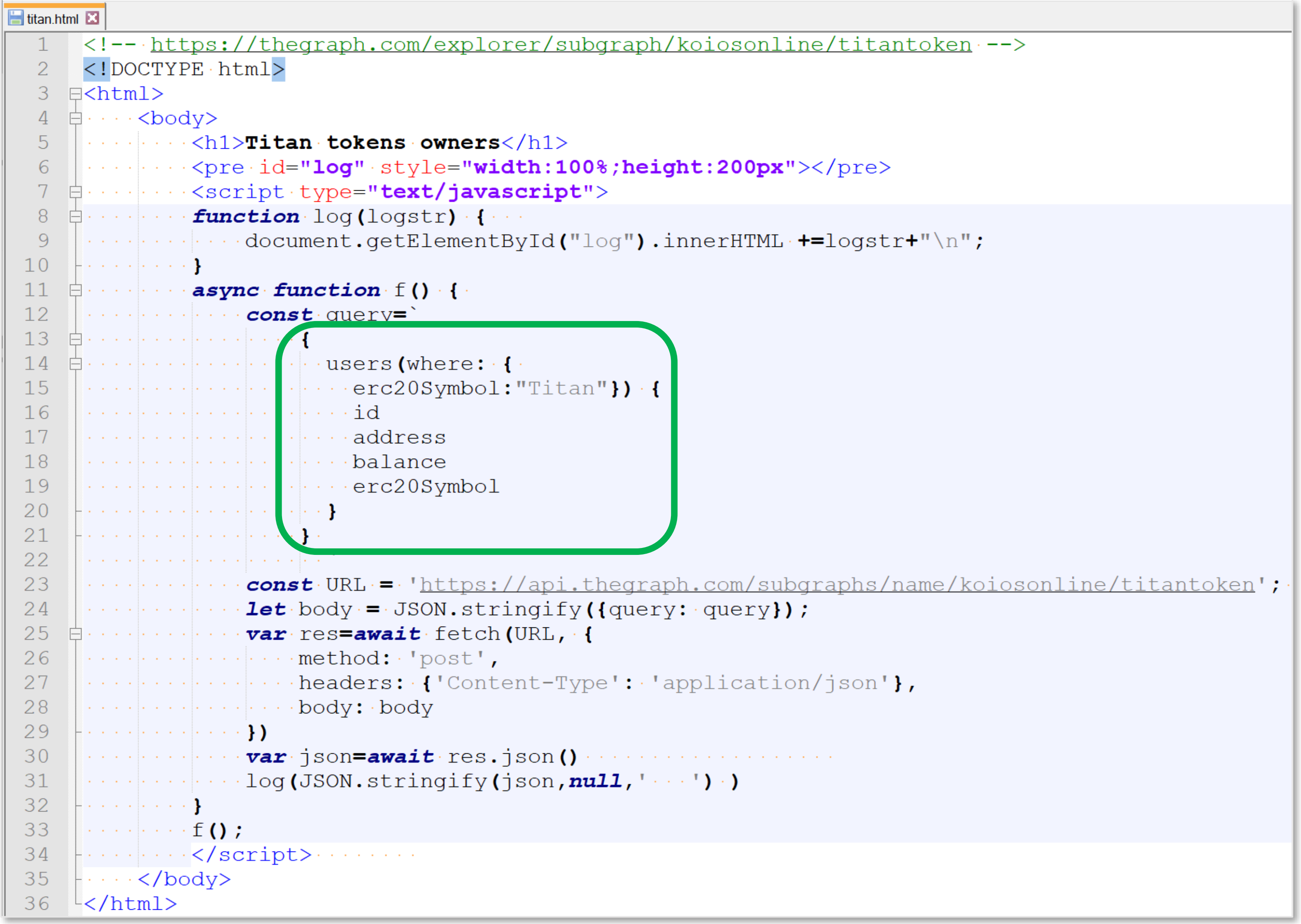


thegraph.com/explorer/subgraph/koiosonline/titantoken?selected=logs
Search
Error
Warn
Info
Debug
Sort by: Newest first

```
3/23/2021, 4:46:47 PM  INFO   Applying 2 entity operation(s), block_hash:
                              0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401

3/23/2021, 4:46:47 PM  INFO   Done processing Ethereum trigger, waiting_ms: 0, handler: handleTransfer, total_ms: 131, trigger_type: Log,
                              address: 0xc571…fbb9, signature: Transfer(indexed address,indexed address,uint256), runtime_host: 1/1,
                              block_hash: 0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401

3/23/2021, 4:46:47 PM  DEBUG  Contract call finished, time: 120ms, function_signature: symbol():(string), function: symbol, contract:
                              ERC20Token, address: 0xc571…fbb9, runtime_host: 1/1, block_hash:
                              0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401

3/23/2021, 4:46:47 PM  INFO   In handleTransfer Titan, data_source: ERC20Token2, runtime_host: 1/1, block_hash:
                              0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401

3/23/2021, 4:46:47 PM  DEBUG  Start processing Ethereum trigger, data_source: ERC20Token2, handler: handleTransfer, trigger_type: Log,
                              address: 0xc571…fbb9, signature: Transfer(indexed address,indexed address,uint256), runtime_host: 1/1,
                              block_hash: 0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401

3/23/2021, 4:46:47 PM  INFO   1 trigger found in this block for this subgraph, block_hash:
                              0x96e045a61d4f609c2bd4a5f1faa12d618e43aad58acfb168450893c32ad4ac8d, block_number: 8285401
```

