EUREKA

Prerequisites

IMPORTANT, please complete the following

- 1. Read the <u>Polkadot x EasyA notion page</u>, this should be like your "rule book" for the hackathon, refer to this when in doubt
- 2. Complete the Polkadot crash course on the EasyA app, you can get the app from easya.io
- 3. Setup the required software on your computer:
 - 1. VSCode*
 - 2. Github*
 - 3. Git*
 - 4. Metamask wallet*
 - 5. TRAC Test tokens*1
 - 6. WND Test tokens, WND Config*
 - 7. ChatGPT*
 - 8. Lovable*
 - 9. Metamask tools**
 - 10. Docker***
 - 11. Canva (frontend requirement)
 - 12. NPM/NVM (frontend requirement)
 - 13. Python (backend requirement)
 - 14. PAPI (frontend requirement)
 - 15. Substrate API Sidecar (frontend requirement)
 - 16. Polkadot SDK (backend requirement) // To build your own blockchain
 - 17. Subxt (backend requirement) RUST **
 - 18. Pallet-Revive (backend requirement)
 - 19. DKG SDK (backend requirement)
 - 20. Cursor (optional but useful for development)

- *1 NOTE this will show as 0 in metamask wallet even after you have tokens due to UX bug with Metamask
- ** need both Metamask SDK and Wallet API
- *** only required if you want to run the app on your laptop (other option is for us to deploy to a server)

^{*} required;

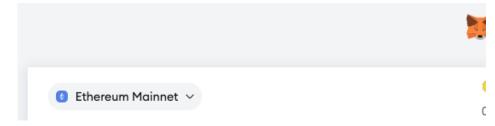
Please put your wallet Addresses below, we all need to get test tokens to test our app so create a test metamask account (DON'T USE YOUR MAIN CRYPTO WALLET)

Name	WND (Polkadot) Address	TRAC (NeuroWeb) Address	ETH (Sepolia) Address
Daniel	0x65B85C546fbb0211aCd676a8 52397588360fAC37	0x65B85C546fbb0211aCd676a8 52397588360fAC37	0x65B85C546fbb0211aCd676a8 52397588360fAC37
Yuri			
Jack	0xeb202166015976623cDe87 d4f2cAeF41abdb7177		0xeb202166015976623cDe87 d4f2cAeF41abdb7177
Gustavo	0x5a7Ef77ED01cd50e094F6cbc 65e3416010a0B6B2		0x5a7Ef77ED01cd50e094F6cbc 65e3416010a0B6B2
Faris			

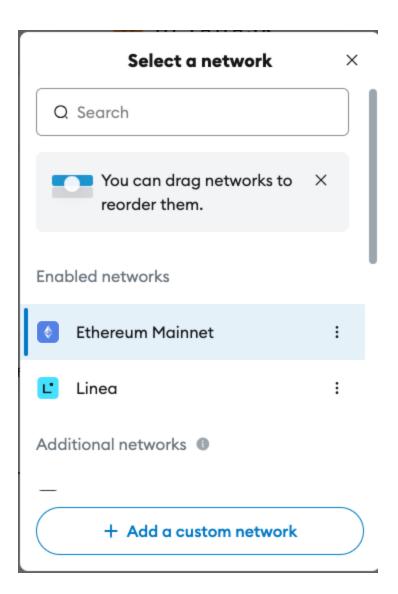
Guide to add Tokens to Meta Mask Wallet

Follow these steps to add WND to Meta Mask Wallet:

1. Click on "Ethereum Mainnet" button



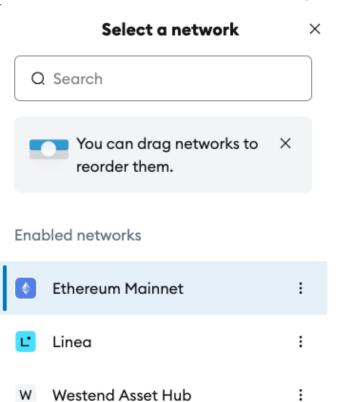
2. Click on "Add a custom network" button



