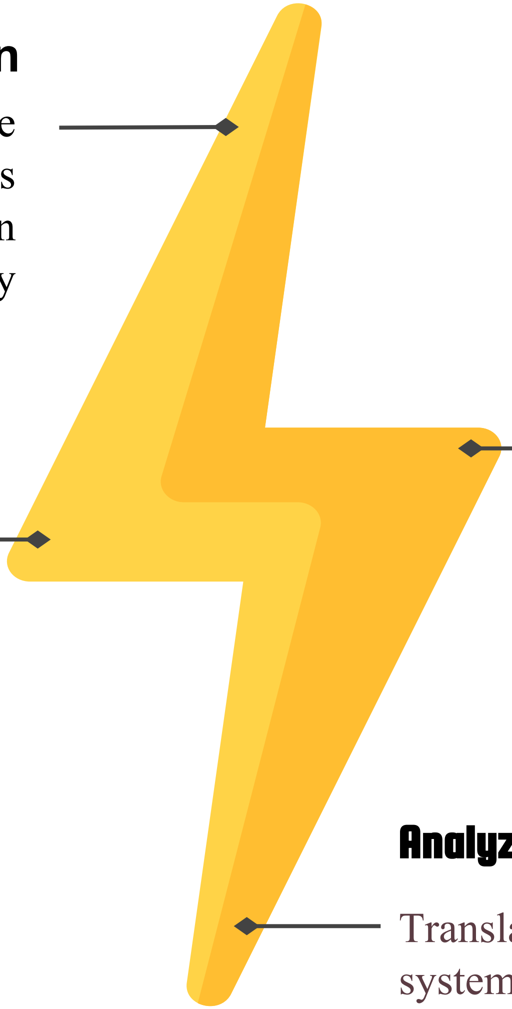
Smart Contract: a case study

Samia Guesmi
ISIMS
University of Udine

PRIN 2020 NiRvAna
Riunione fine primo anno, Venezia 5-7 giugno, 2023

Our Objectives



Blockchain

Advancing Expertise in Smart Contracts and Blockchain Technology

Building Hands-On Proficiency

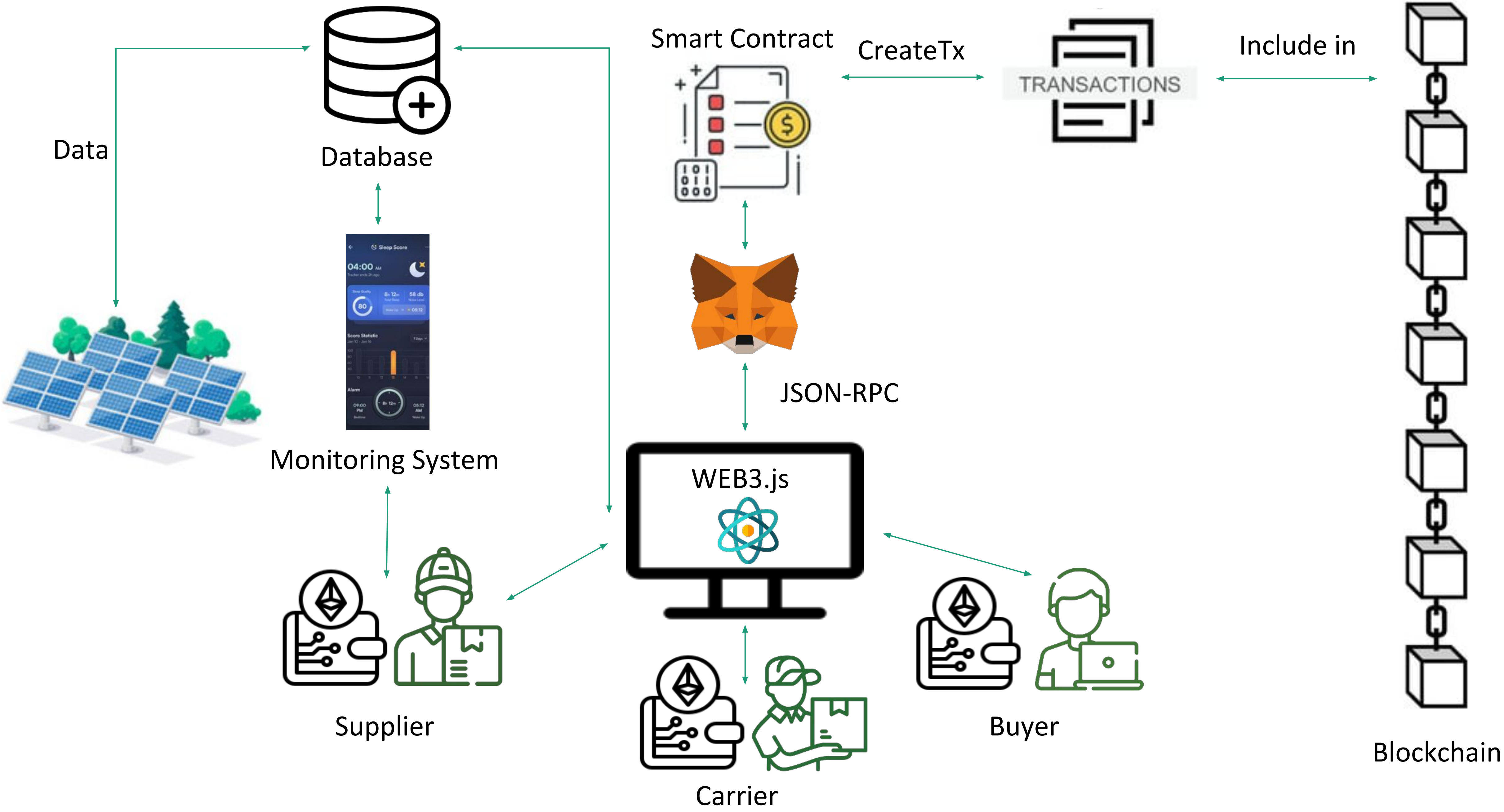
Creating a Customized System for Comprehensive Analysis and Experimentation

Enabling Integration

Incorporating both Centralized and Decentralized storage of Elements into our System

Analyzing Security

Translating parts of the system Components into Process Algebras for formal verification


Database
Data
Monitoring System
Smart Contract
CreateTx
TRANSACTIONS
Include in
JSON-RPC
WEB3.js
Supplier
Carrier
Buyer
Blockchain