https://thegraph.com/explorer/subgraph/koiosonline/titantoken?selected=logs

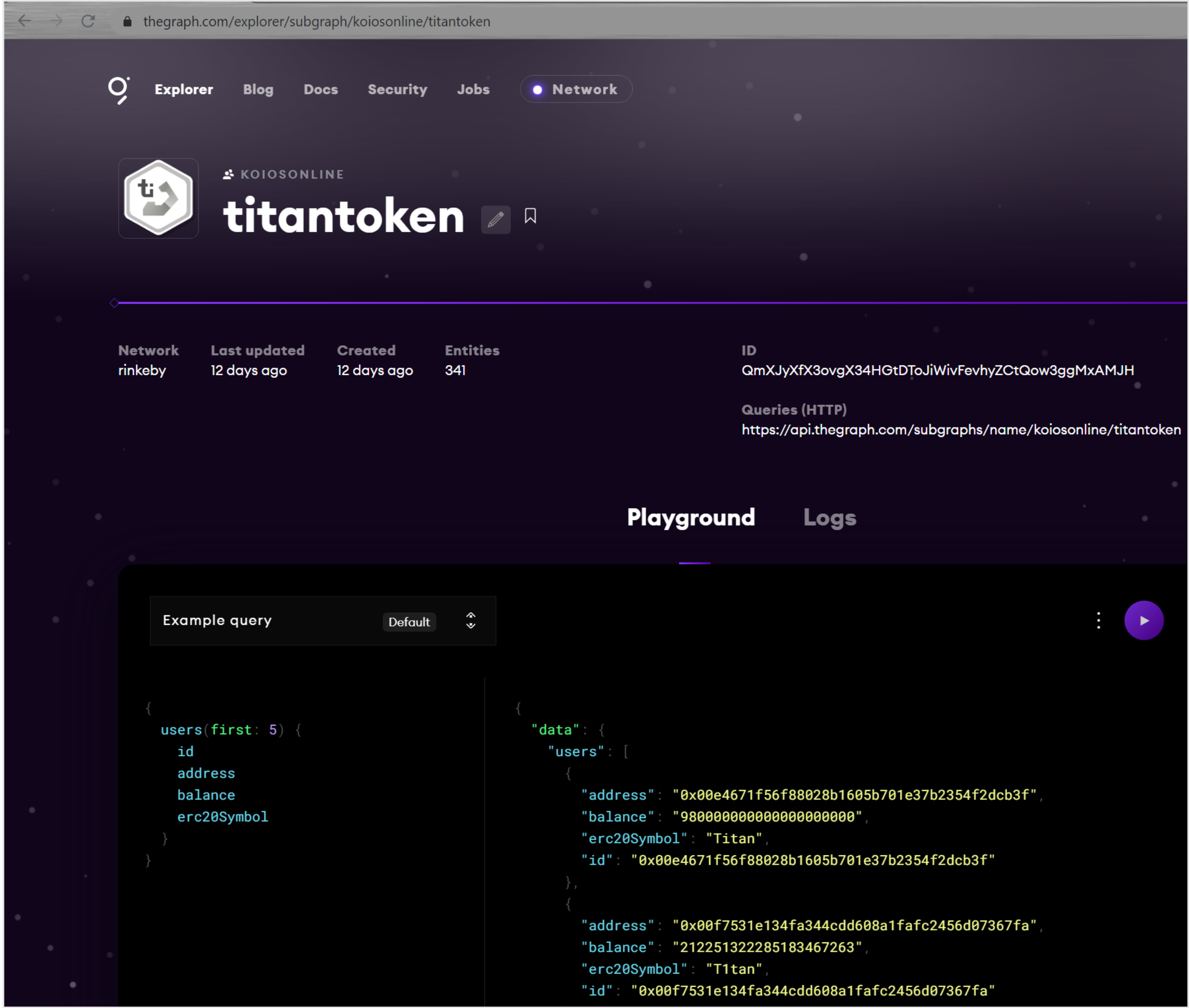
Retrieve Graph data



```
<!-- https://thegraph.com/explorer/subgraph/koiosonline/titantoken -->
<!DOCTYPE html>
<html>
    <body>
        <h1>Titan tokens owners</h1>
        <pre id="log" style="width:100%;height:200px"></pre>
        <script type="text/javascript">
        function log(logstr) {
            document.getElementById("log").innerHTML +=logstr+"\n";
        }
        async function f() {
            const query=`
                {
                  users(where: {
                    erc20Symbol:"Titan"}) {
                    id
                    address
                    balance
                    erc20Symbol
                  }
                }

            const URL = 'https://api.thegraph.com/subgraphs/name/koiosonline/titantoken';
            let body = JSON.stringify({query: query});
            var res=await fetch(URL, {
                method: 'post',
                headers: {'Content-Type': 'application/json'},
                body: body
            })
            var json=await res.json()
            log(JSON.stringify(json,null,'   ') )
        }
        f();
        </script>
    </body>
</html>
```