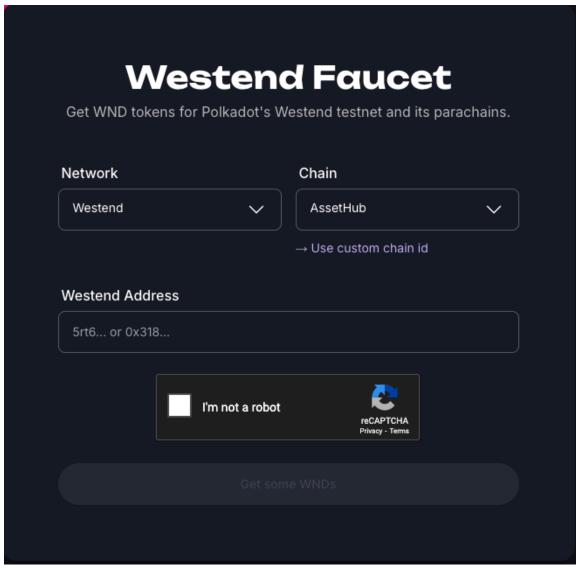
3. Fill out the details using https://contracts.polkadot.io/connect-to-asset-hub/

Netw	ork name
We	stend Asset Hub
Defau	ilt RPC URL
wes	stend-asset-hub-eth-rpc.polka 🔻
Chair	n ID
420)420421
Curre	ncy symbol
WN	ID
Block	explorer URL
blo	ckscout-asset-hub.parity-chai 、

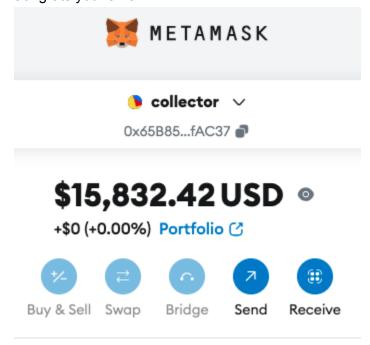
4. Now select "Westend Asset Hub" network from your wallet



5. Fill out the address on West End Faucet

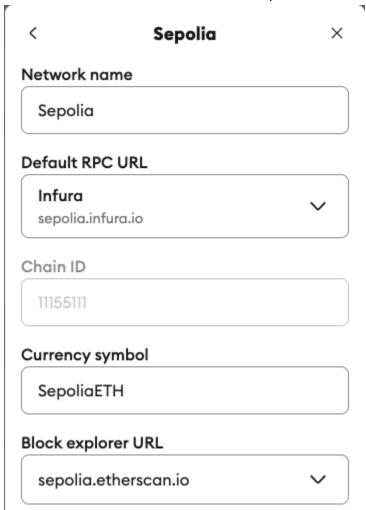


6. Congrats you're rich!



Follow these steps to add test ETH to your wallet

1. Add custom network and fill it out with Sepolia Faucet info

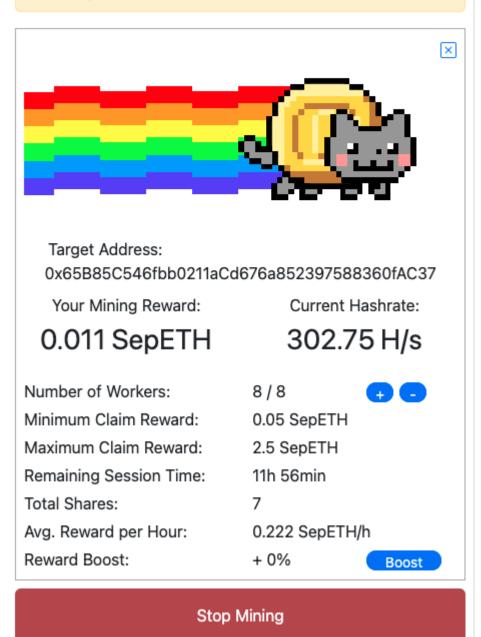


2. Get test tokens from Sepolia Test Faucet

3. Once you've put your wallet address and filled out the captcha you should start receiving

Sepolia PoW Faucet

The faucet is currently experiencing unusually high mining activity (>500 kH/s). For higher rewards, I recommend visiting again when the activity is lower.



ETH!