Plan

01 **Project Approach**

Diagram and Process

02 **Decentralized Storage**

Blockchain Technology

03 **Smart Contract**

Technical Aspects
and Implementation

04 **Centralized Data Management**

Integrating SQL Database

05 **Information Flow**

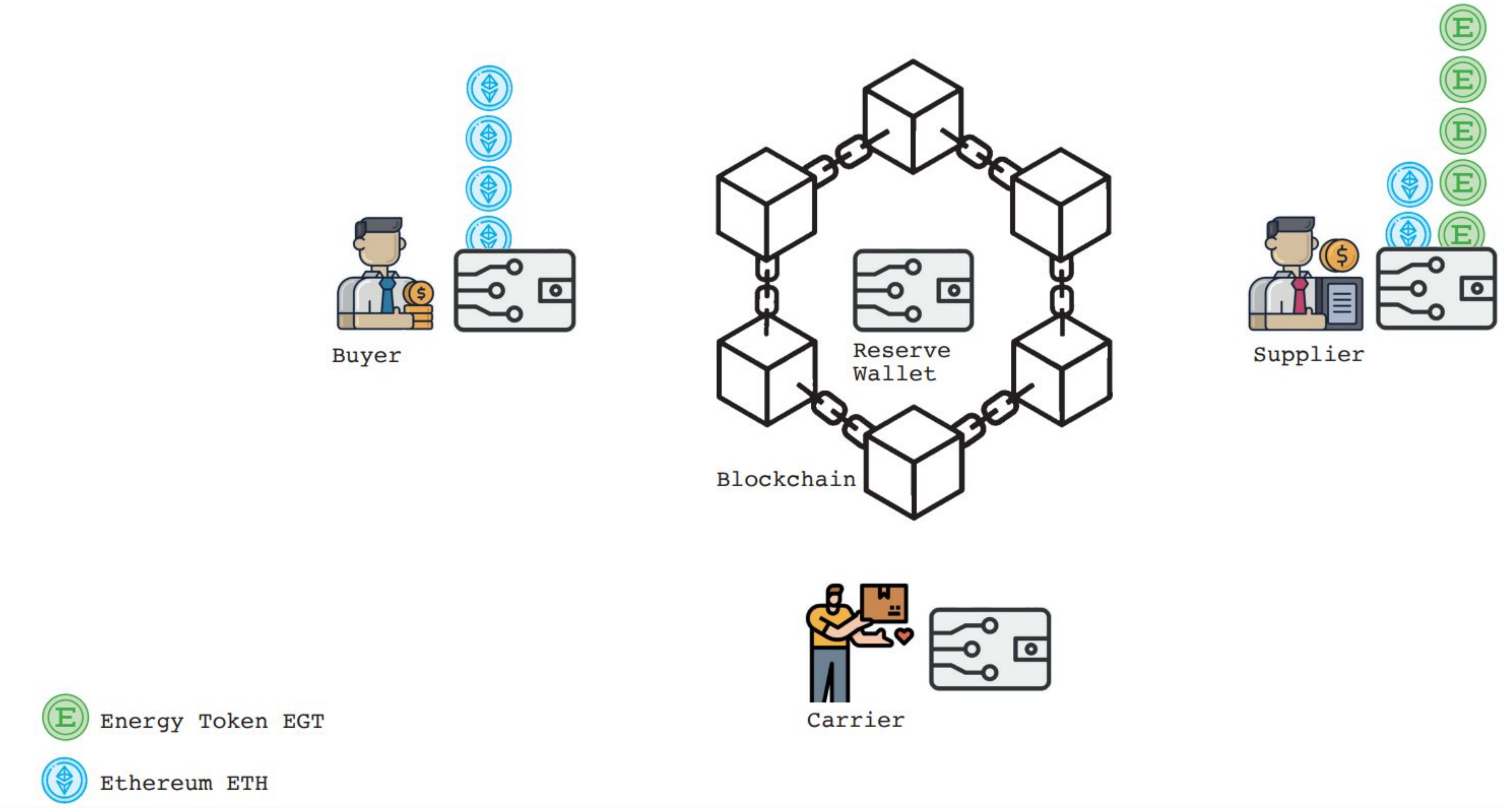
Specific Use Case

06 **Implementation**

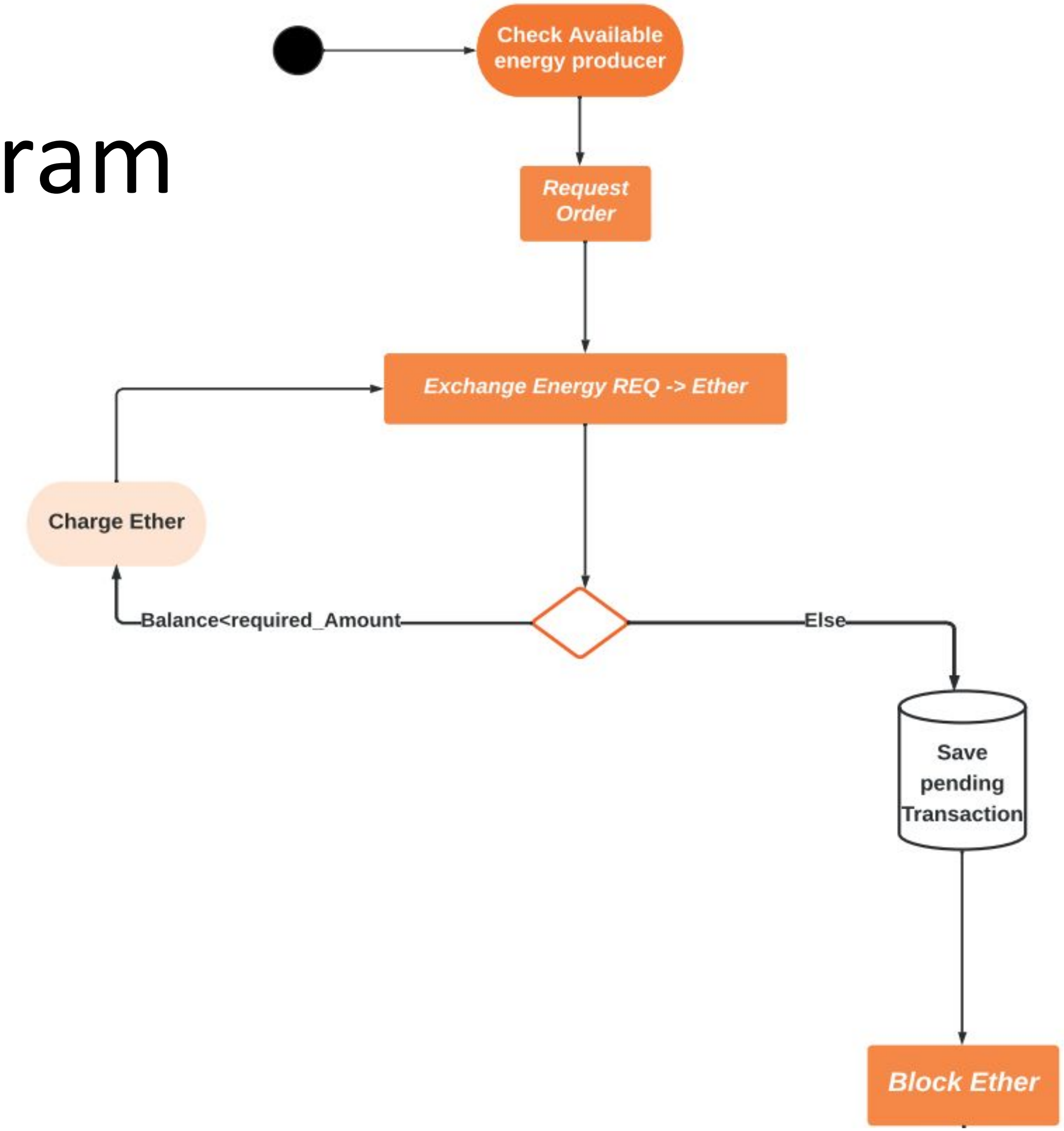
Technology Stack

Demonstration of   the solution

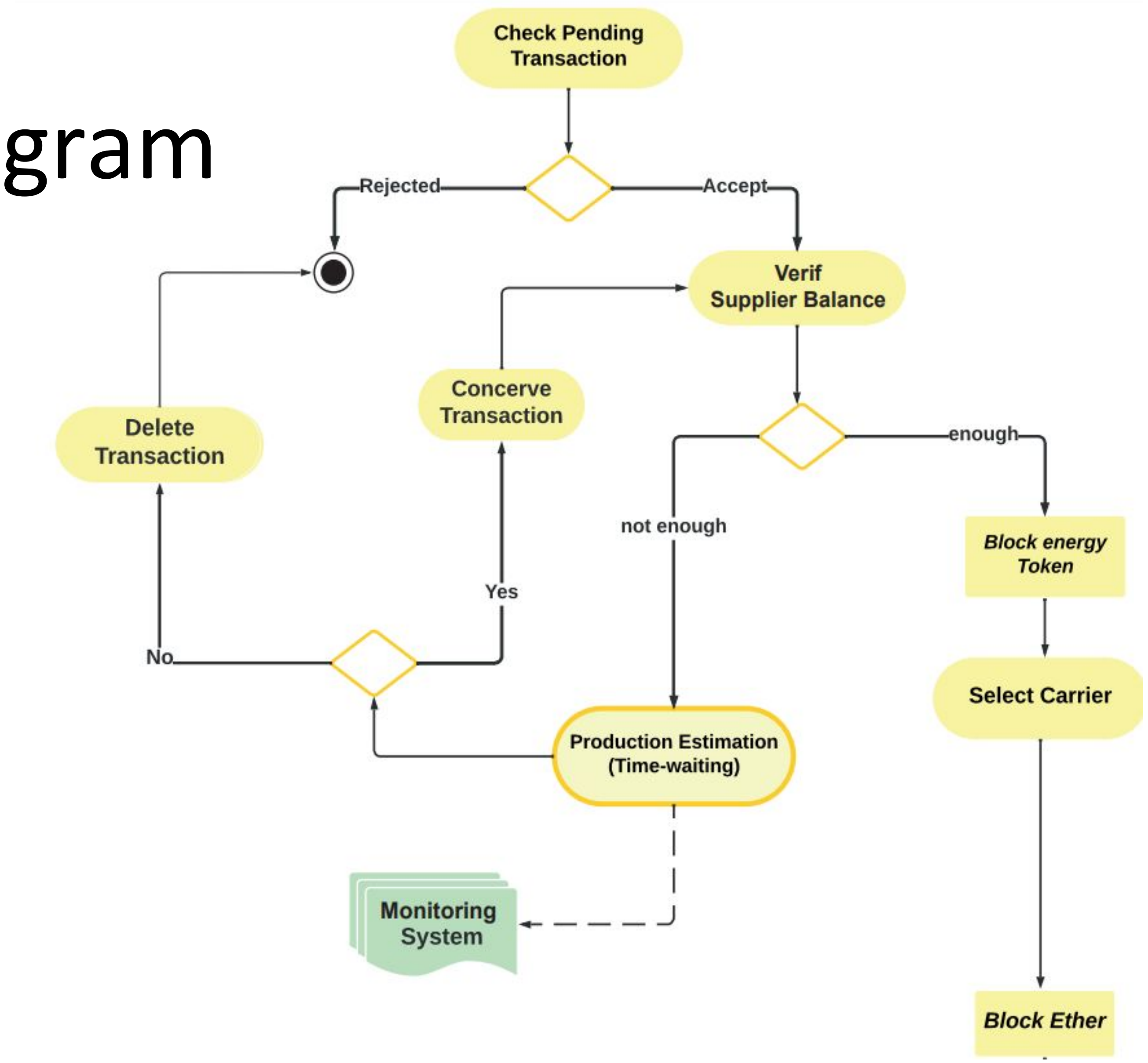
Project Approach : Actors



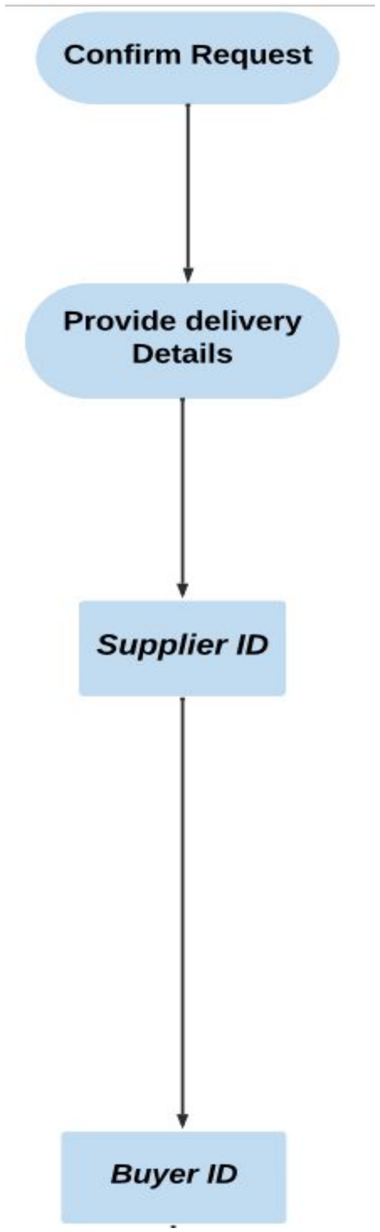
Project Approach: Buyer Activity Diagram



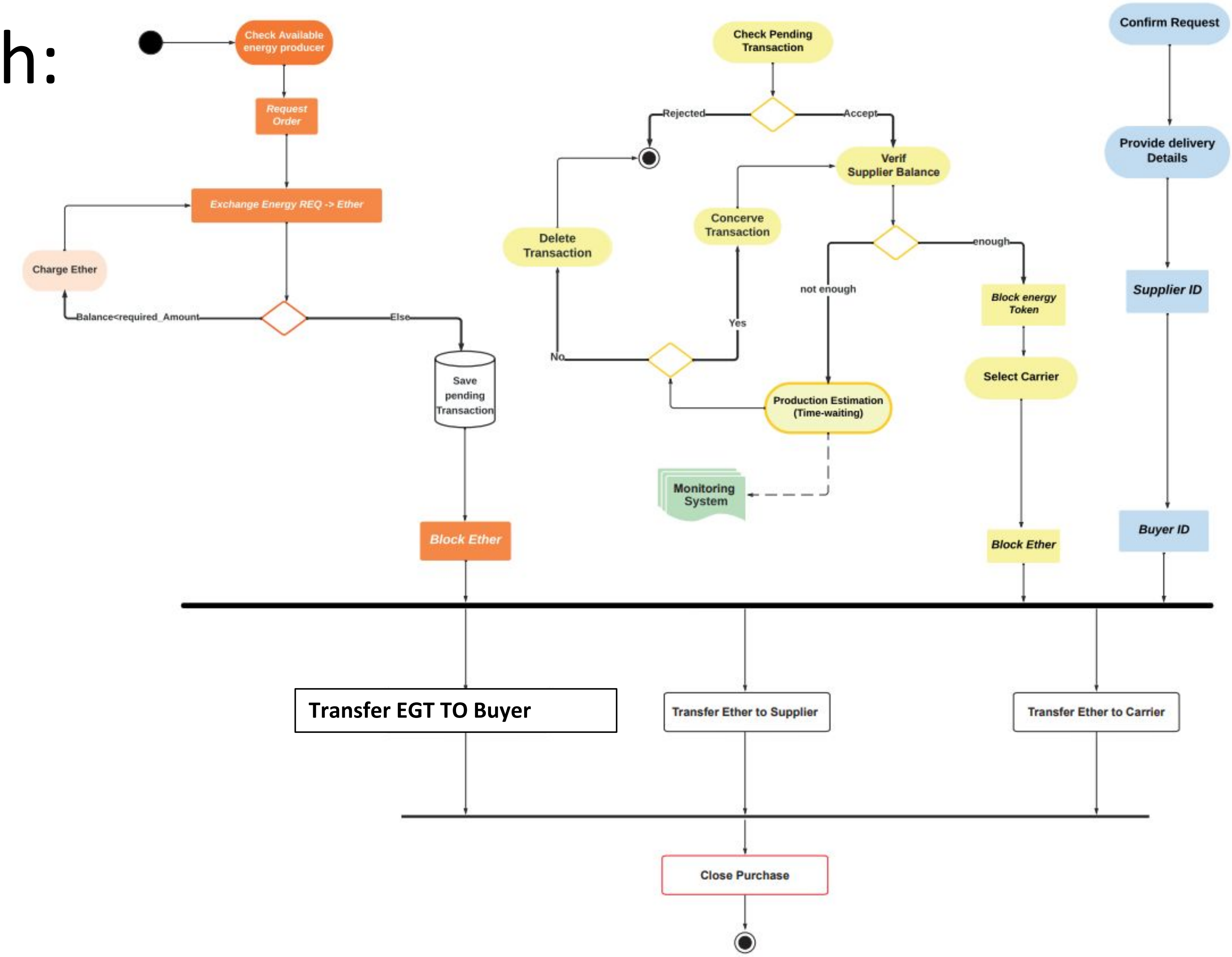
Project Approach: Supplier Activity Diagram



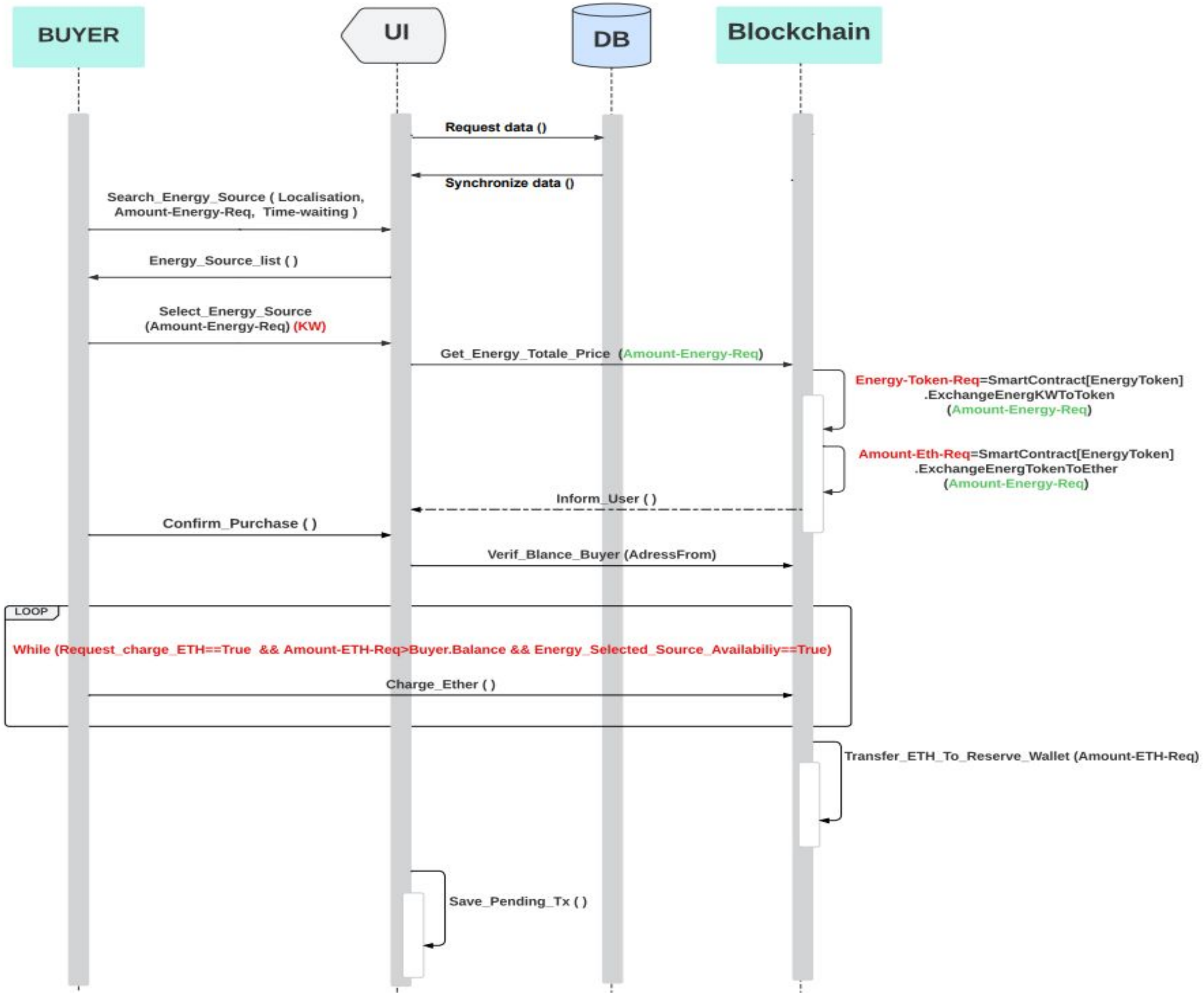
Project Approach: Carrier Activity Diagram