https://thegraph.com/explorer/subgraph/koiosonline/titantoken

Test query



titantoken

Network	Last updated	Created	Entities
rinkeby	12 days ago	12 days ago	341

ID
QmXJyXfX3ovgX34HGtDToJiWivFevhyZCtQow3ggMxAMJH

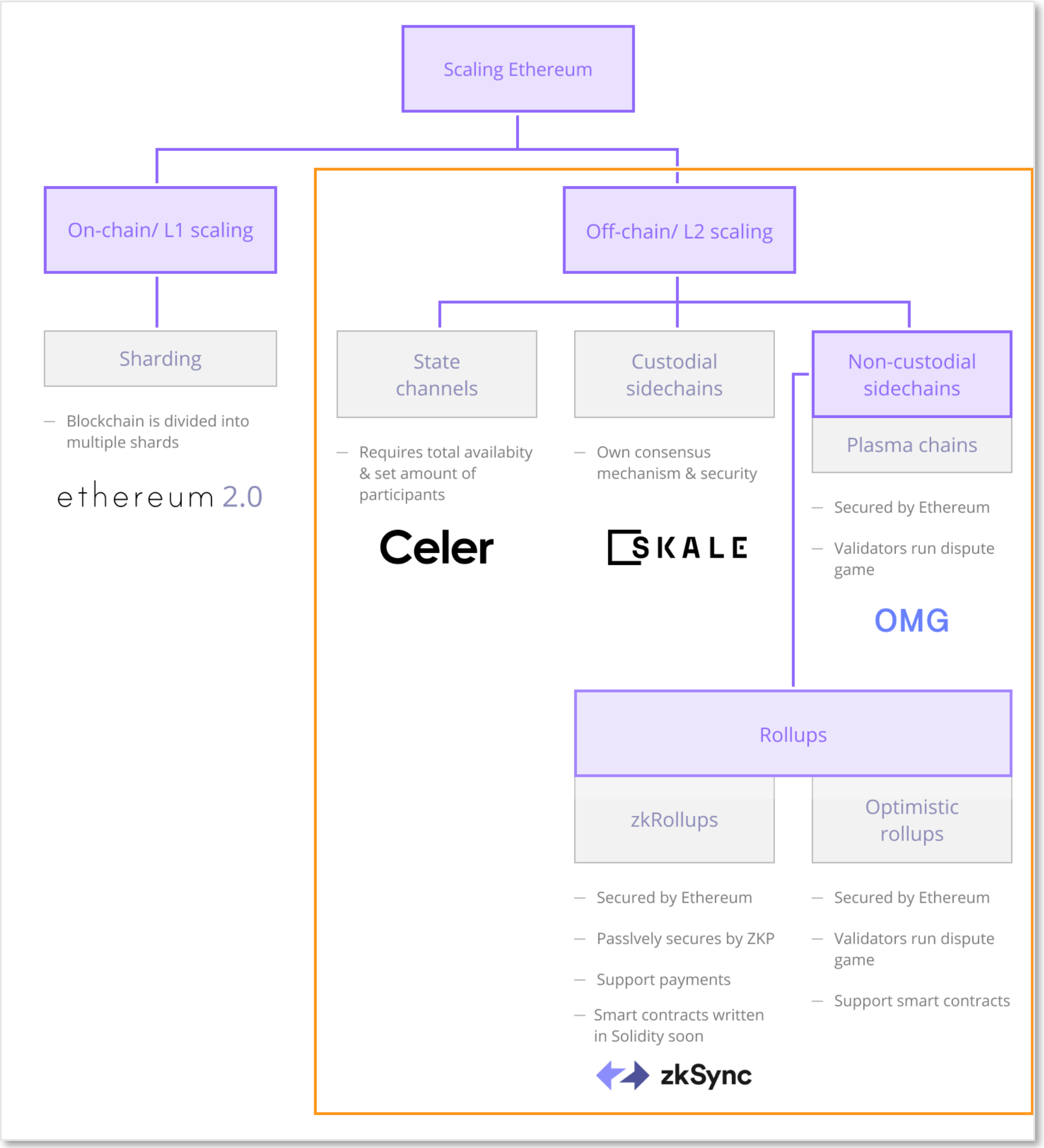
Queries (HTTP)
https://api.thegraph.com/subgraphs/name/koiosonline/titantoken

```
{
  users(first: 5) {
    id
    address
    balance
    erc20Symbol
  }
}
```

```
{
  "data": {
    "users": [
      {
        "address": "0x00e4671f56f88028b1605b701e37b2354f2dcb3f",
        "balance": "980000000000000000000",
        "erc20Symbol": "Titan",
        "id": "0x00e4671f56f88028b1605b701e37b2354f2dcb3f"
      },
      {
        "address": "0x00f7531e134fa344cdd608a1fafc2456d07367fa",
        "balance": "212251322285183467263",
        "erc20Symbol": "T1tan",
        "id": "0x00f7531e134fa344cdd608a1fafc2456d07367fa"
```

https://thegraph.com/explorer/subgraph/koiosonline/titantoken

Layer 2 chains



Scaling Ethereum

On-chain/ L1 scaling

Sharding

- Blockchain is divided into multiple shards

ethereum 2.0

Off-chain/ L2 scaling

State channels

- Requires total availabity & set amount of participants

Celer

Custodial sidechains

- Own consensus mechanism & security

SKALE

Non-custodial sidechains

Plasma chains

- Secured by Ethereum
- Validators run dispute game

OMG

Rollups

zkRollups

- Secured by Ethereum
- Passlvely secures by ZKP
- Support payments
- Smart contracts written in Solidity soon

zkSync

Optimistic rollups

- Secured by Ethereum
- Validators run dispute game
- Support smart contracts

https://defiprime.com/ethereum-l2

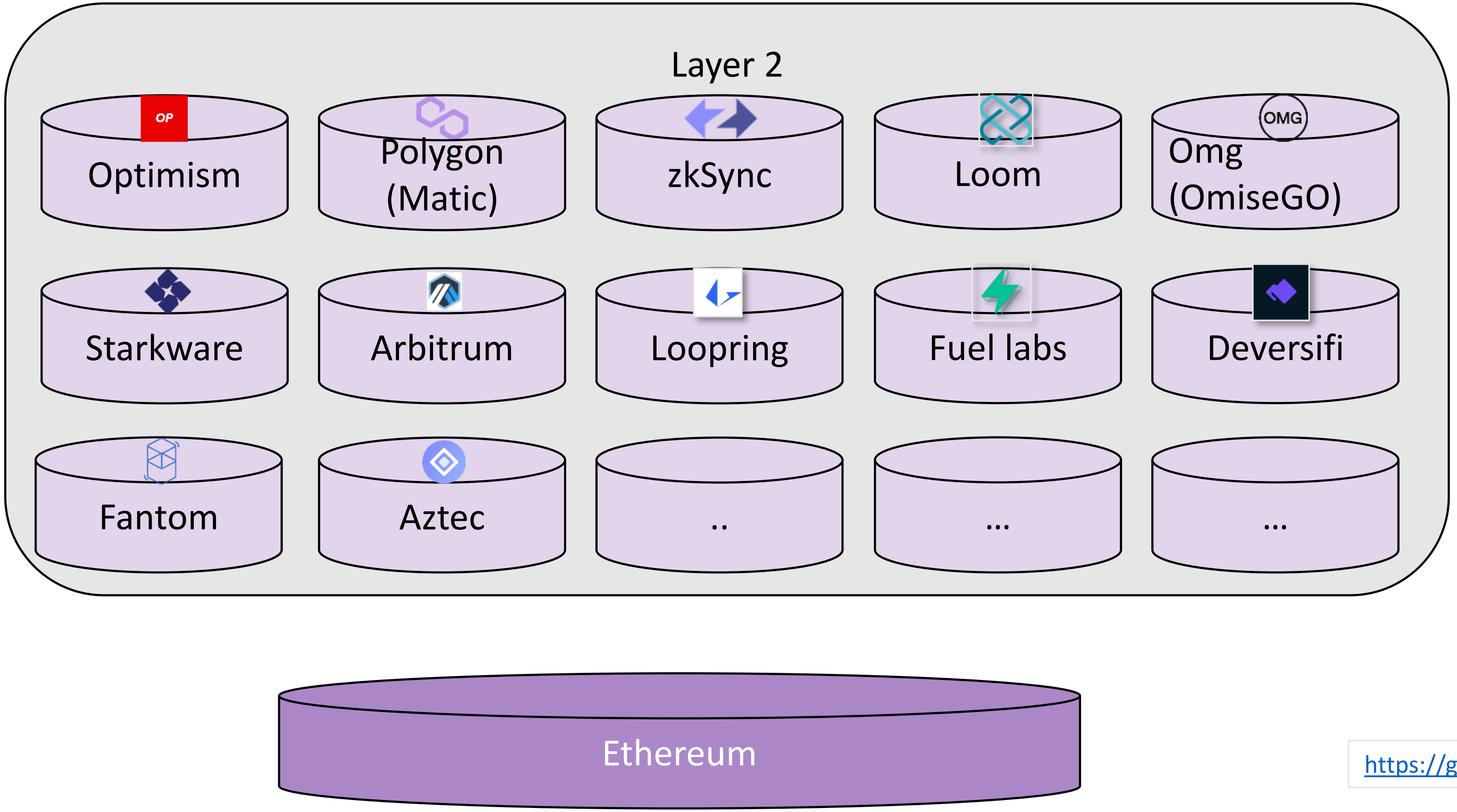
https://ethereum.org/en/developers/docs/layer-2-scaling

https://medium.com/matter-labs/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955