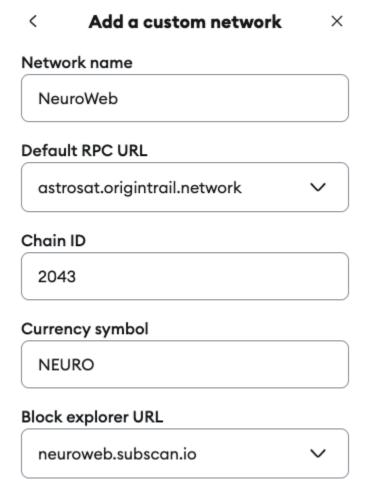
Note, you won't receive any tokens until you click "Stop Mining" and then click on "Claim Reward"!

You should now have some Sepolia in your wallet!



Adding Neuro Web Tokens is more involved, follow the steps below to get them:

1. Add a new network with the following properties



2. Then You need access to the <u>OriginTrail discord server</u>, then in #faucet-bot channel type !help command for info

- 3. In #faucet-bot channel execute the following command: !fundme_neuroweb <wallet_address>
- 4. After some time you should have tokens in your wallet

Problem Statement

- 1. Alice receives a fake bill from Bob for her utility bill, to her ADDRESS with an AMOUNT for company X
- 2. Alice believes this to be the true utility bill and she pays the money but instead of it going to company X it goes Bob, so Alice has fallen victim to FRAUD
- 3. We need to solve this problem, but instead of trying to do like a bank where we take action after the FRAUD we try to prevent it from happening
- 4. We want to solve this using blockchain but the problem is blockchain is public, so instead of storing the private data on chain we just store a hash
- 5. We generate the appropriate hash using the smart contract

Smart Contract

The smart contract is a self-executing program stored on a blockchain that automatically enforces and executes the terms of an agreement once predefined conditions are met

Properties of smart contract:

- Quality Logic-Based: It contains the business logic (like "if X happens, then do Y").
- **Trustless**: No need for a middleman the blockchain ensures everything runs as coded.
- **[Immutable**: Once deployed, it can't be altered (unless there's an upgrade mechanism built in).
- **Transparent**: Everyone can see the code and how it operates on public blockchains.

NFTs

We can thus represent the given utility bill defined in the problem statement as a Non Fungible Token (NFT). This is because we want each contract to be unique, non replicable and thus using NFTs to represent utility bills is a perfect use case for NFTs.

ERC-721

Ethereum defines NFTs using the <u>ERC-721</u> standard, this is the specific standard we'll be using in our solidity smart contracts.

ERC-721 Key Properties

The key properties of ERC-721 are summarized below

• @ Uniqueness:

Each token is distinct and has a unique tokenId. No two are the same.

• **Q** Ownership:

Tracks who owns each token using the ownerOf(tokenId) function.

• S Transferability:

Tokens can be transferred between addresses using transferFrom() or safeTransferFrom().

Metadata:

Each token can point to off-chain metadata via tokenURI(tokenId) (e.g., artwork, attributes).

Owners can approve others to manage their tokens (approve() and setApprovalForAll()).

• ***** Interoperability:

Recognized by marketplaces and dApps that support the ERC-721 standard.

You can view the full properties from <u>EIP-721</u>

Utility NFT (UNFT)

How do we use NFTs to solve the problem defined in the problem statement? Well one solution would be to provide the information required for each contract in the metadata attribute; the metadata would be stored off chain and only the unique identifier (hash) of the contract and the NFT would be stored on chain.

To solve our problem the company issuing the invoice mints an NFT, this NFT has a hash which is published on-chain. The metadata associated with the given NFT is stored off-chain, and is what contains the sensitive data associated with the bill.

How can the customer access this metadata without repeating the problem defined in the problem statement? Well there are two ways: one would be for the user to receive a code from the company for each bil via email, this code would then be used in the API to access the metadata; the second more complex solution would be to have a keypair associated with each company the customer has a bill from, then each time the company issues a bill they send the metadata encrypted and then the customer can decrypt it using their key (this avoid the need to issue codes each time a bill is issued which reduces the attack vector). We should initially do this off-chain, using the former suggested solution, (due to the time constraints of the hackathon) however as future steps we could look into implementing more secure methods such as ZKPs and meta data storage using DKG.