Project Approach: Global Activity Diagram



Project Approach: Buyer Sequence Diagram



BUYER

UI

DB

Blockchain

Request data ()

Synchronize data ()

Search_Energy_Source (Localisation, Amount-Energy-Req, Time-waiting)

Energy_Source_list ( )

Select_Energy_Source (Amount-Energy-Req) (KW)

Get_Energy_Totale_Price (Amount-Energy-Req)

Energy-Token-Req=SmartContract[EnergyToken]
.ExchangeEnergKWToToken
(Amount-Energy-Req)

Amount-Eth-Req=SmartContract[EnergyToken]
.ExchangeEnergTokenToEther
(Amount-Energy-Req)

Inform_User ( )

Confirm_Purchase ( )

Verif_Blance_Buyer (AdressFrom)

LOOP

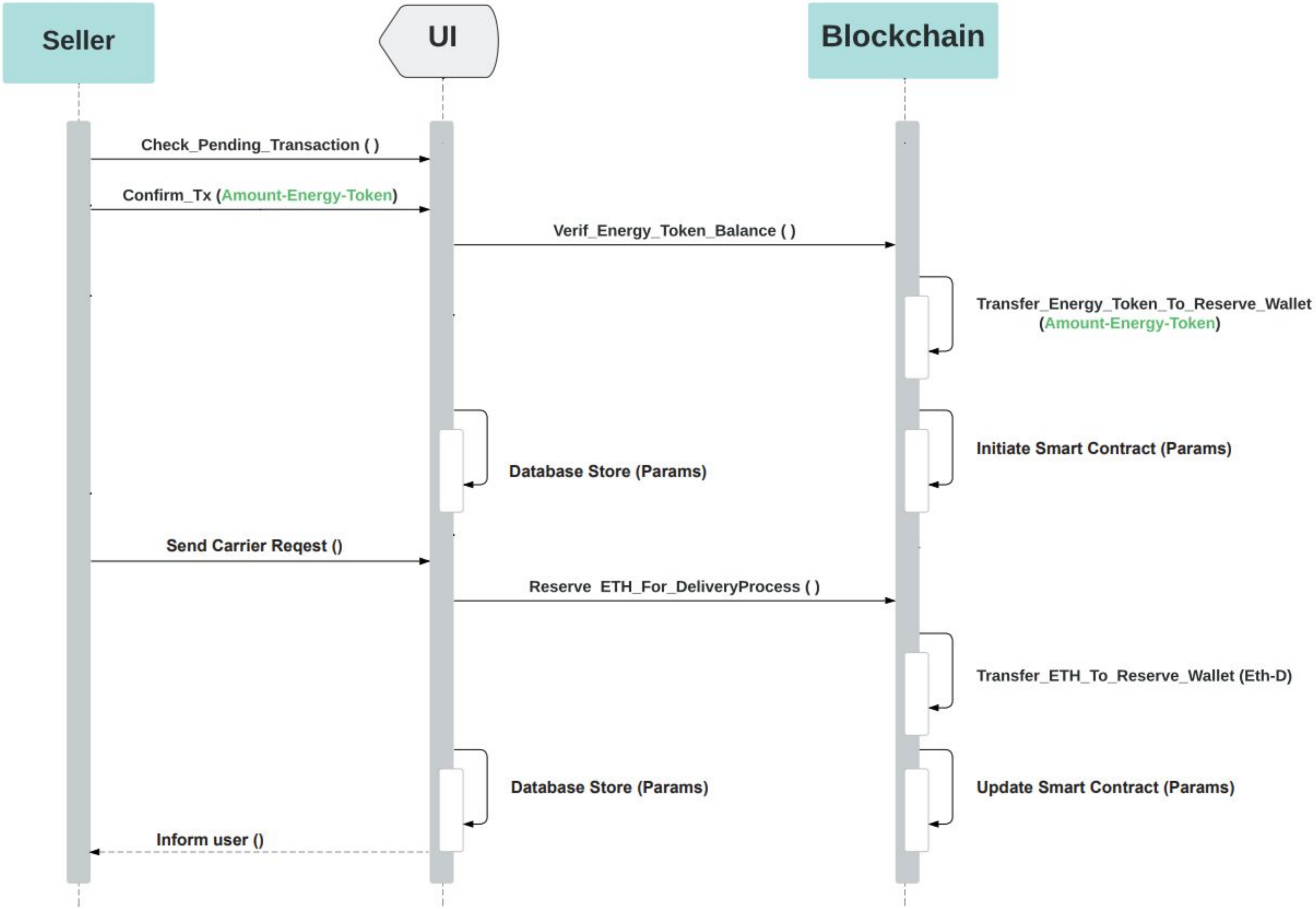
While (Request_charge_ETH==True && Amount-ETH-Req>Buyer.Balance && Energy_Selected_Source_Availabiliy==True)

Charge_Ether ( )

Transfer_ETH_To_Reserve_Wallet (Amount-ETH-Req)

Save_Pending_Tx ( )

Project Approach: Seller Sequence Diagram



Seller

UI

Blockchain

Check_Pending_Transaction ( )

Confirm_Tx (Amount-Energy-Token)

Verif_Energy_Token_Balance ( )

Transfer_Energy_Token_To_Reserve_Wallet (Amount-Energy-Token)

Database Store (Params)

Initiate Smart Contract (Params)

Send Carrier Reqest ()

Reserve ETH_For_DeliveryProcess ( )

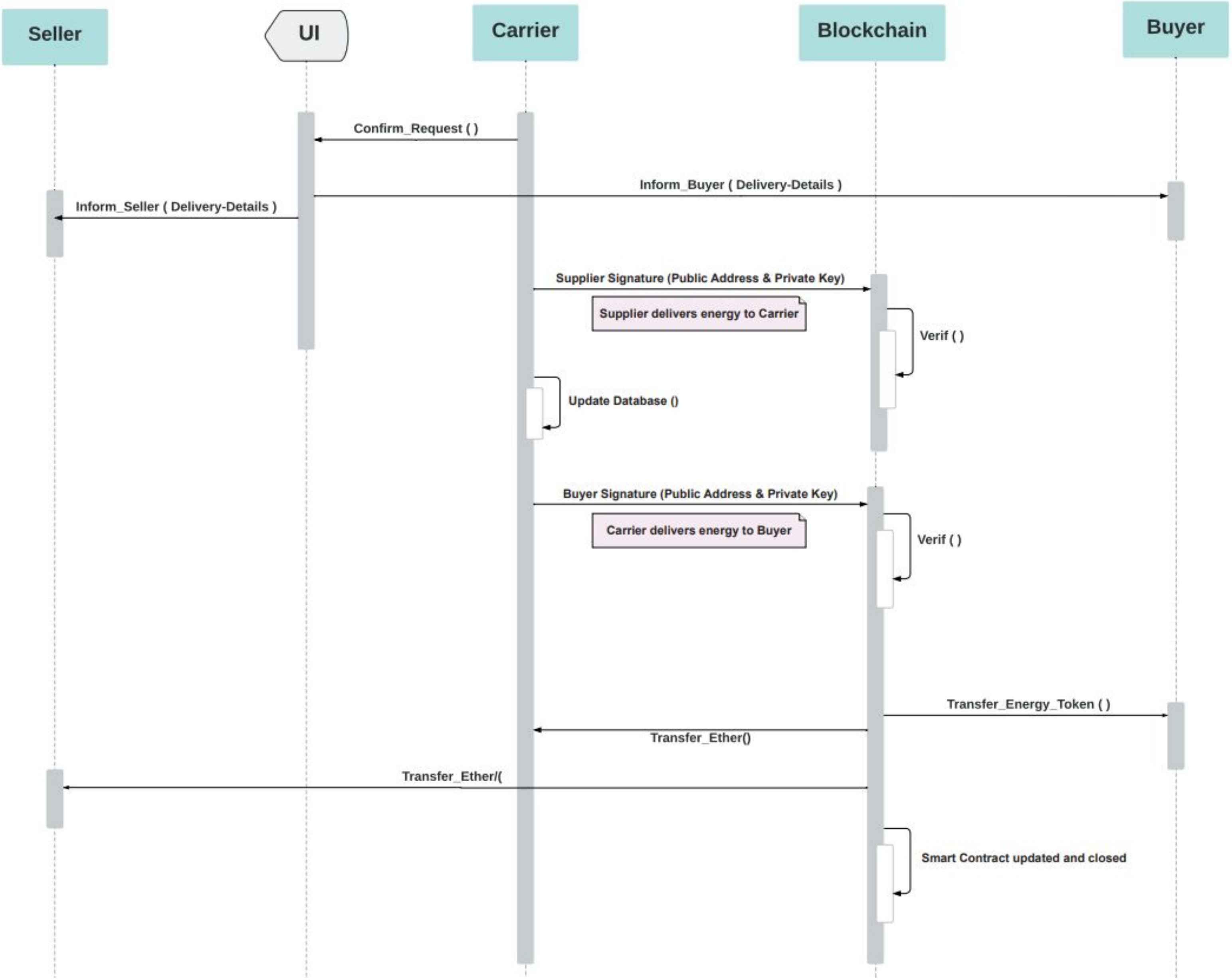
Transfer_ETH_To_Reserve_Wallet (Eth-D)

Database Store (Params)

Update Smart Contract (Params)

Inform user ()

Project Approach: Carrier Sequence Diagram



Seller

UI

Carrier

Blockchain

Buyer

Confirm_Request ( )

Inform_Buyer (Delivery-Details)

Inform_Seller (Delivery-Details)

Supplier Signature (Public Address & Private Key)

Supplier delivers energy to Carrier

Verif ( )

Update Database ()

Buyer Signature (Public Address & Private Key)

Carrier delivers energy to Buyer

Verif ( )

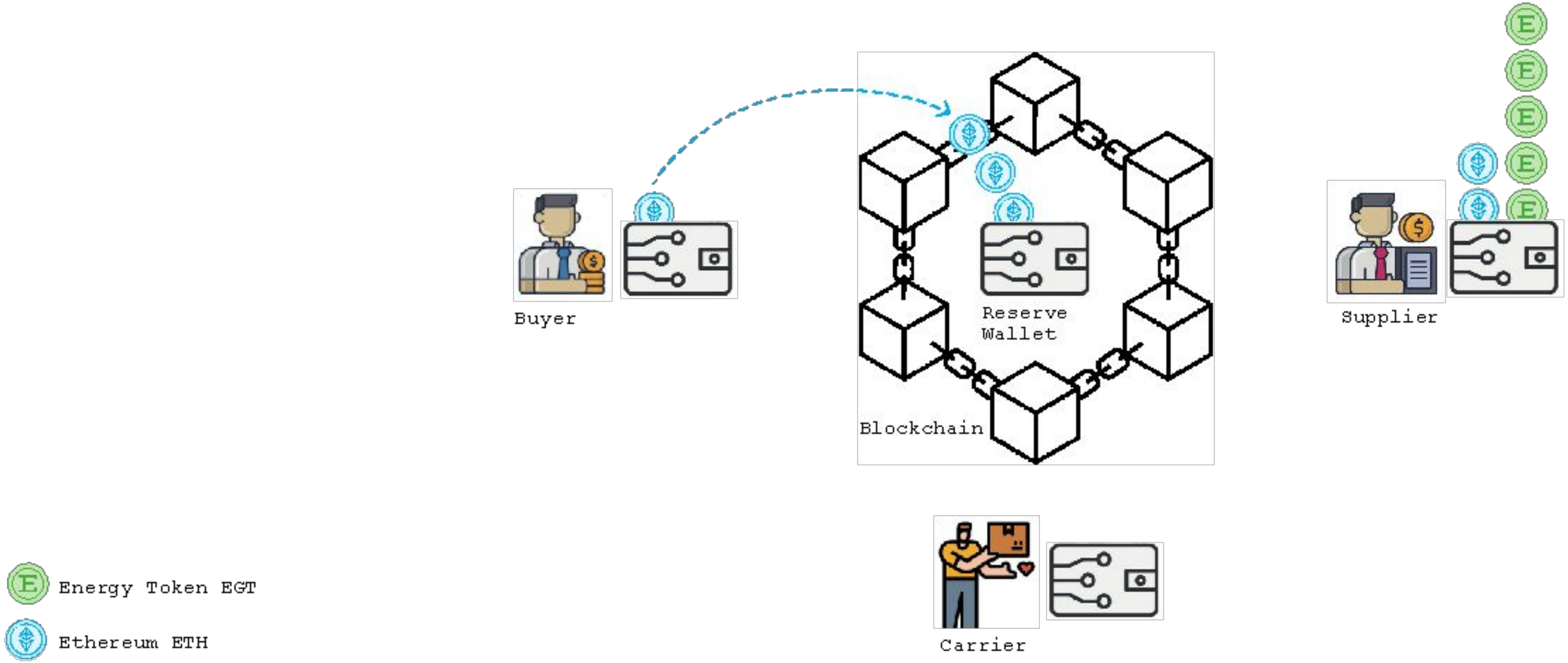
Transfer_Energy_Token ( )

