Ethereum DAPPS

How to create an Ethereum Dapp

Sheets
https://web3examples.com/Saxion

Intro Gerard Persoon

- Education
  - Computer science (TU Delft), IT Audit (VU), Startup Validation Lab (Yes!Delft)
- Roles
  - Software developer
  - Line manager & Technical project manager
  - IT Auditor
- Teaching
  - The hague university of applied science (programming blockchains)
  - HES Amsterdam
  - Tilburg University
- Companies
  - Enovation, Ernst & Young, IBM, ABN AMRO, DB Schenker, HMC
- Contact
  - mail@gpersoon.com
  - https://www.linkedin.com/in/gpersoon
  - Twitter: @gpersoon

Content

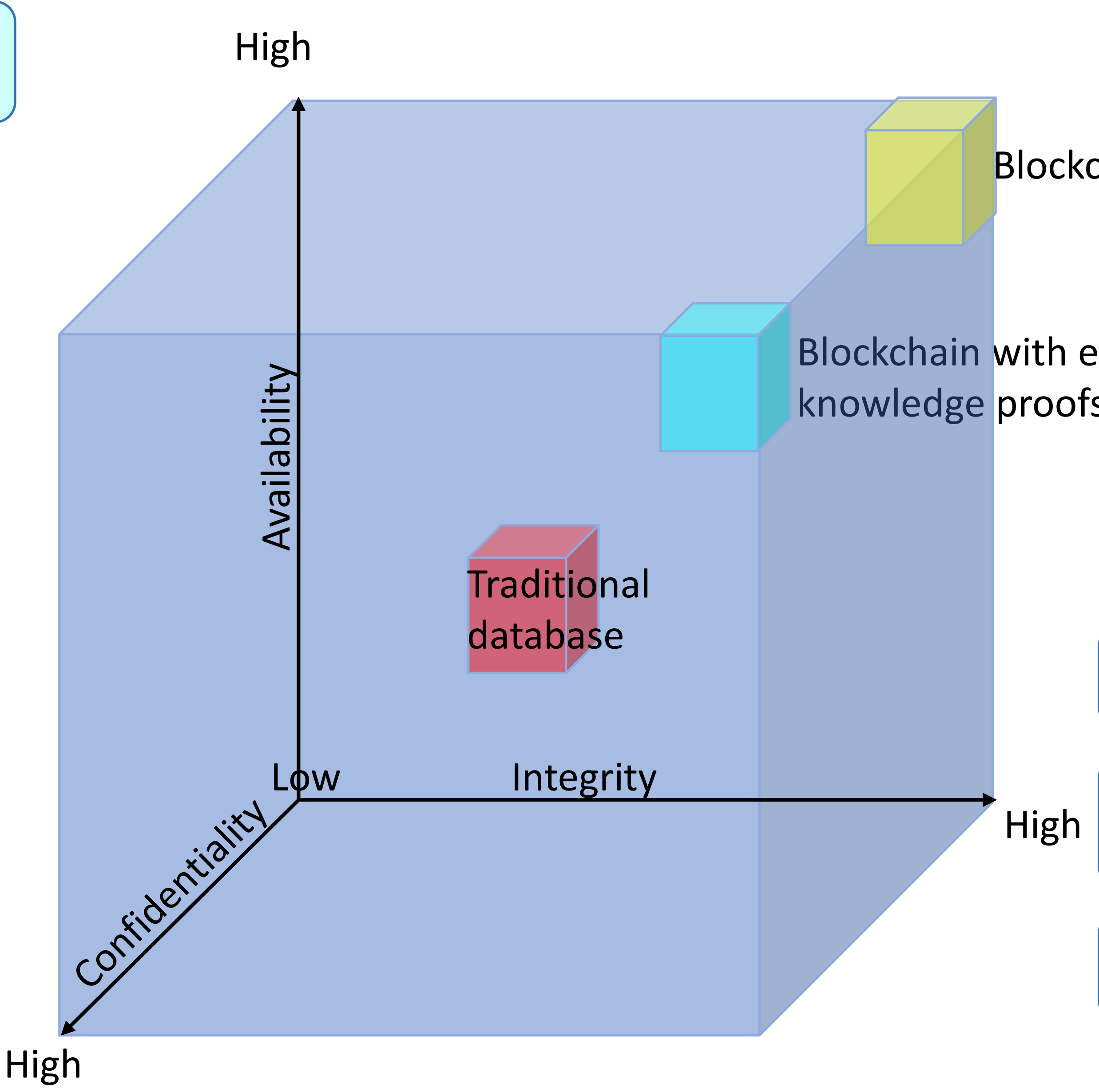
1. Short introduction of what Ethereum is
2. How to get started with the Ethereum SDK
3. Write a basic smart contract

What is Ethereum?