Suggested attributes to include in the metadata are:

- Invoice number: unique identifier for the invoice
- Invoice date: the date the invoice was issued
- Payment due date: the date the payment is expected to be made
- Seller/supplier information: name, address, and contact information
- Buyer/customer information: name, address, and contact information
- Description of goods or services: a clear and concise description of what is being sold
- Quantity: the number of items or services being invoiced
- Unity Price: the price of each individual item or service
- Subtotal: the total cost of the goods or services before any taxes or discounts
- Taxes: any applicable taxes, such as VAT
- Discounts: any applicable discounts
- Total amount due: the final amount the customer owes
- Payment terms: specify the timeframe for payment
- Accepted payment methods: methods that the seller accepts
- Company logo
- Additional information of instructions

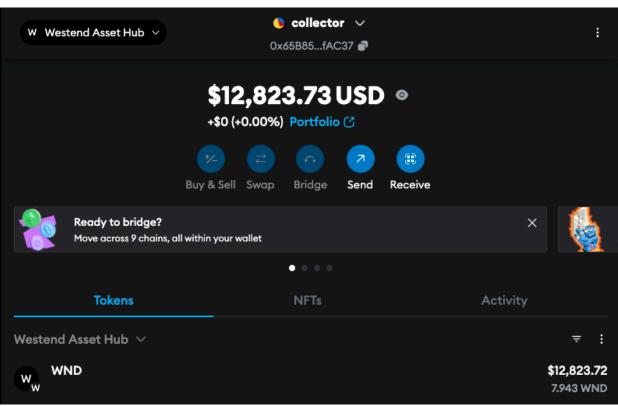
Since all of this is private sensitive data, it's important that this information is stored, retrieved and transferred in a safe, trustable and verifiable way. Using traditional web2 methods where the data is stored off-chain in private servers and queried with API is the only feasible option in the given time window, however we plan to move to more secure solutions using ZKPs and DKG in the future.

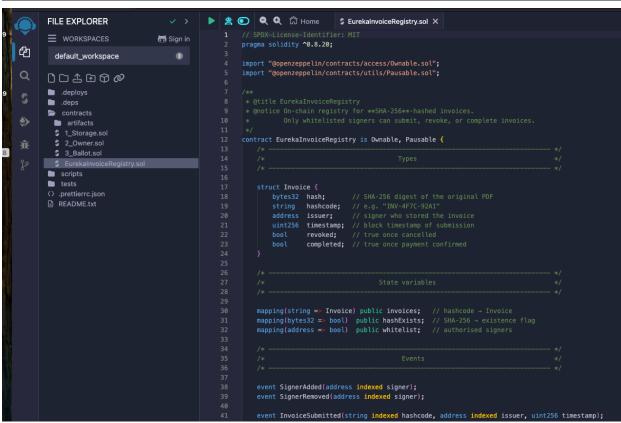
Implementation

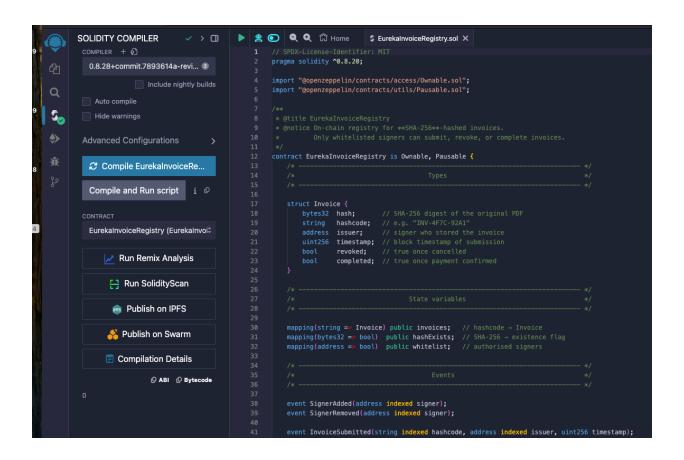
- 1. Write smart contract, we'll use solidity because of familiarity (DONE)
- 2. Deploy the contract to Westend (DONE)
- 3. Execute contract methods to publish invoice on-chain (DONE)
- Get data from blockchain using API (PENDING)
- 5. Show results from API calls to the user, so that they can see that their PDF has been verified using the blockchain (PENDING)