Transfer_Ether()

Transfer_Ether/(

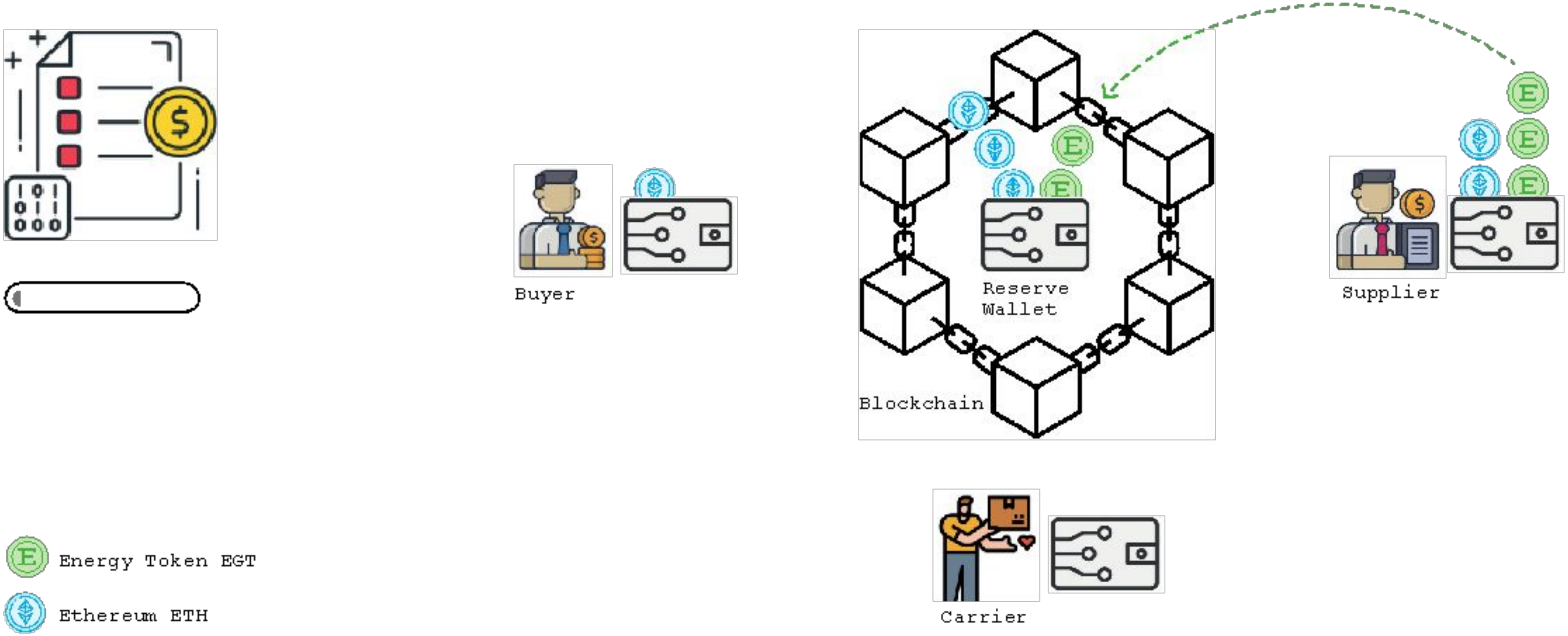
Smart Contract updated and closed

Project Approach:
Token exchange Step 1



Project Approach: Token exchange Step 2

Smart contract: initiate



Buyer

Reserve Wallet

Blockchain

Supplier

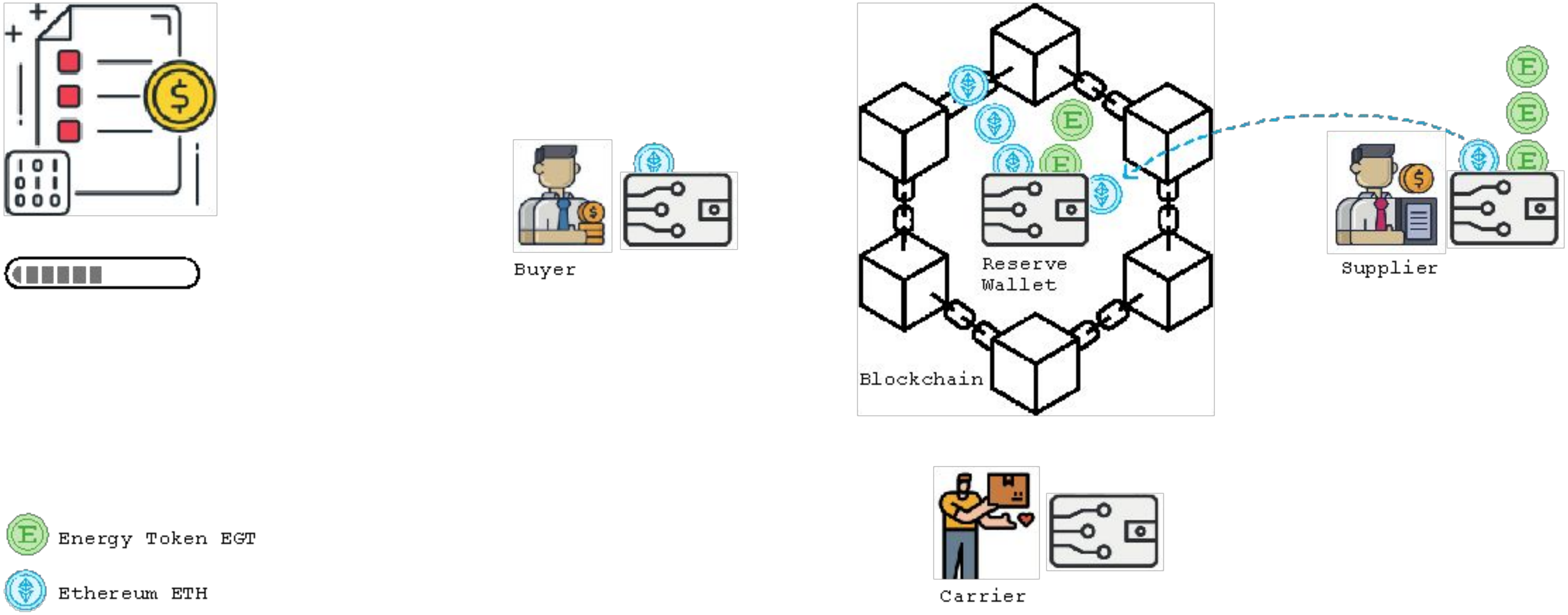
Carrier

Energy Token EGT

Ethereum ETH

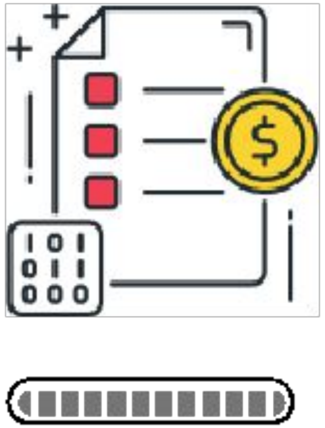
Project Approach: Token exchange Step 3

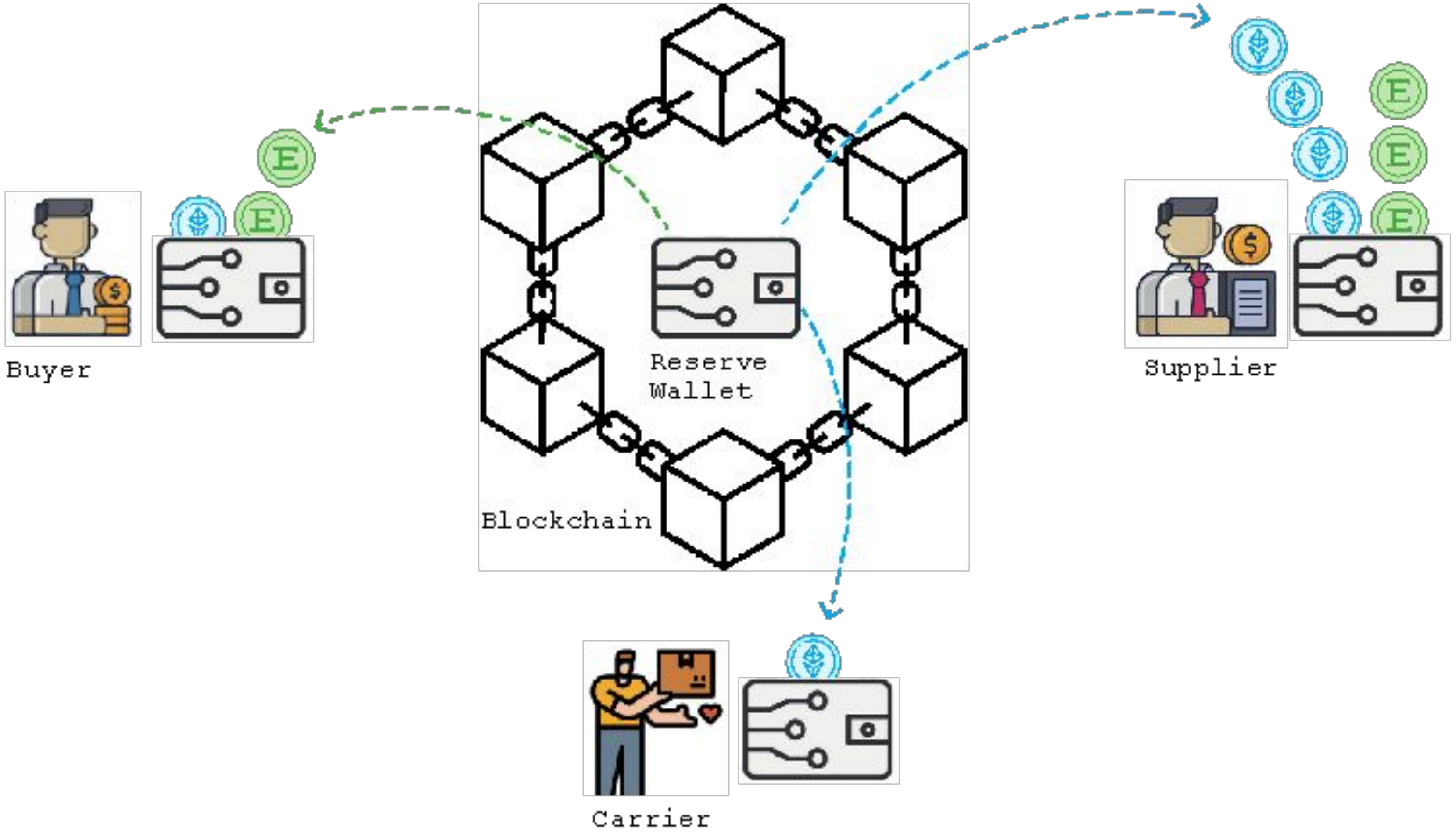
Smart contract: in progress



Project Approach: Token exchange Step 4

Smart contract: complete

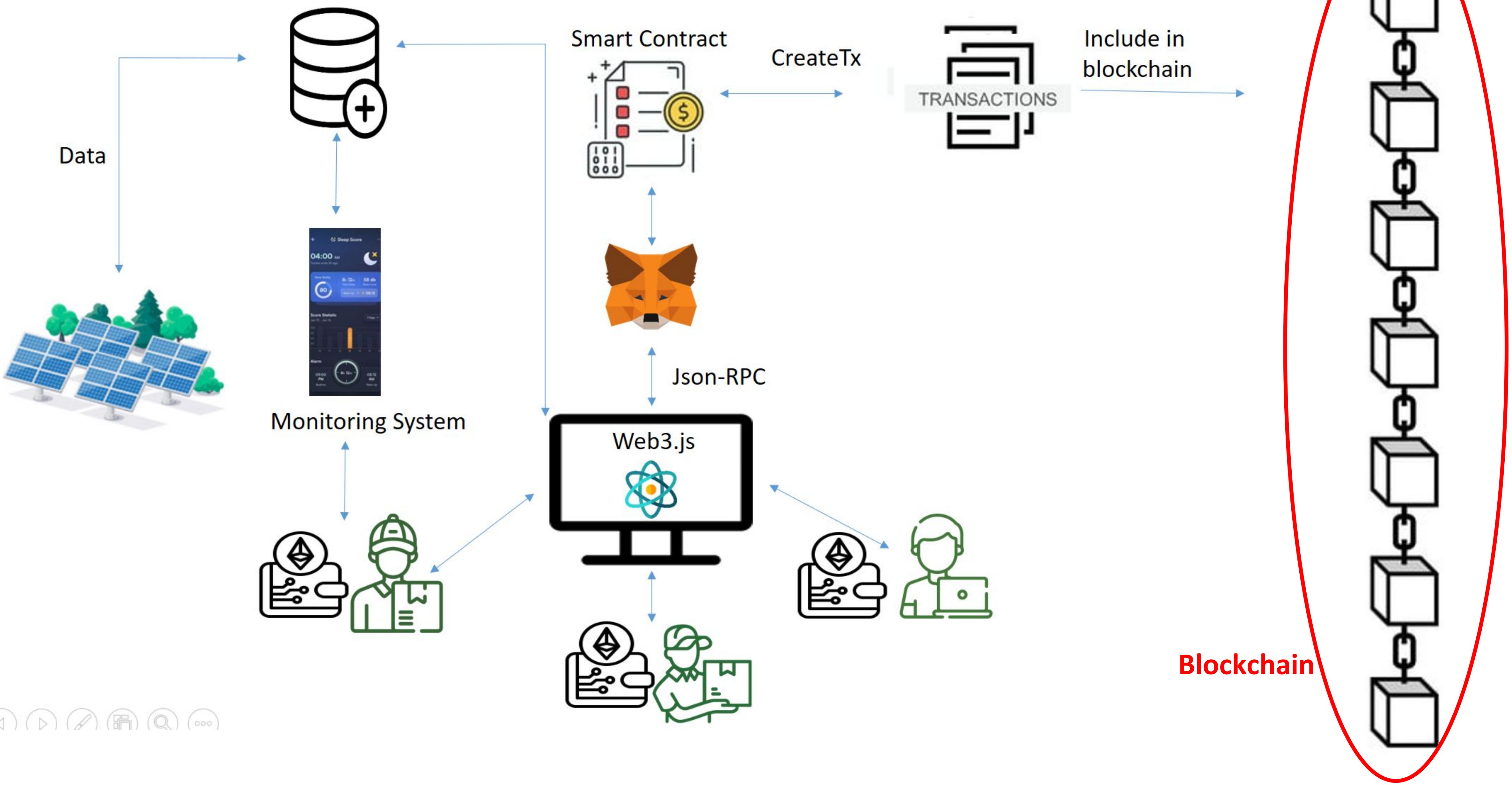




E Energy Token EGT

Ethereum ETH

Decentralized Storage : Blockchain



Decentralized Storage: Blockchain

A Globally Shared Transactional Database, Secured by Cryptographic chain of Block, Distributed Across a Decentralized Network of Computers (Nodes)

Why Blockchain in Energy Trading System ?

Trustless

- peer-to-peer transactions decentralized and distributed energy marketplace;
- Eliminates the need for intermediaries through collective verification of the ecosystem (**mining process**).

Automated Transactions:

Smart contracts

Tractability:

A transparent and immutable ledger that records all transactions and data

Confidentiality:

- full privacy and anonymity
- encryption cryptography

Public Key: identify the account

Private key: Sign the transaction and provide proof of ownership

Type Of Blockchain

[✓ Public Blockchain: Permissionless]

Private / consortium Blockchain: Permissioned

Public Blockchain: Ethereum

System of rewards and penalties that strongly incentivize participant to be honest and available online as much as possible => **Security and integrity**

Execution Layer

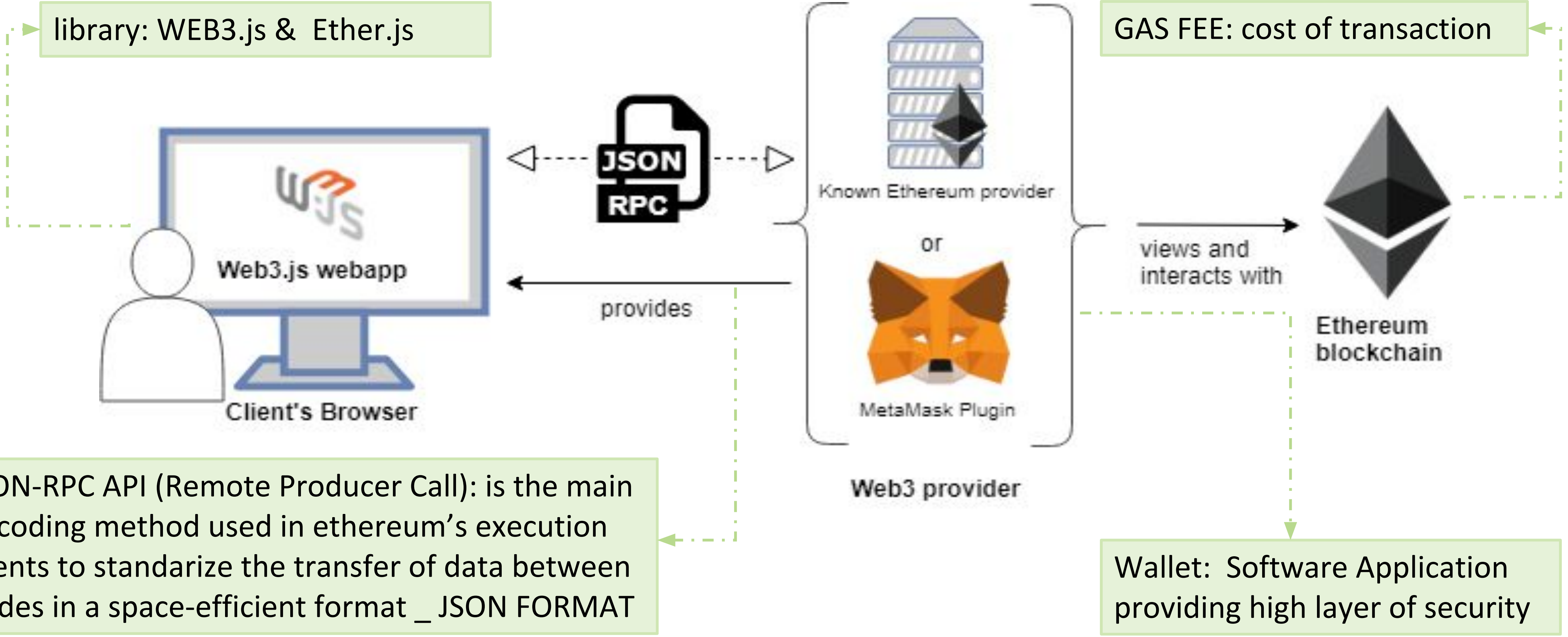
- ❑ Listen to new Transactions in the network, executes them in **Evm** and holds the latest state of data

Consensus Layer

- ❑ Implement the consensus mechanisim **Proof of Stack** which is the responsible for construction new block and incorporates the execution transaction into the block

Interaction with blockchain