Layer 2

https://github.com/starkware-libs/

https://github.com/AztecProtocol



https://github.com/Fantom-Foundation

https://github.com/fuellabs

https://github.com/maticnetwork

https://github.com/loomnetwork

https://github.com/omgnetwork

https://github.com/matter-labs/zksync

https://github.com/ethereum-optimism/optimism-monorepo

https://github.com/OffchainLabs/arbitrum

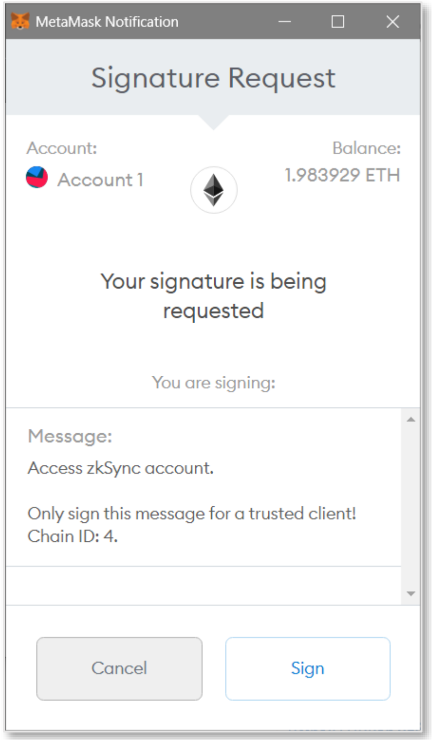
https://github.com/Loopring

https://github.com/deversifi

Zero Knowledge terms

Abbreviations	Meaning
ZK	Zero-Knowledge
Succinct	Short and to the point / verifiable in short time (requires trusted setup)
Non-interactive	One message (so no need for multiple rounds)
SNARK	Succinct Non-interactive adaptive ARgument of Knowledge
Argument	Proof
Transparent	No trusted setup
STARK	Scalable Transparent ARguments of Knowledge (quantum-resistant)
Bulletproef	Short non-interactive zero-knowledge proofs that require no trusted setup (range proofs) (not quantum-resistant)
R1CS	Rank-1 Constraint System

ZKSync Bridge



MetaMask Notification

Signature Request

Account: Account 1

Balance: 1.983929 ETH

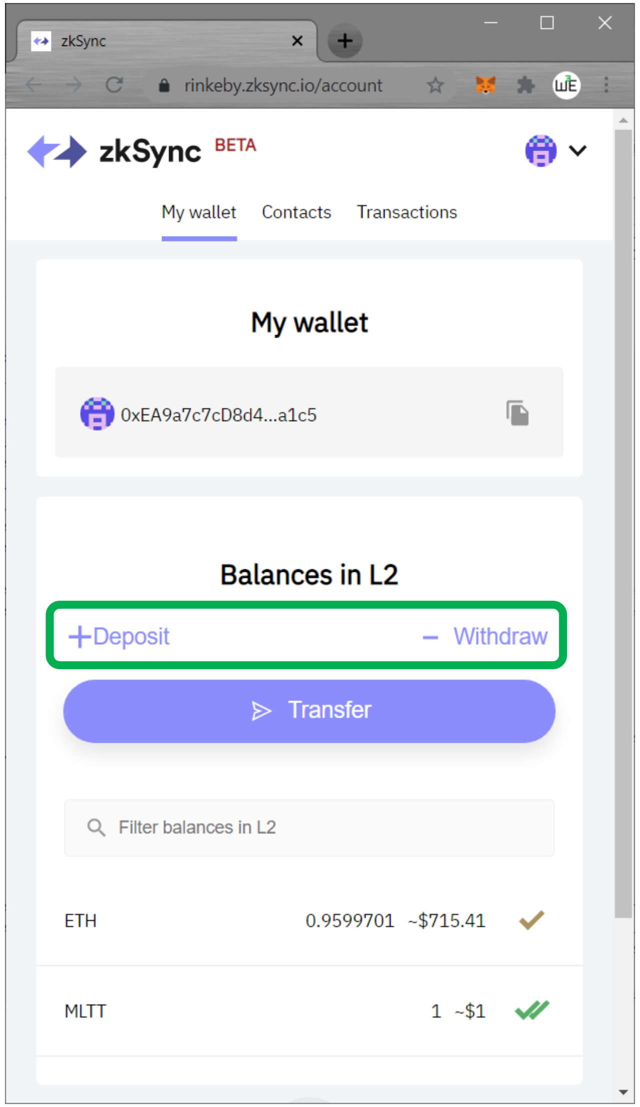
Your signature is being requested

You are signing:

Message:

Access zkSync account.

Only sign this message for a trusted client!
Chain ID: 4.