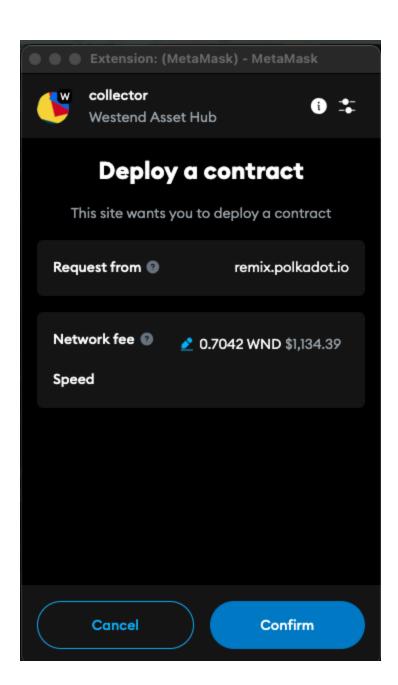
Screenshot Testing Proofs

Screen shots to keep track and provide proof of testing!



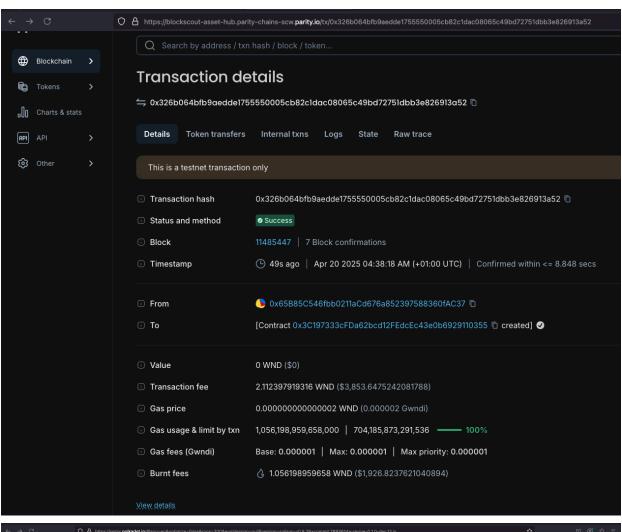


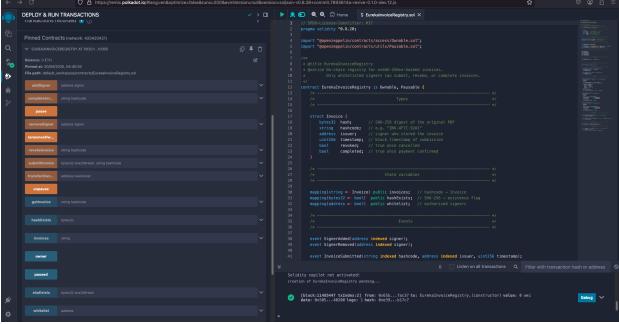






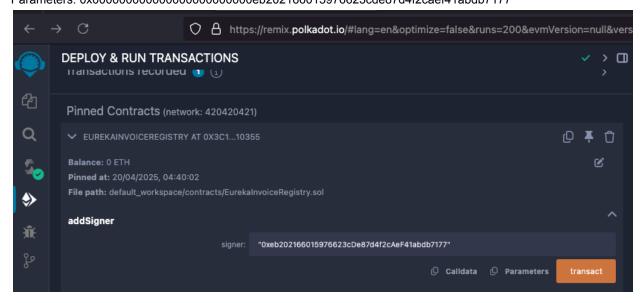
Contract deployment × View on block explorer Status Confirmed Copy transaction ID From То 0x65B85...fA... (→ New contract Transaction Nonce 10 Amount -0 WND Gas Limit (Units) 704185873291536 Gas Used (Units) 1056198959658000 Base fee (GWEI) 0.000001 Priority fee (GWEI) 0.000001 Total gas fee 2.112398 WND \$3,402.90 USD Max fee per gas <0.000001 WND \$0.00 USD Total 2.11239792 WND \$3,402.90 USD + Activity log