- Read Block Data
- Interacting with Smart Contract
- Sending Transaction



library: WEB3.js & Ether.js

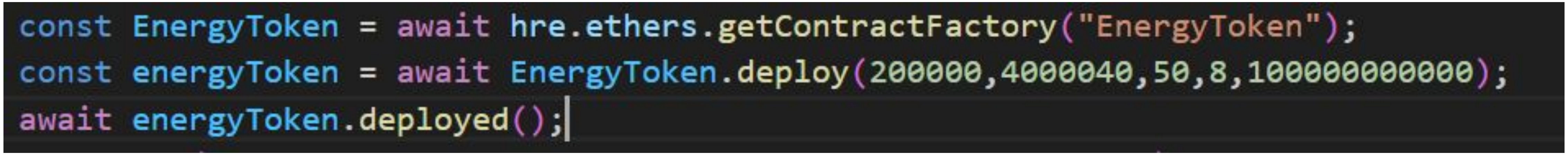
GAS FEE: cost of transaction

JSON-RPC API (Remote Producer Call): is the main encoding method used in ethereum's execution clients to standarize the transfer of data between nodes in a space-efficient format _ JSON FORMAT

Wallet: Software Application providing high layer of security

Smart Contract

- Creation phase: Solidity
- Compile and deployed phase: Hardhat, Sepolia Network and Alchamy



```
const EnergyToken = await hre.ethers.getContractFactory("EnergyToken");
const energyToken = await EnergyToken.deploy(200000,4000040,50,8,100000000000);
await energyToken.deployed();
```

- **Address**

hexadecimal string composed of 40 characters
Unique identifier that represents a deployed contract on the blockchain
It allows for interaction, verification, and value transfer to and from the contract

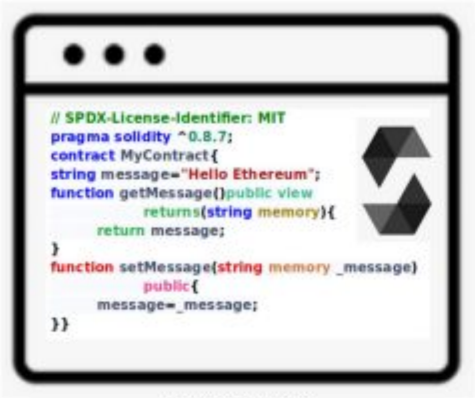
- **ABI: Application Binary Interface**

Standard to communicate with smart contract
Smart contract uses ABI to interpret and decode the data received
Also when a smart contract sends data it encodes the data according to the ABI

- **Bytcode**

low-level representation of the contract's instructions that can be directly executed by the blockchain's virtual machine (EVM)

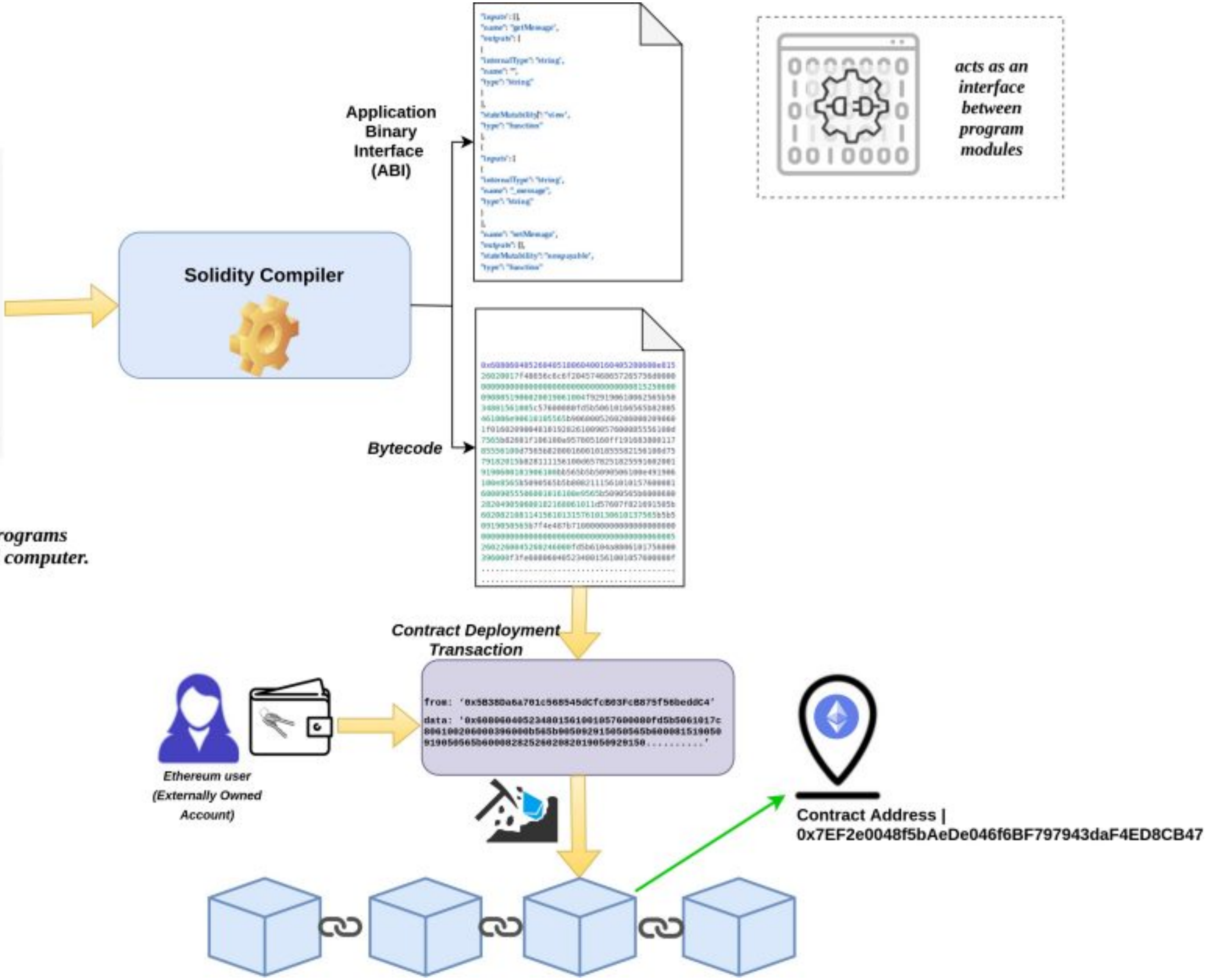
DEPLOYMENT OF A SMART CONTRACT



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.7;
contract MyContract{
string message="Hello Ethereum";
function getMessage()public view
            returns(string memory){
      return message;
}
function setMessage(string memory _message)
            public{
      message=_message;
}}
```

Smart Contract

Smart Contracts are immutable computer programs that run on the decentralized Ethereum world computer.



Solidity Compiler
Application Binary Interface (ABI)
acts as an interface between program modules
Bytecode
Contract Deployment Transaction
Ethereum user (Externally Owned Account)
Contract Address | 0x7EF2e0048f5bAeDe046f6BF797943daF4ED8CB47