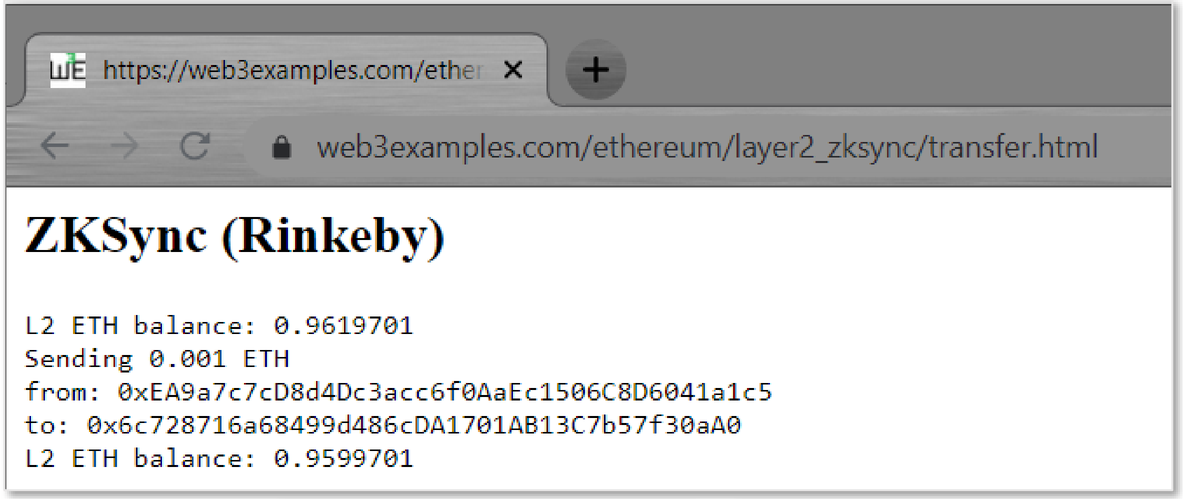
My wallet

0xEA9a7c7cD8d4...a1c5

Balances in L2

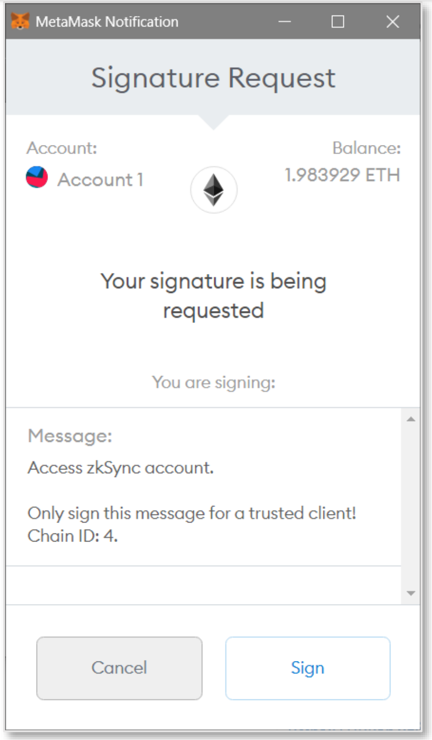
ETH	0.9599701 ~$715.41 ✓
MLTT	1 ~$1 ✓✓

ZKSync


https://web3examples.com/ether
web3examples.com/ethereum/layer2_zksync/transfer.html

ZKSync (Rinkeby)

```
L2 ETH balance: 0.9619701
Sending 0.001 ETH
from: 0xEA9a7c7cD8d4Dc3acc6f0AaEc1506C8D6041a1c5
to: 0x6c728716a68499d486cDA1701AB13C7b57f30aA0
L2 ETH balance: 0.9599701
```

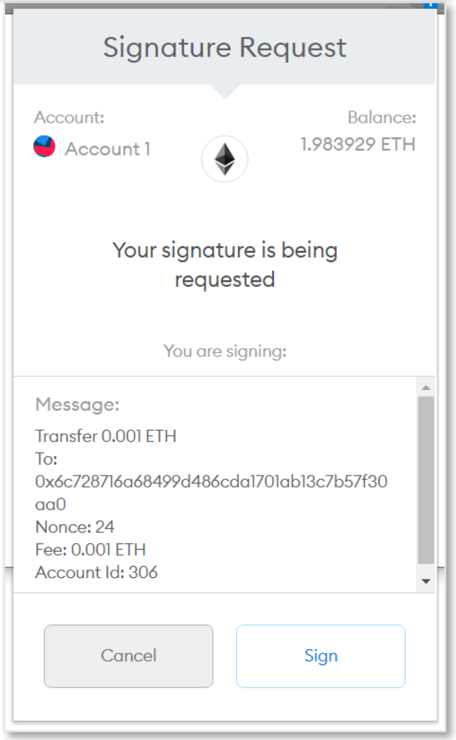


Your signature is being requested

You are signing:

Message:
Access zkSync account.

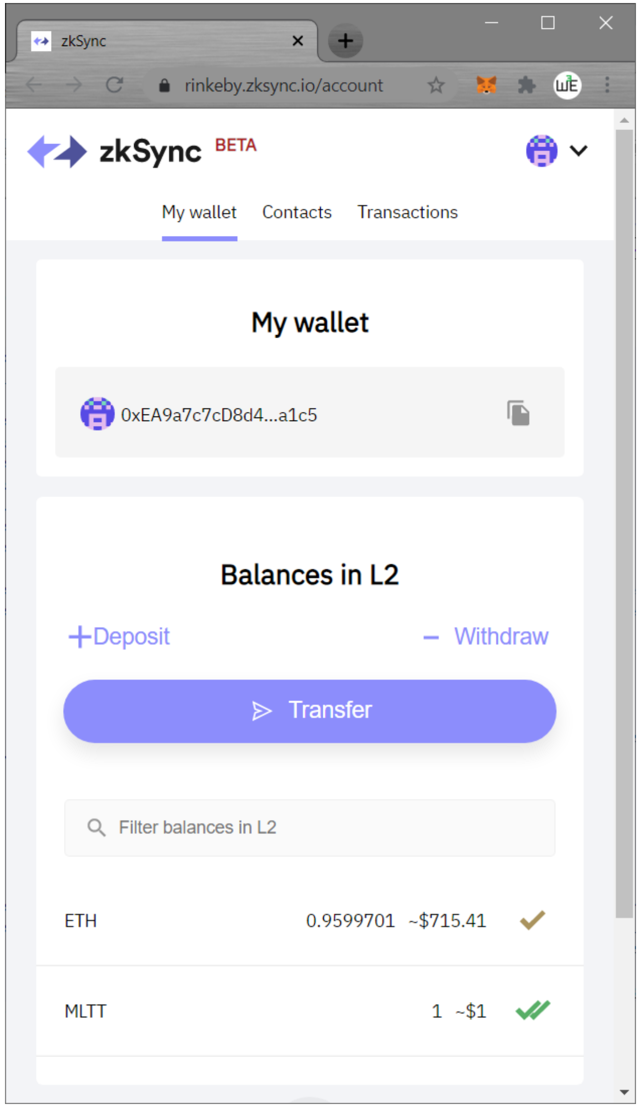
Only sign this message for a trusted client!
Chain ID: 4.