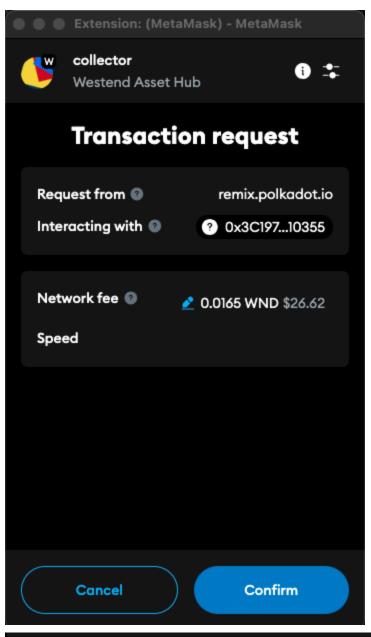




Testing contract methods

addSigner

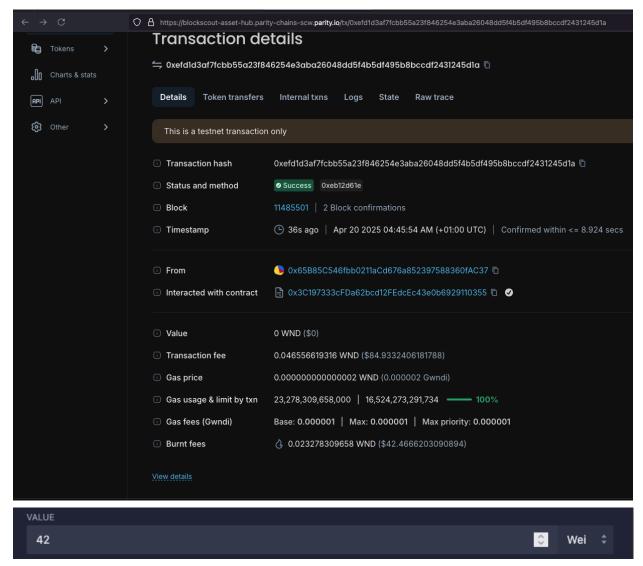






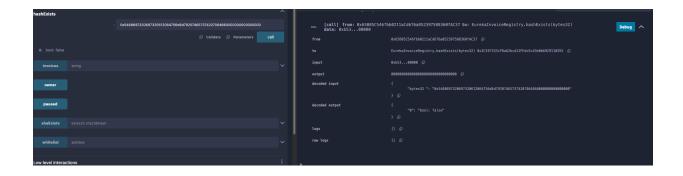
Add Signer × View on block explorer Status Confirmed Copy transaction ID From То 0x65B85...fA... ? 0x3C197..... **Transaction** Nonce -0 WND Amount Gas Limit (Units) 16524273291734 Gas Used (Units) 23278309658000 Base fee (GWEI) 0.000001 Priority fee (GWEI) 0.000001 Total gas fee 0.046557 WND \$74.96 USD Max fee per gas <0.000001 WND \$0.00 USD 0.04655662 WND Total \$74.96 USD

+ Activity log



Need fill value out, cannot be zero for function calls that require gas fees

hashExists



getInvoice

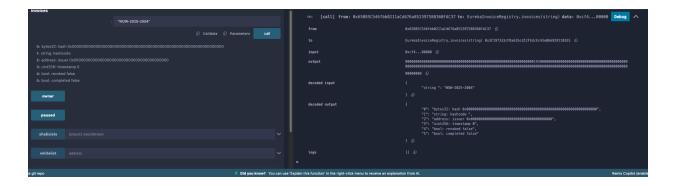
Calldata:

Parameters:



Invoices

This function just fetches the invoice given the string, and we passed the same call data as above, (non-sense data) so we get back empty invoice since no invoice with given hashcode exists



addSigner

calldata:0xeb12d61e00000000000000000000000005b85c546fbb0211acd676a852397588360fa c37

Parameters: 0x00000000000000000000000005b85c546fbb0211acd676a852397588360fac37

submitInvoice

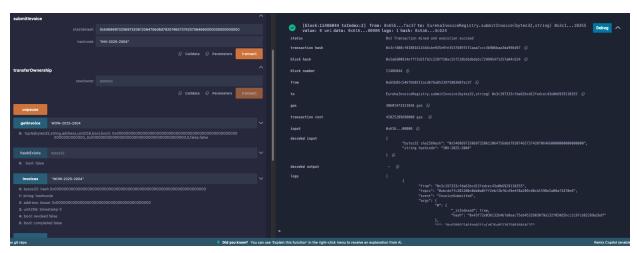
This is the important function, before we had no invoices, however a lot of things can go wrong here!