```
"inputs":[],
"name": "getMessage",
"outputs": [
{
"internalType": "string",
"name": "",
"type": "string"
}
],
"stateMutability": "view",
"type": "function"
},
{
"inputs":[
{
"internalType": "string",
"name": "_message",
"type": "string"
}
],
"name": "setMessage",
"outputs": [],
"stateMutability": "nonpayable",
"type": "function"
```

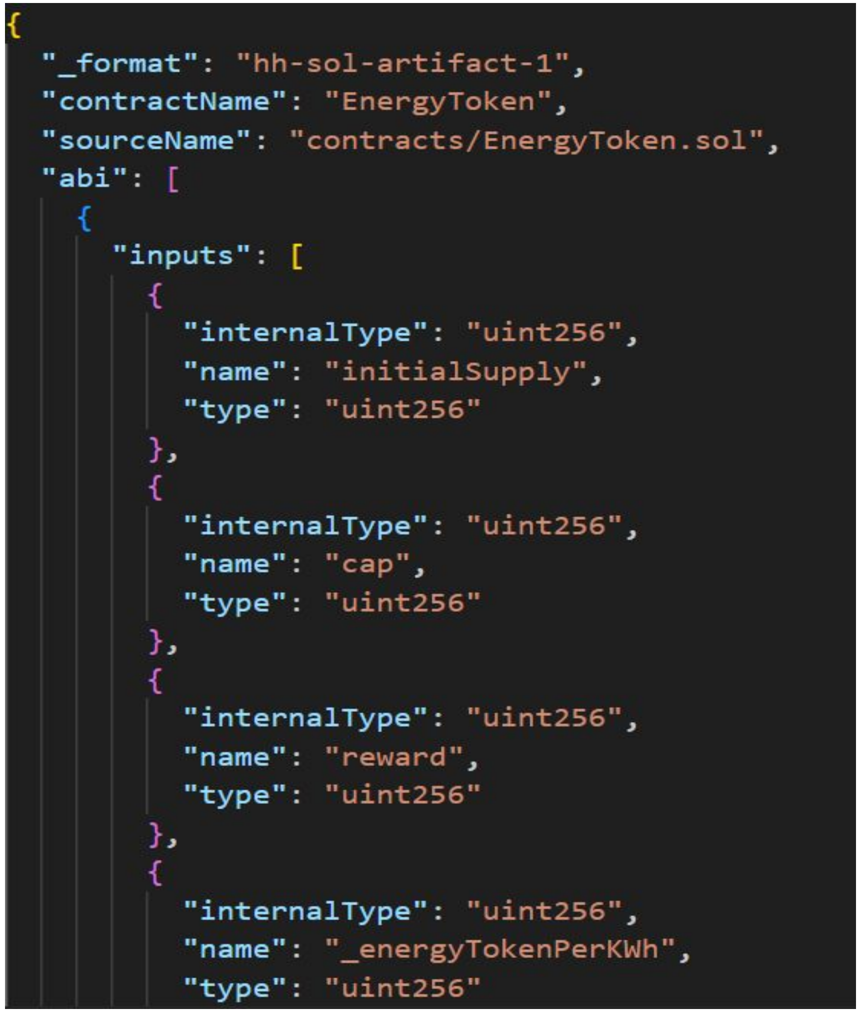
```
0x608060405260405180604001604052806000e815
26020017f48656c6c6f20457468657265756d0000
0000000000000000000000000000000815250000
090805190602001906100042929190610062565b50
348015610005c576000000fd5b5061010665565b82805
461000e90061010556565b60600005260200000209060
1f016020900481019282610090576000085556100d
75655b82801f106100a957805160ff19168380011
785550100d75655b8280016001010855582156100d75
79182015b82811115610006578251825591602001
919060010190610000b565b5b5090506100e491906
100e8565b5090565b5b8082111561010157600081
600090555000010161000e9565b509056565b0000680
2820490506000182168061011d57607f8216915050b
60208210811415610131576101306101375655b5b5
091905056565b7f4e487b71000000000000000000000
0000000000000000000000000000000000000000085
2600226000452602460000fd5b6104b08061017560000
3960000f3fe608060405234801561001057600000f
.........................................
.........................................
```

```
from: '0x5B38Da6a701c568545dCfcB03FcB875f56beddC4'

data: '0x608060405234801561001057600080fd5b5061017c
80610020600003960000b565b90505092915050565b600081519050
91905056565b6000828252602082019050929150...........'
```

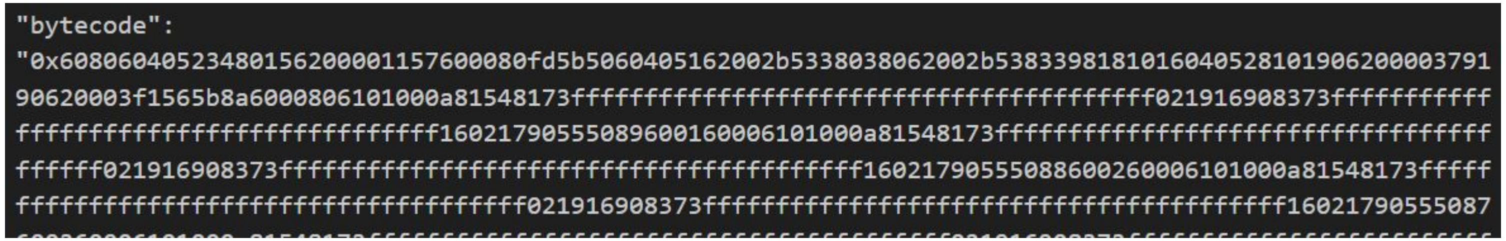
Address: 0x872072D791e7bd761c9501c7CC2ea2CF5cFFb0FB

ABI



```
{
  "_format": "hh-sol-artifact-1",
  "contractName": "EnergyToken",
  "sourceName": "contracts/EnergyToken.sol",
  "abi": [
    {
      "inputs": [
        {
          "internalType": "uint256",
          "name": "initialSupply",
          "type": "uint256"
        },
        {
          "internalType": "uint256",
          "name": "cap",
          "type": "uint256"
        },
        {
          "internalType": "uint256",
          "name": "reward",
          "type": "uint256"
        },
        {
          "internalType": "uint256",
          "name": "_energyTokenPerKWh",
          "type": "uint256"
```

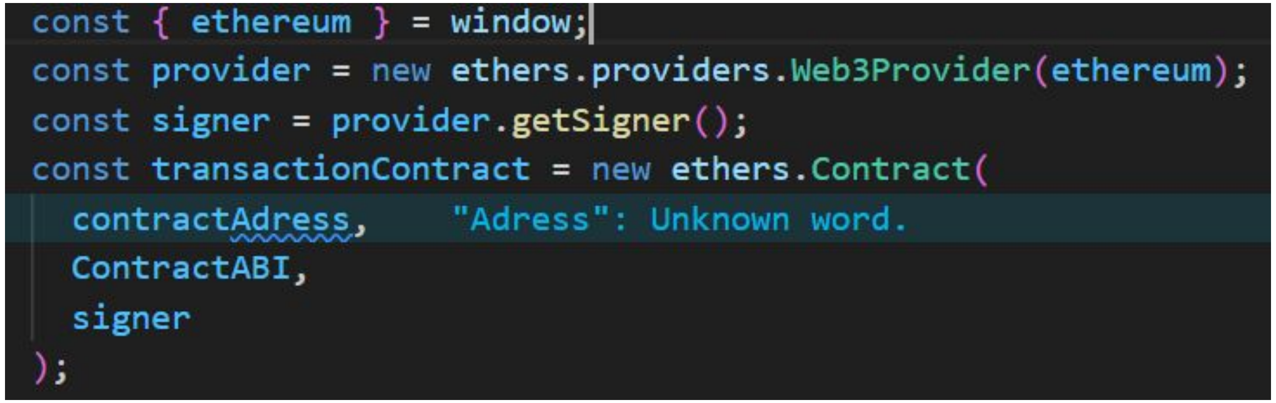
Bytecode



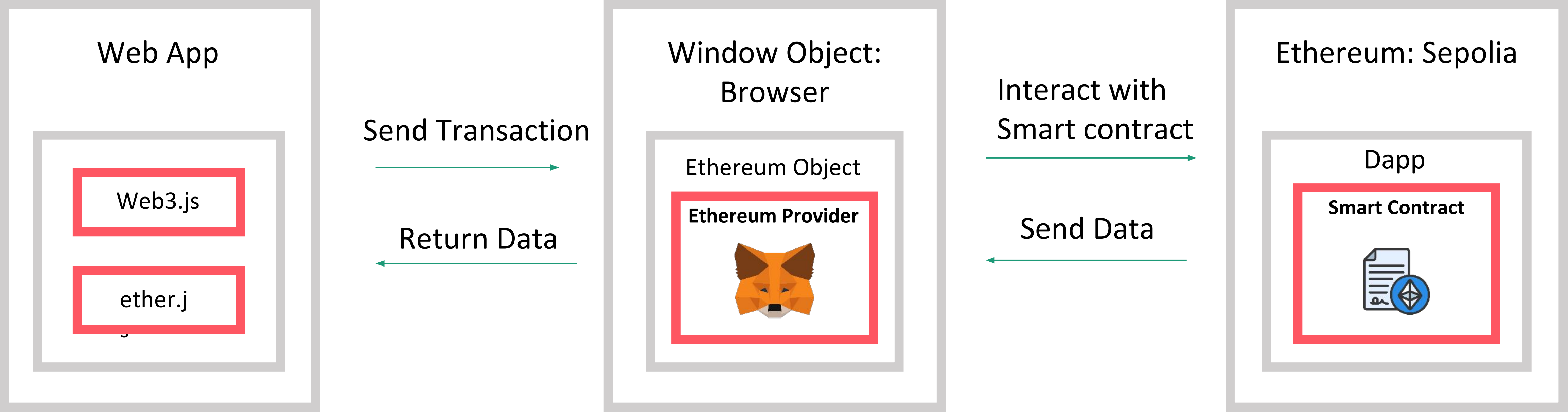
```
"bytecode":
"0x60806040523480156200001157600080fd5b5060405162002b5338038062002b538339818101604052810190620000379190620003f1565b8a6000806101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff16021790555089600160006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff16021790555088600260006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff16021790555087
```

To interact with the deployed smart contract use the address and the ABI

To create (deploy) new instance of an existing smart contract use the ABI and the bytcode => new address



```
const { ethereum } = window;
const provider = new ethers.providers.Web3Provider(ethereum);
const signer = provider.getSigner();
const transactionContract = new ethers.Contract(
  contractAdress,     "Adress": Unknown word.
  ContractABI,
  signer
);
```



Web App

Web3.js

ether.j

Send Transaction

Return Data

Window Object: Browser

Ethereum Object

Ethereum Provider

Interact with Smart contract

Send Data

Ethereum: Sepolia

Dapp

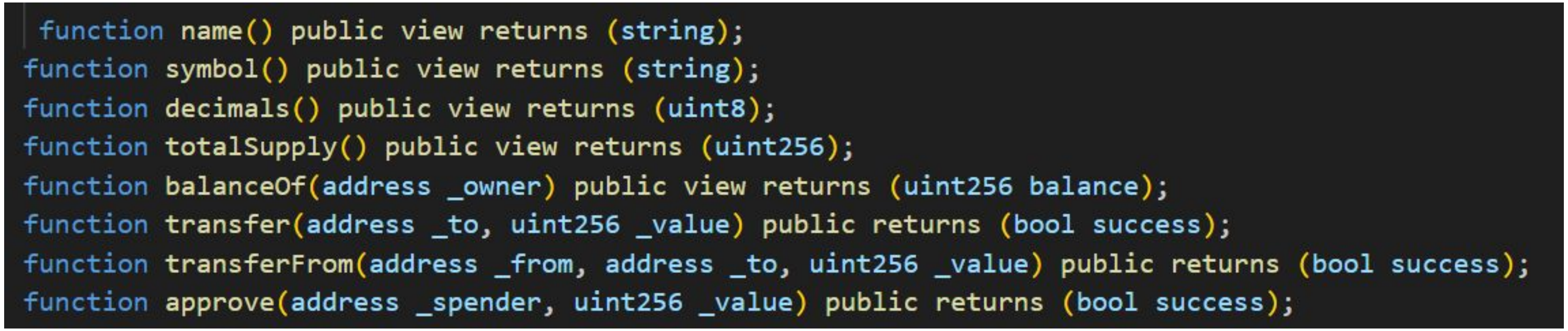
Smart Contract

Energy Token

Energy Token **EGT**: digital presentation of unit of energy can be bought, sold and traded like any other asset.

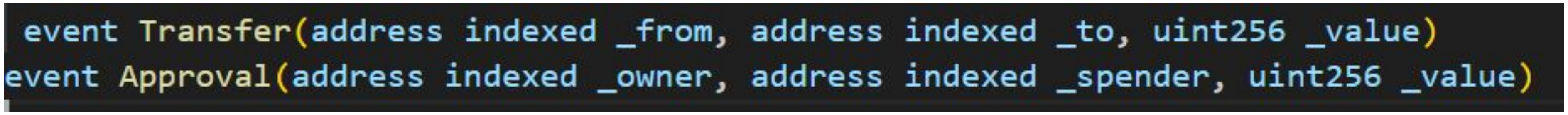
Difference between coin and token:
Coin: refers to the native cryptocurrency of a specific blockhain like Bitcoin, Ether.
Coded on the core protocol level and not on the smart contract level.
Token: is a cryptocurrency built on top of an existing blockchain

ERC20 « Ethereum Request for Comments **»** standard (interface) provides a set of **rules** and **functions** that define how tokens should behave on the Ethereum platform.