Your signature is being requested

You are signing:

Message:
Transfer 0.001 ETH
To:
0x6c728716a68499d486cda1701ab13c7b57f30aa0
Nonce: 24
Fee: 0.001 ETH
Account Id: 306

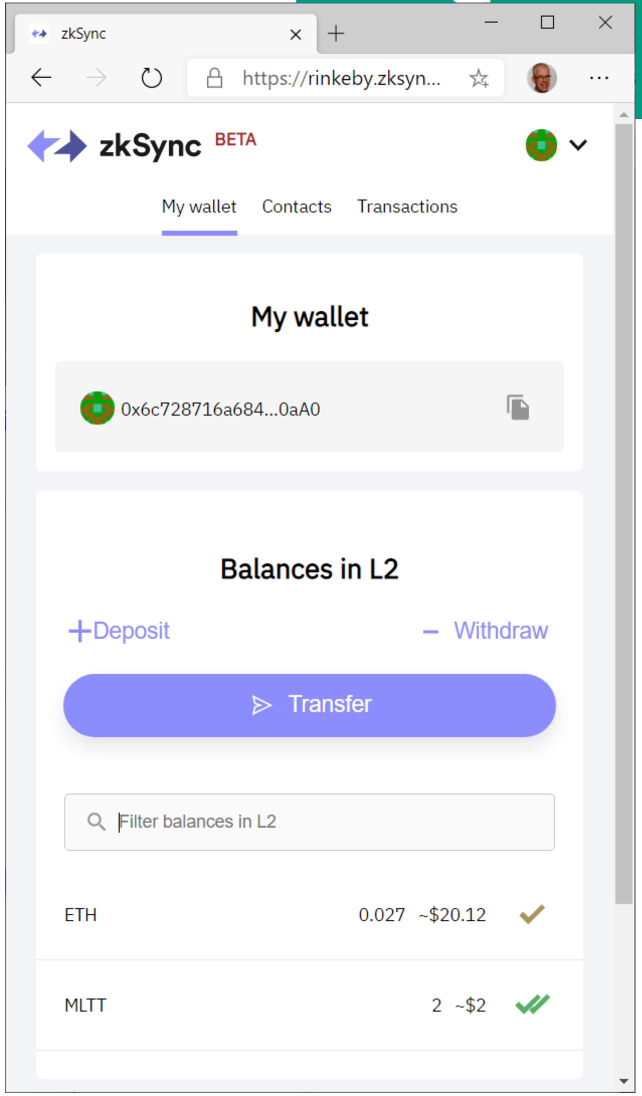


My wallet

0xEA9a7c7cD8d4...a1c5

Balances in L2

ETH	0.9599701 ~$715.41	✓
MLTT	1 ~$1	✓✓



My wallet

0x6c728716a684...0aA0

Balances in L2

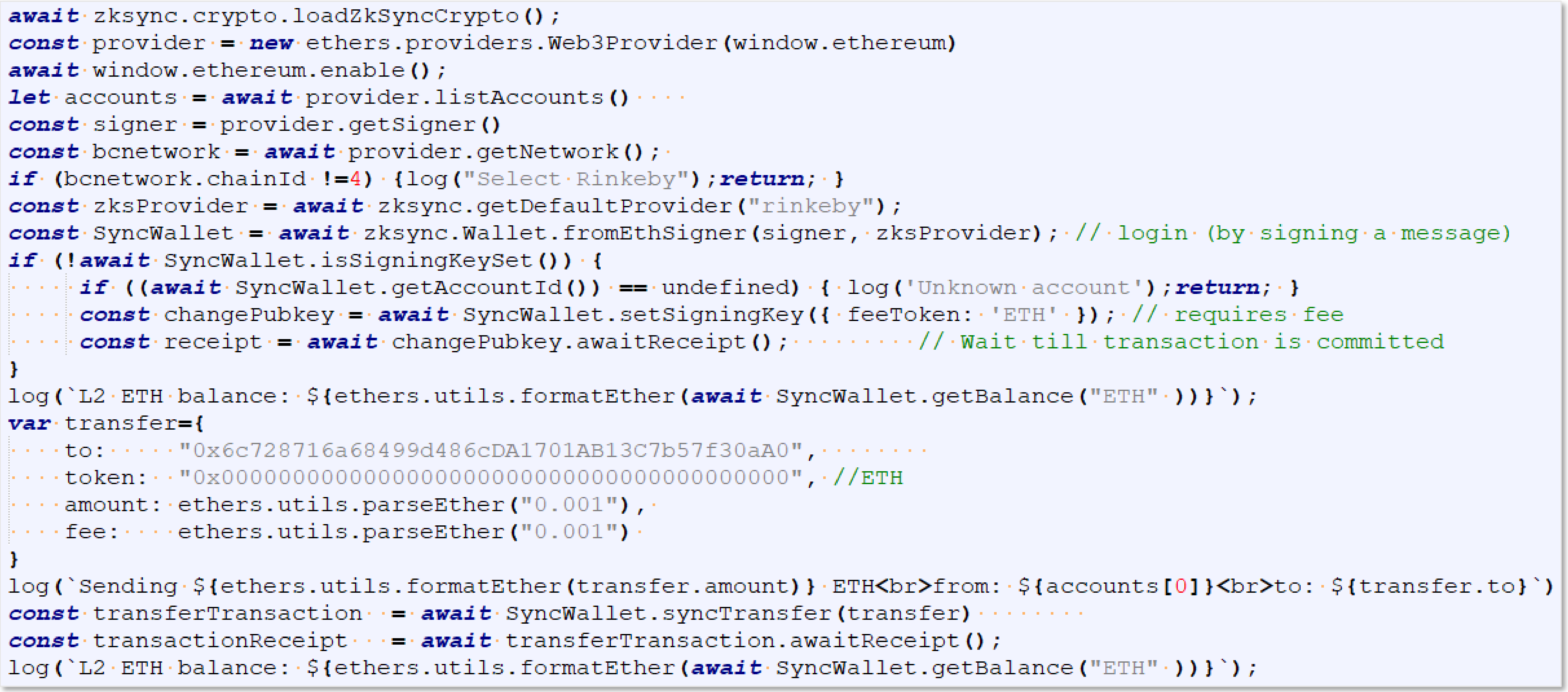
ETH	0.027 ~$20.12	✓
MLTT	2 ~$2	✓✓

https://rinkeby.zksync.io/account

https://rinkeby.zkscan.io

https://web3examples.com/ethereum/layer2_zksync/transfer.html

ZKSync

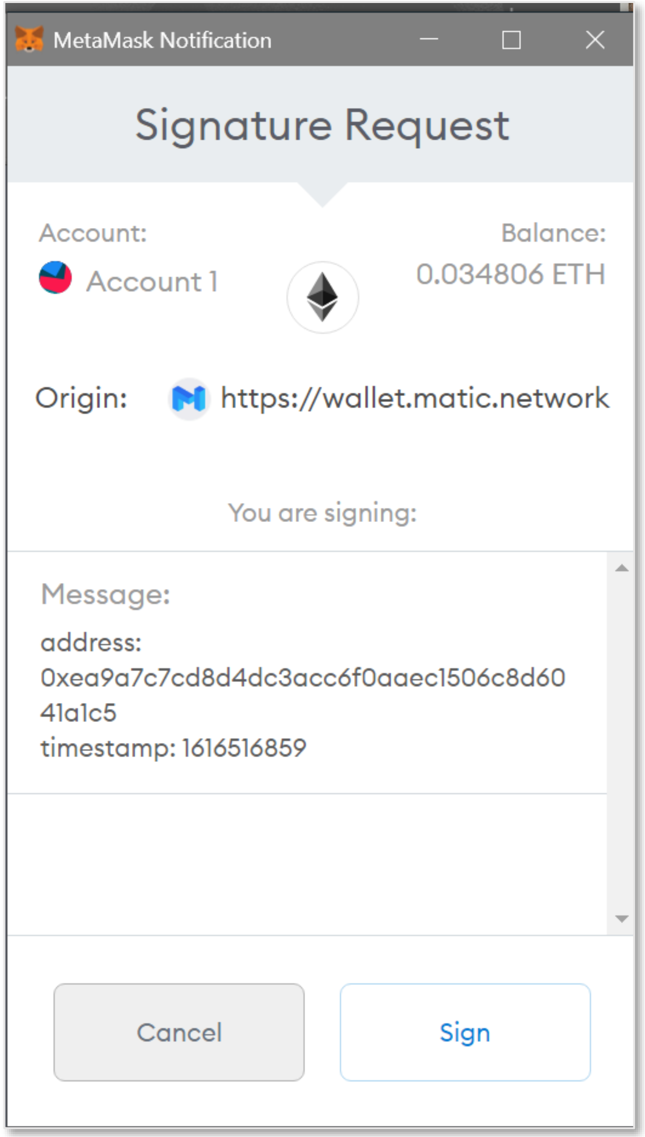


```
await zksync.crypto.loadZkSyncCrypto();
const provider = new ethers.providers.Web3Provider(window.ethereum)
await window.ethereum.enable();
let accounts = await provider.listAccounts()    
const signer = provider.getSigner()
const bcnetwork = await provider.getNetwork(); 
if (bcnetwork.chainId !=4) {log("Select Rinkeby");return; }
const zksProvider = await zksync.getDefaultProvider("rinkeby");
const SyncWallet = await zksync.Wallet.fromEthSigner(signer, zksProvider); // login (by signing a message)
if (!await SyncWallet.isSigningKeySet()) {
    if ((await SyncWallet.getAccountId()) == undefined) { log('Unknown account');return; }
    const changePubkey = await SyncWallet.setSigningKey({ feeToken: 'ETH' }); // requires fee
    const receipt = await changePubkey.awaitReceipt();         // Wait till transaction is committed
}
log(`L2 ETH balance: ${ethers.utils.formatEther(await SyncWallet.getBalance("ETH" ))}`);
var transfer={
    to:     "0x6c728716a68499d486cDA1701AB13C7b57f30aA0",        
    token:  "0x0000000000000000000000000000000000000000", //ETH
    amount: ethers.utils.parseEther("0.001"), 
    fee:    ethers.utils.parseEther("0.001") 
}
log(`Sending ${ethers.utils.formatEther(transfer.amount)} ETH<br>from: ${accounts[0]}<br>to: ${transfer.to}`)
const transferTransaction  = await SyncWallet.syncTransfer(transfer)       
const transactionReceipt   = await transferTransaction.awaitReceipt();
log(`L2 ETH balance: ${ethers.utils.formatEther(await SyncWallet.getBalance("ETH" ))}`);
```