Be careful, not quoting the string will give error encoding arguments, also using a non zero value or not selecting an estimated gas fee with limit 3000000 will give the infamous rpc gas error message!

This function has to have valid sha256 and also hashcode quoted otherwise again infamous rpc gas error message.

Calldata:

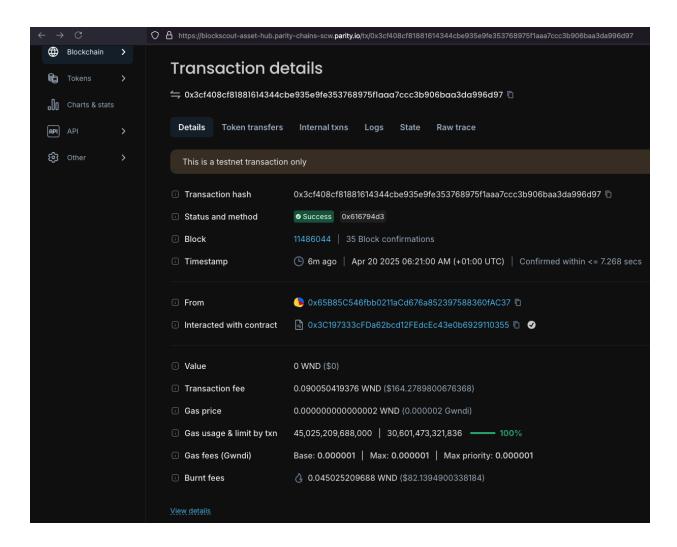
Parameters:



Now the contract is on the blockchain!



Contract interaction × View on block explorer Status Confirmed Copy transaction ID From То 0x65B85...fA... (→) ? 0x3C197..... **Transaction** Nonce Amount -0 WND Gas Limit (Units) 30601473321836 Gas Used (Units) 45025209688000 Base fee (GWEI) 0.000001 Priority fee (GWEI) 0.000001 Total gas fee 0.09005 WND \$145.46 USD Max fee per gas <0.000001 WND \$0.00 USD 0.09005042 WND Total \$145.46 USD + Activity log