```
function name() public view returns (string);
function symbol() public view returns (string);
function decimals() public view returns (uint8);
function totalSupply() public view returns (uint256);
function balanceOf(address _owner) public view returns (uint256 balance);
function transfer(address _to, uint256 _value) public returns (bool success);
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success);
function approve(address _spender, uint256 _value) public returns (bool success);
```

Functions

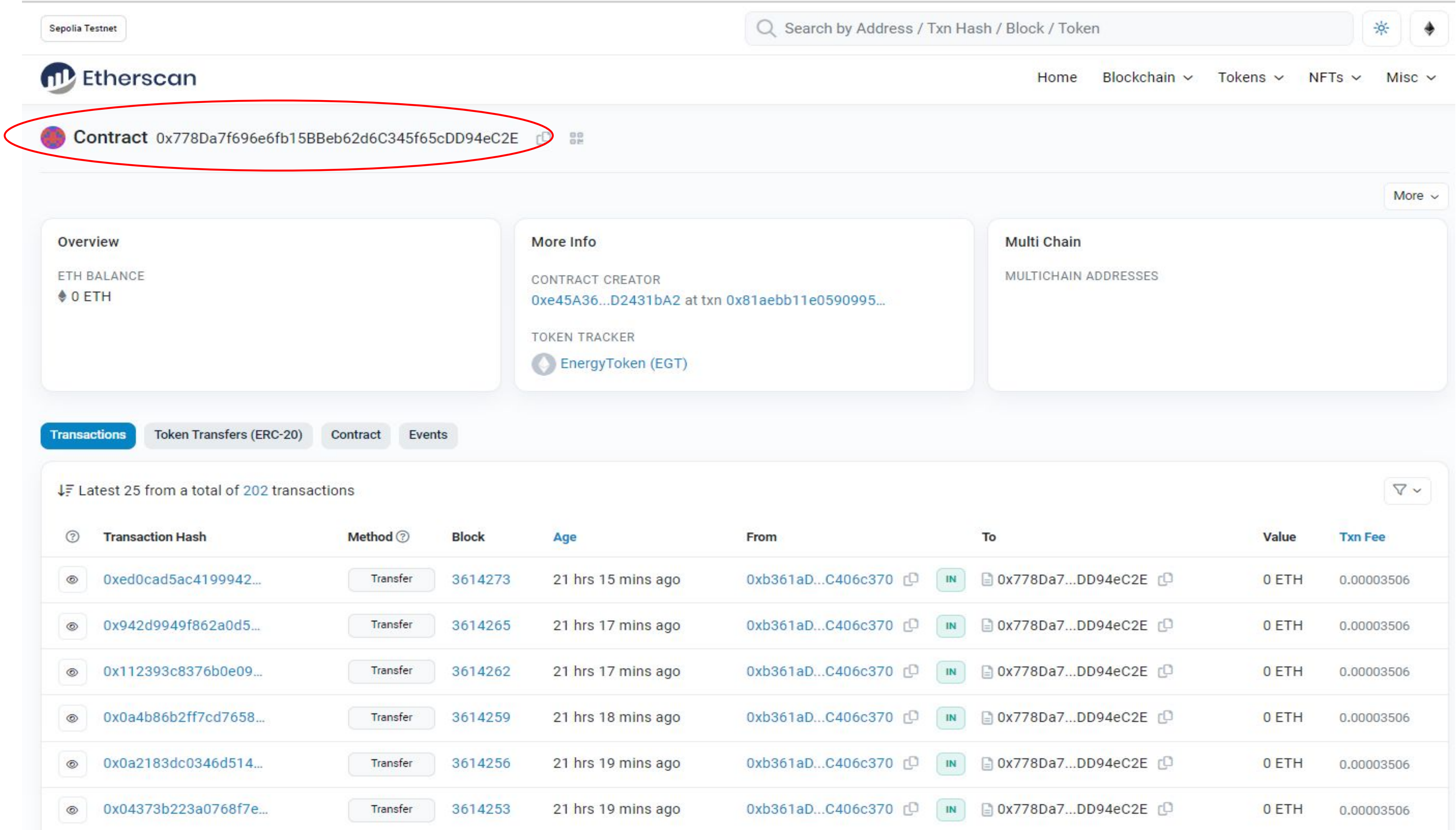