https://web3examples.com/ethereum/layer2_zksync/transfer.html

https://github.com/web3examples/ethereum/blob/master/layer2_zksync/transfer.html

Polygon (Matic) Bridge



Signature Request

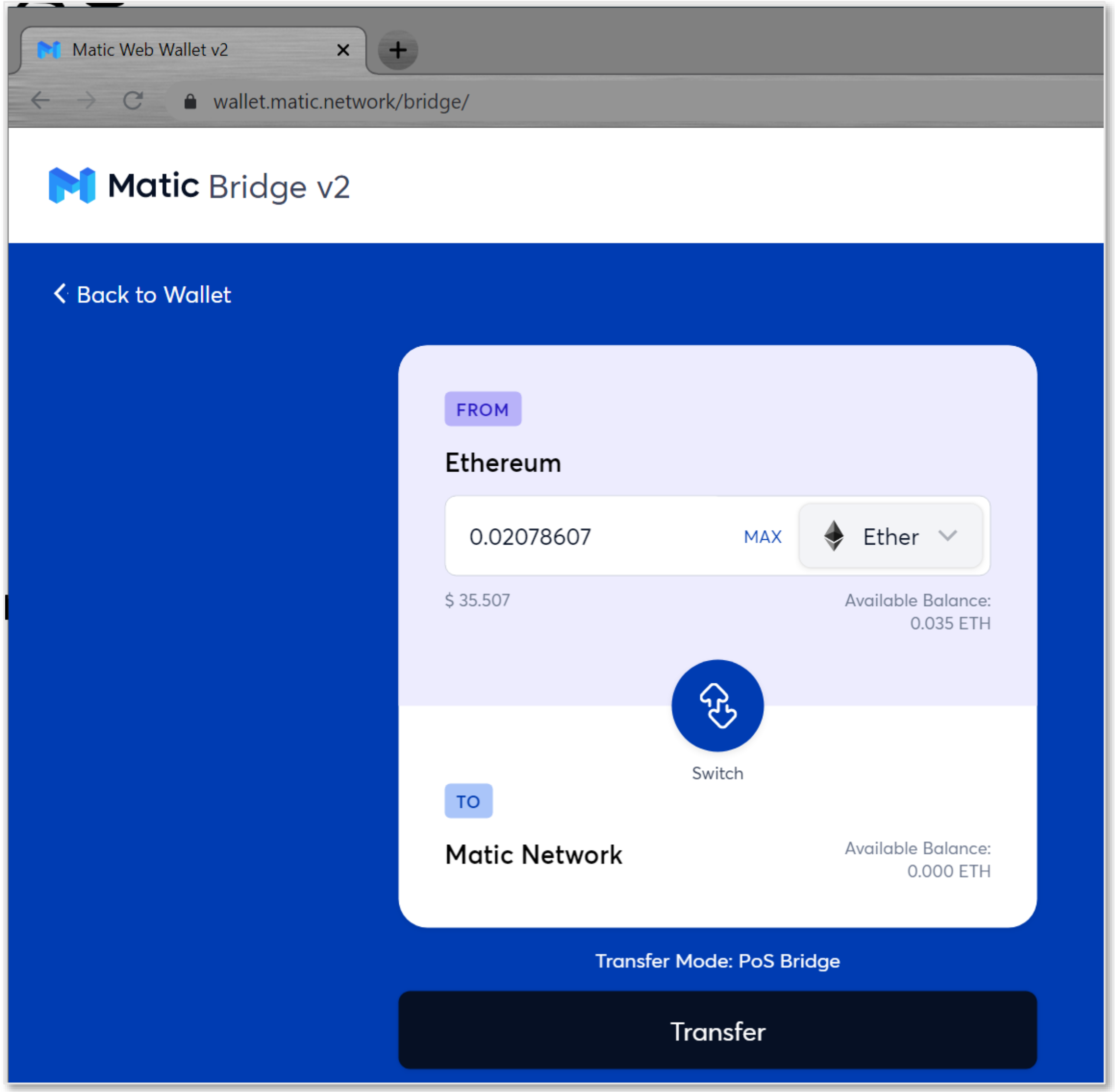
Account: Account 1

Balance: 0.034806 ETH

Origin: https://wallet.matic.network

You are signing:

Message:
address:
0xea9a7c7cd8d4dc3acc6f0aaec1506c8d60
41a1c5
timestamp: 1616516859



FROM
Ethereum

0.02078607 MAX Ether

$ 35.507

Available Balance:
0.035 ETH

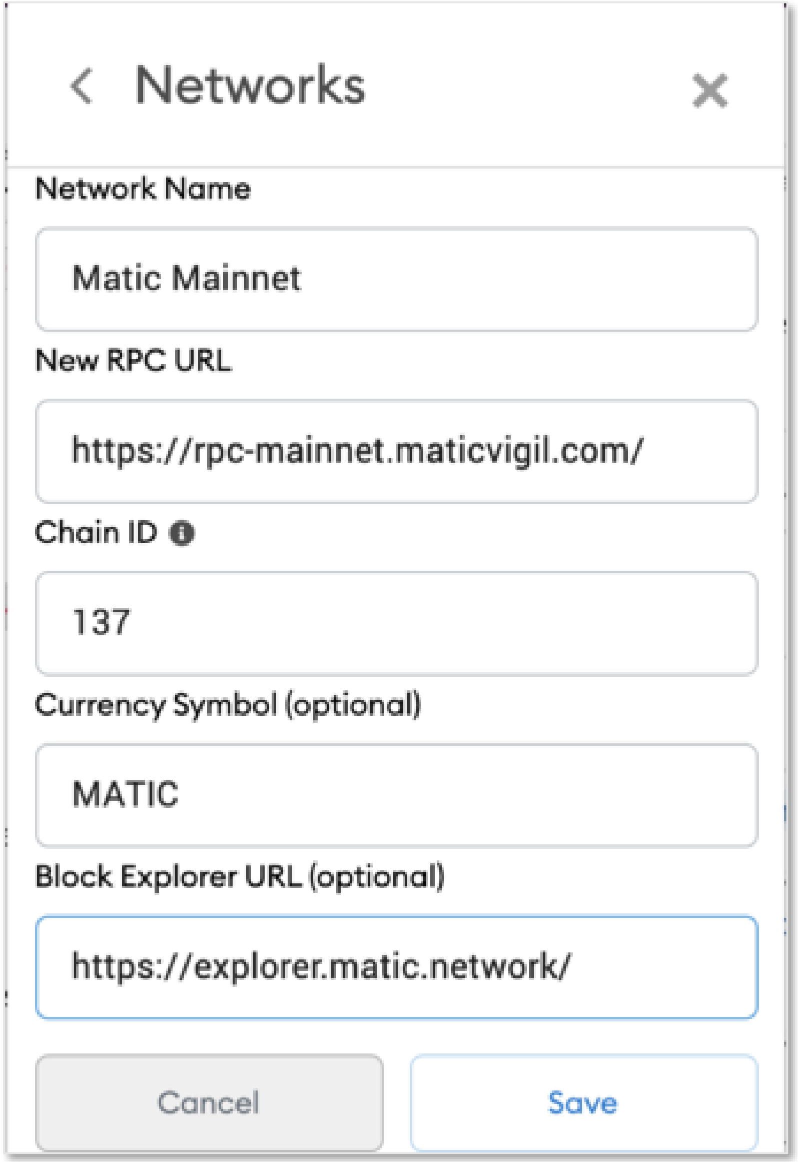
TO
Matic Network

Available Balance:
0.000 ETH

Transfer Mode: PoS Bridge

https://wallet.matic.network/bridge

Configure Metamask



Network Name

Matic Mainnet

New RPC URL

https://rpc-mainnet.maticvigil.com/

Chain ID

137

Currency Symbol (optional)

MATIC

Block Explorer URL (optional)

https://explorer.matic.network/

https://docs.matic.network/docs/develop/metamask/config-matic

Assignment

* provide your github account (create one if you don't have it) and i'll create a github repo to store and run the code.

Create a Covid application in solidity that does the following: (using https://remix.ethereum.org)
- register as a person (only with your ethereum address to keep the GDPR impact minimal)
- register when a person is vaccinated (this is done by the vaccination organisation, so using a different ethereum account)
- register when a person is tested   (this is done by the test organisation, so using a different ethereum account)
- register the test result of a person   (this is done by the test organisation, so using a different ethereum account)
- register the temperature of the person (this is done by the person himself)

- have a function that shows if you are allowed to go to a festival:

yes if: { you are vaccinated twice or you have a negative test (of max 1 day old) } and your temperature is below 38 degrees celsius

Note: this is not GDPR compliant because everything on the blockchain is visible!

Make a website of this,
Via: https://oneclickdapp.com
or use javascript (see https://web3examples.com/ethereum/web3js_browser)