Creating more invoices





Transaction request

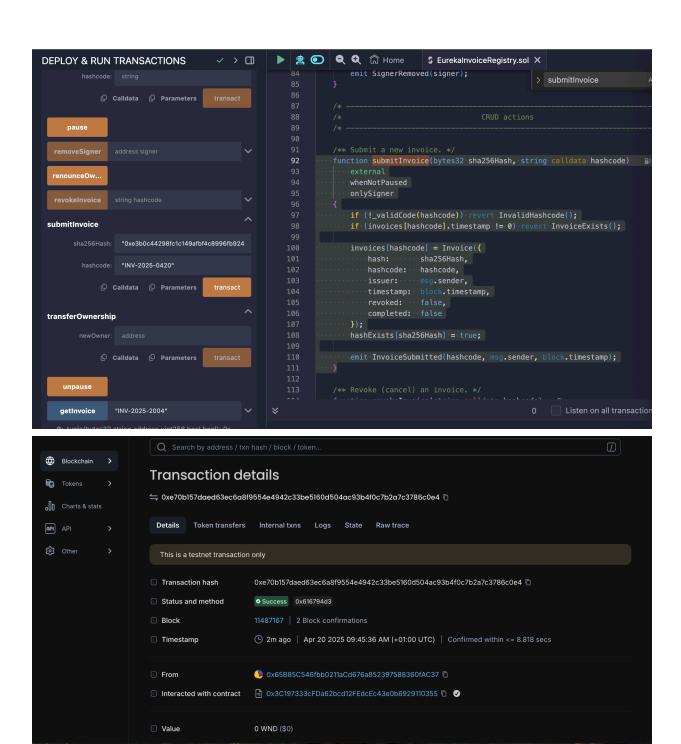
Request from (2) remix.polkadot.io

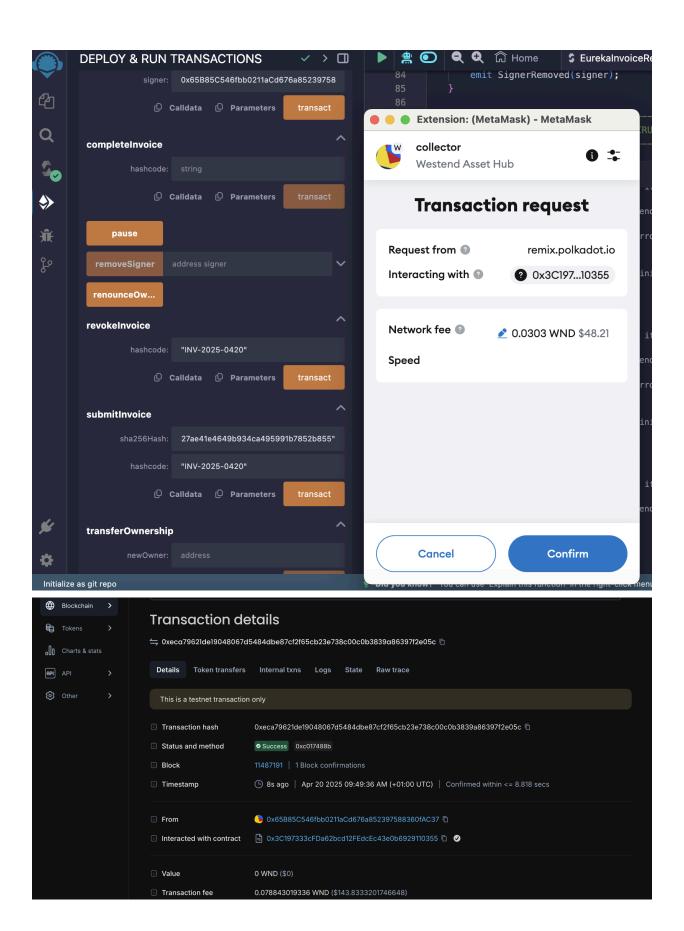
Interacting with (2) 0x3C197...10355

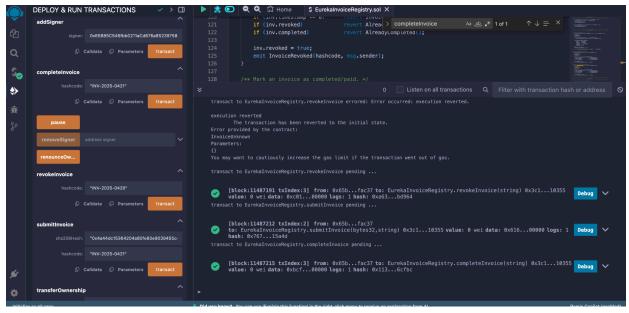
Network fee

№ 0.0306 WND \$48.72

Speed







Full invoices in json format

```
PENDING to verify invoice
export const exampleInvoice: Invoice = {
 hash: "0x5468697320697320612064756d6d7920746573742070646600000000000000000",
 hashcode: "INV-2025-2004",
 issuer: "0x65B85C546fbb0211aCd676a852397588360fAC37",
 timestamp: 1745126460,
 revoked: false,
 completed: false
};
REVOKED invoice
{
       "0": "bytes32: hash
0xe3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
      "1": "string: hashcode INV-2025-0420",
      "2": "address: issuer 0x65B85C546fbb0211aCd676a852397588360fAC37",
      "3": "uint256: timestamp 1745138832",
      "4": "bool: revoked true",
      "5": "bool: completed false"
}
COMPLETED invoice
       "0": "bytes32: hash
0x4a44dc15364204a80fe80e9039455cc1608281820fe596e5a4f6f15b6a36d475",
```

```
"1": "string: hashcode INV-2025-0421",

"2": "address: issuer 0x65B85C546fbb0211aCd676a852397588360fAC37",

"3": "uint256: timestamp 1745139192",

"4": "bool: revoked false",

"5": "bool: completed true"
}
```

Useful Resources Links

Useful website to check chain details: https://chainlist.org/

Reference docs for contracts on Polkadot:

https://contracts.polkadot.io

Useful website for smart contracts:

https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html

Deploy solidity contracts in browser using remix:

https://remix.polkadot.io/

Deploying smart contracts using hardhat:

https://hardhat.org/hardhat-runner/docs/getting-started#overview