```
event Transfer(address indexed _from, address indexed _to, uint256 _value)
event Approval(address indexed _owner, address indexed _spender, uint256 _value)
```

Event

OpenZeppelin

Smart Contract: 0x778Da7f696e6fb15BBeb62d6C345f65cDD94eC2E



Contract 0x778Da7f696e6fb15BBeb62d6C345f65cDD94eC2E

Overview

ETH BALANCE
0 ETH

More Info

CONTRACT CREATOR
0xe45A36...D2431bA2 at txn 0x81aebb11e0590995...

TOKEN TRACKER
EnergyToken (EGT)

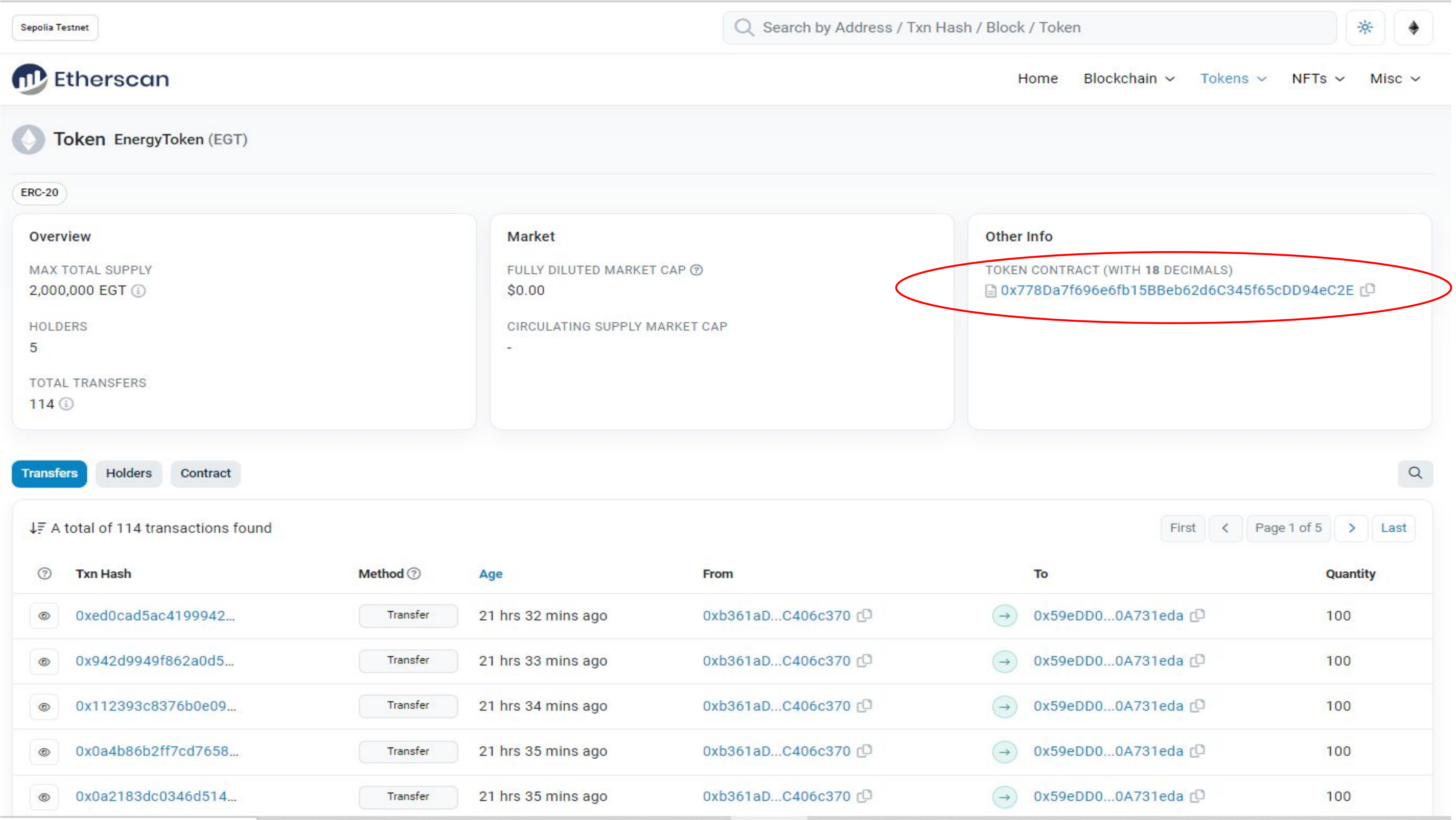
Multi Chain

MULTICHAIN ADDRESSES

Latest 25 from a total of 202 transactions

Transaction Hash	Method	Block	Age	From		To	Value	Txn Fee
0xed0cad5ac4199942...	Transfer	3614273	21 hrs 15 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506
0x942d9949f862a0d5...	Transfer	3614265	21 hrs 17 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506
0x112393c8376b0e09...	Transfer	3614262	21 hrs 17 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506
0x0a4b86b2ff7cd7658...	Transfer	3614259	21 hrs 18 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506
0x0a2183dc0346d514...	Transfer	3614256	21 hrs 19 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506
0x04373b223a0768f7e...	Transfer	3614253	21 hrs 19 mins ago	0xb361aD...C406c370	IN	0x778Da7...DD94eC2E	0 ETH	0.00003506

Energy Token EGT for « 0x778Da7f696e6fb15BBeb62d6C345f65cDD94eC2E »



Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

Home Blockchain Tokens NFTs Misc

Token EnergyToken (EGT)

ERC-20

Overview

MAX TOTAL SUPPLY
2,000,000 EGT

HOLDERS
5

TOTAL TRANSFERS
114

Market

FULLY DILUTED MARKET CAP
$0.00

CIRCULATING SUPPLY MARKET CAP
-

Other Info

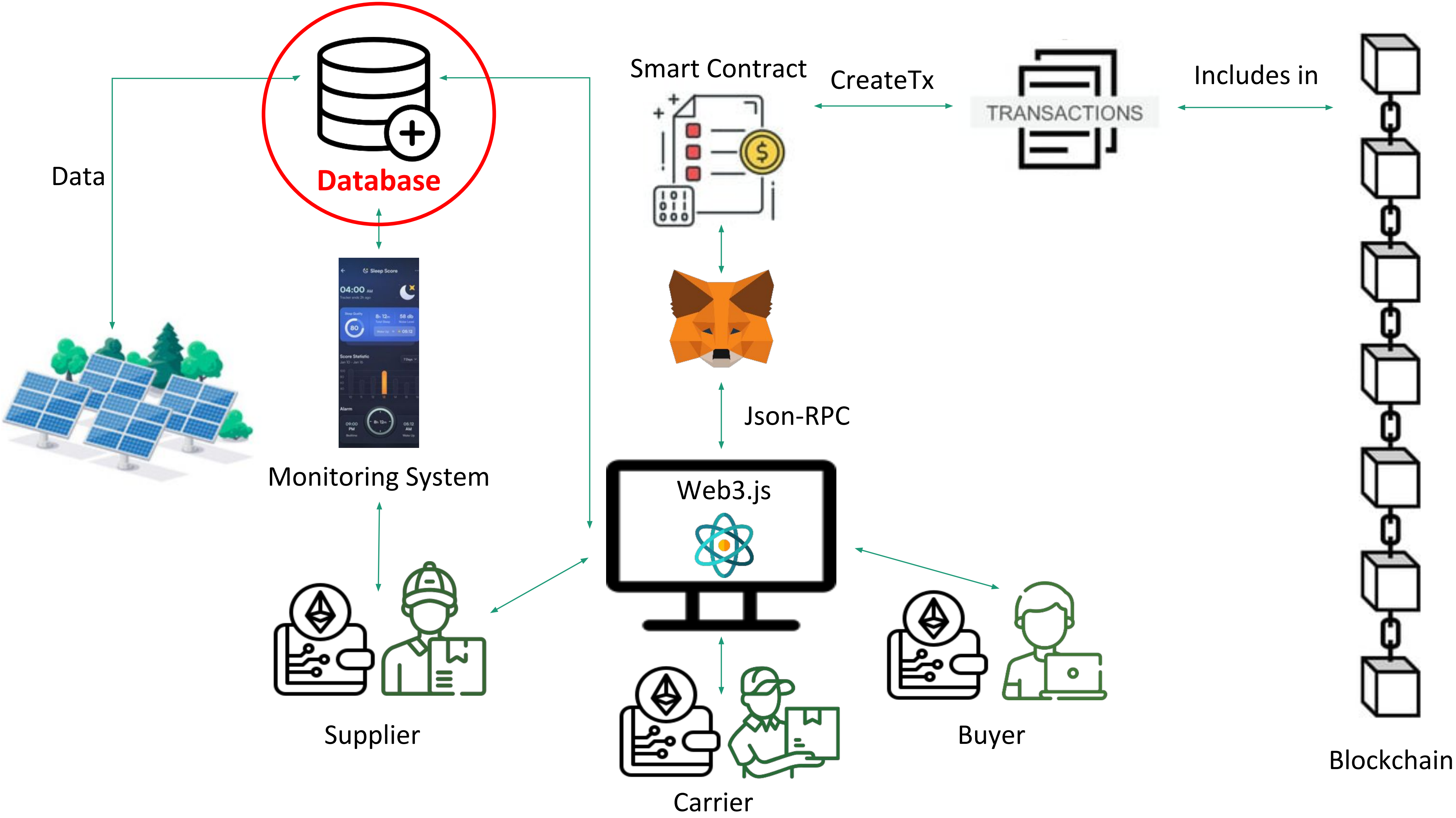
TOKEN CONTRACT (WITH 18 DECIMALS)
0x778Da7f696e6fb15BBeb62d6C345f65cDD94eC2E

Transfers Holders Contract

A total of 114 transactions found

First < Page 1 of 5 > Last

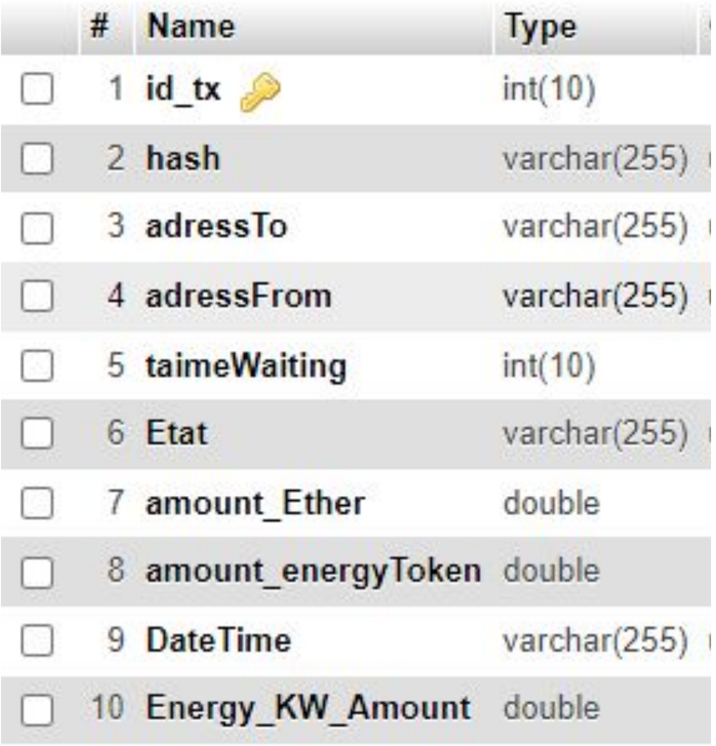
Txn Hash	Method	Age	From		To	Quantity
0xed0cad5ac4199942...	Transfer	21 hrs 32 mins ago	0xb361aD...C406c370	→	0x59eDD0...0A731eda	100
0x942d9949f862a0d5...	Transfer	21 hrs 33 mins ago	0xb361aD...C406c370	→	0x59eDD0...0A731eda	100
0x112393c8376b0e09...	Transfer	21 hrs 34 mins ago	0xb361aD...C406c370	→	0x59eDD0...0A731eda	100
0x0a4b86b2ff7cd7658...	Transfer	21 hrs 35 mins ago	0xb361aD...C406c370	→	0x59eDD0...0A731eda	100
0x0a2183dc0346d514...	Transfer	21 hrs 35 mins ago	0xb361aD...C406c370	→	0x59eDD0...0A731eda	100


Database
Data
Smart Contract
CreateTx
TRANSACTIONS
Includes in
Sleep Score
04:00 AM
80
Score Statistic
Alarm
Monitoring System
Json-RPC
Web3.js
Supplier
Carrier
Buyer
Blockchain

Centralized Storage

- Pending Transaction

Efficient data manipulation and management during pending transactions.

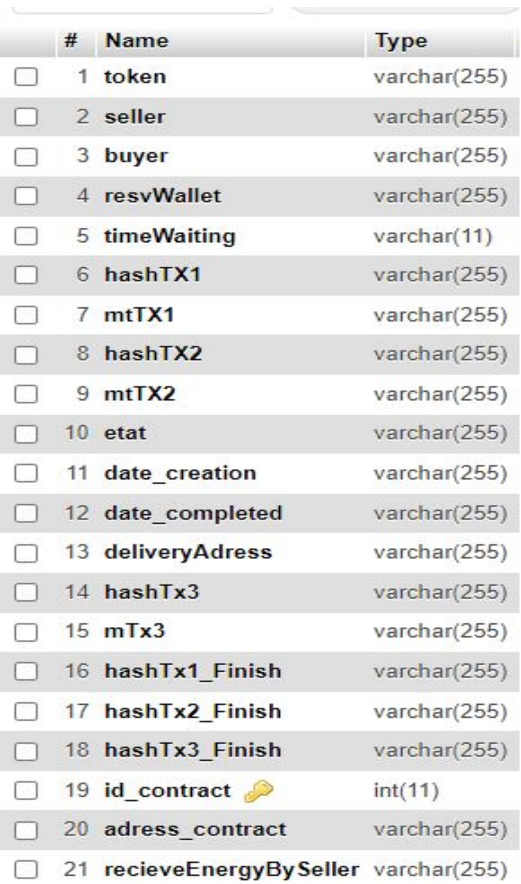


	#	Name	Type
□	1	id_tx	int(10)
□	2	hash	varchar(255)
□	3	adressTo	varchar(255)
□	4	adressFrom	varchar(255)
□	5	taimeWaiting	int(10)
□	6	Etat	varchar(255)
□	7	amount_Ether	double
□	8	amount_energyToken	double
□	9	DateTime	varchar(255)
□	10	Energy_KW_Amount	double

Transaction

- Smart Contract (in process)

handling transaction fees when the smart contract in progress to have access (retrieve smart contract Data) without need in each time to interact with blockchain

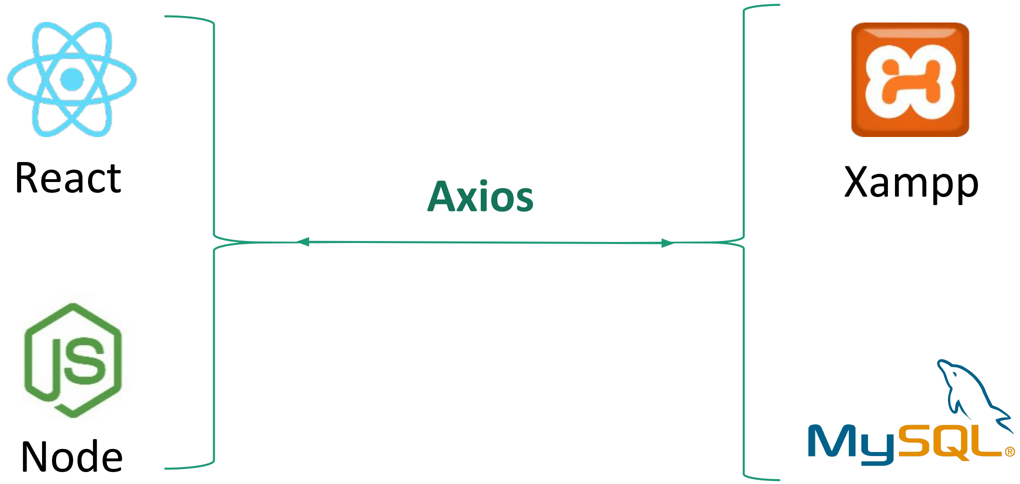


	#	Name	Type
□	1	token	varchar(255)
□	2	seller	varchar(255)
□	3	buyer	varchar(255)
□	4	resvWallet	varchar(255)
□	5	timeWaiting	varchar(11)
□	6	hashTX1	varchar(255)
□	7	mtTX1	varchar(255)
□	8	hashTX2	varchar(255)
□	9	mtTX2	varchar(255)
□	10	etat	varchar(255)
□	11	date_creation	varchar(255)
□	12	date_completed	varchar(255)
□	13	deliveryAdress	varchar(255)
□	14	hashTx3	varchar(255)
□	15	mTx3	varchar(255)
□	16	hashTx1_Finish	varchar(255)
□	17	hashTx2_Finish	varchar(255)
□	18	hashTx3_Finish	varchar(255)
□	19	id_contract	int(11)
□	20	adress_contract	varchar(255)
□	21	recieveEnergyBySeller	varchar(255)

Contract

Technologies

- Web App
- Centralized Store
- Decentralized Store



Vite

tailwindcss v3.0

ethereum

Sepolia Testnet

alchemy

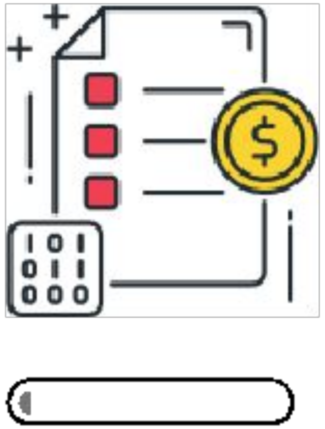
Ethereum wallet: metamask

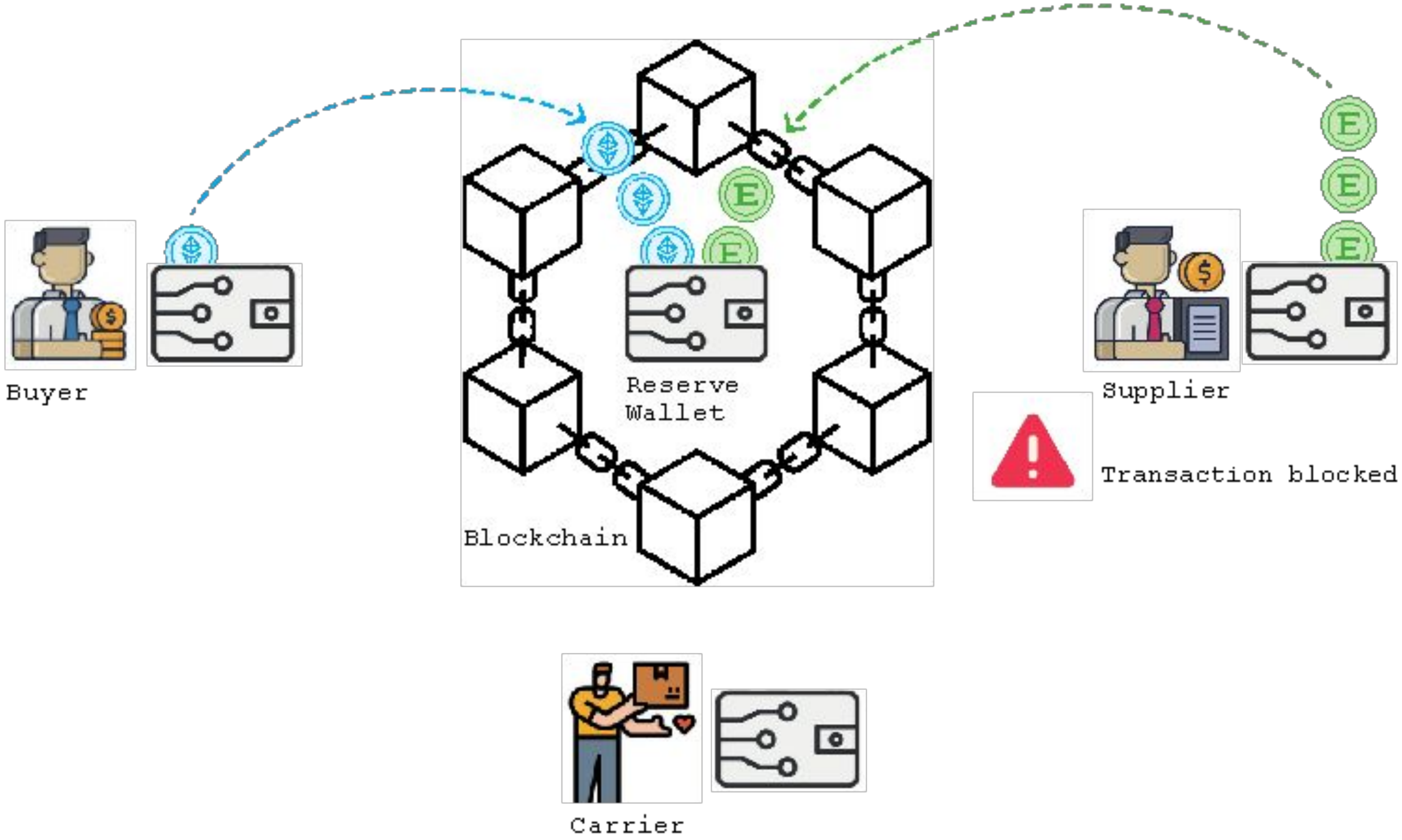
Hardhat

Solidity

Information flow

Transaction blocked





Ⓔ Energy Token EGT

● Ethereum ETH

Future work

- Designing a Highly Adaptable Interface for Every System Actors
- Enhancing Flexibility in the Transportation System: Empowering Buyers to Take Charge
- Modeling and Formal Analysis of the System Using Process Algebra

Demonstration

- DEMO Implementation

Thank you for your attention