- Global database
- Openly accessible
- Pay for use
- Allows for transfer of value
- Most used programmable blockchain

Characteristics of blockchains

Very distributed database
Availability: high



Perfect audit trail of writes
No audit trail for reads

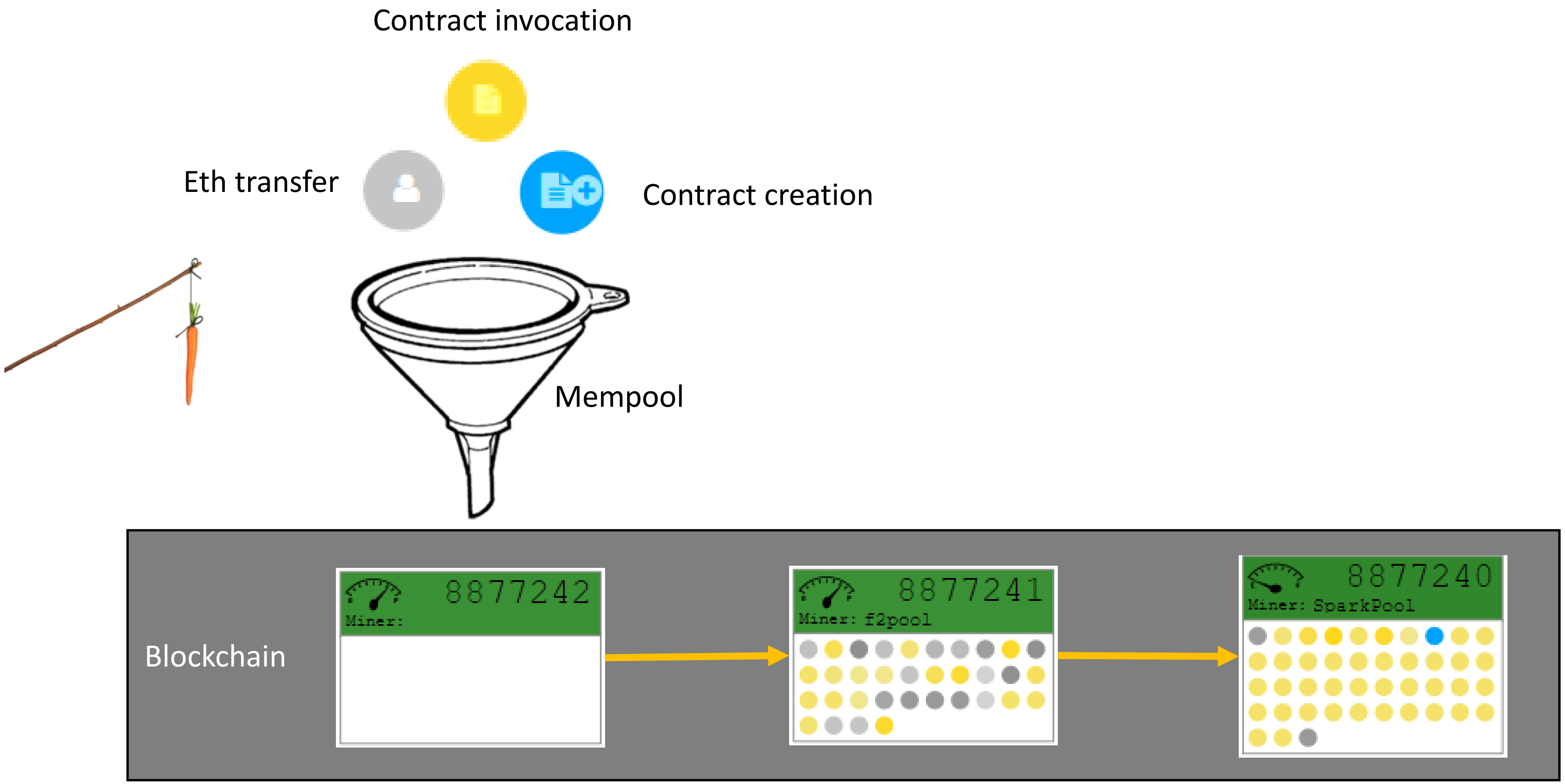
No-one can change (previous) state)
Integrity: high

Fix bugs by redeploying code

Anyone can read (everything)
Confidentiality : low

Modules are re-used (also in unexpected ways)

Second generation blockchain



Contract invocation

Eth transfer

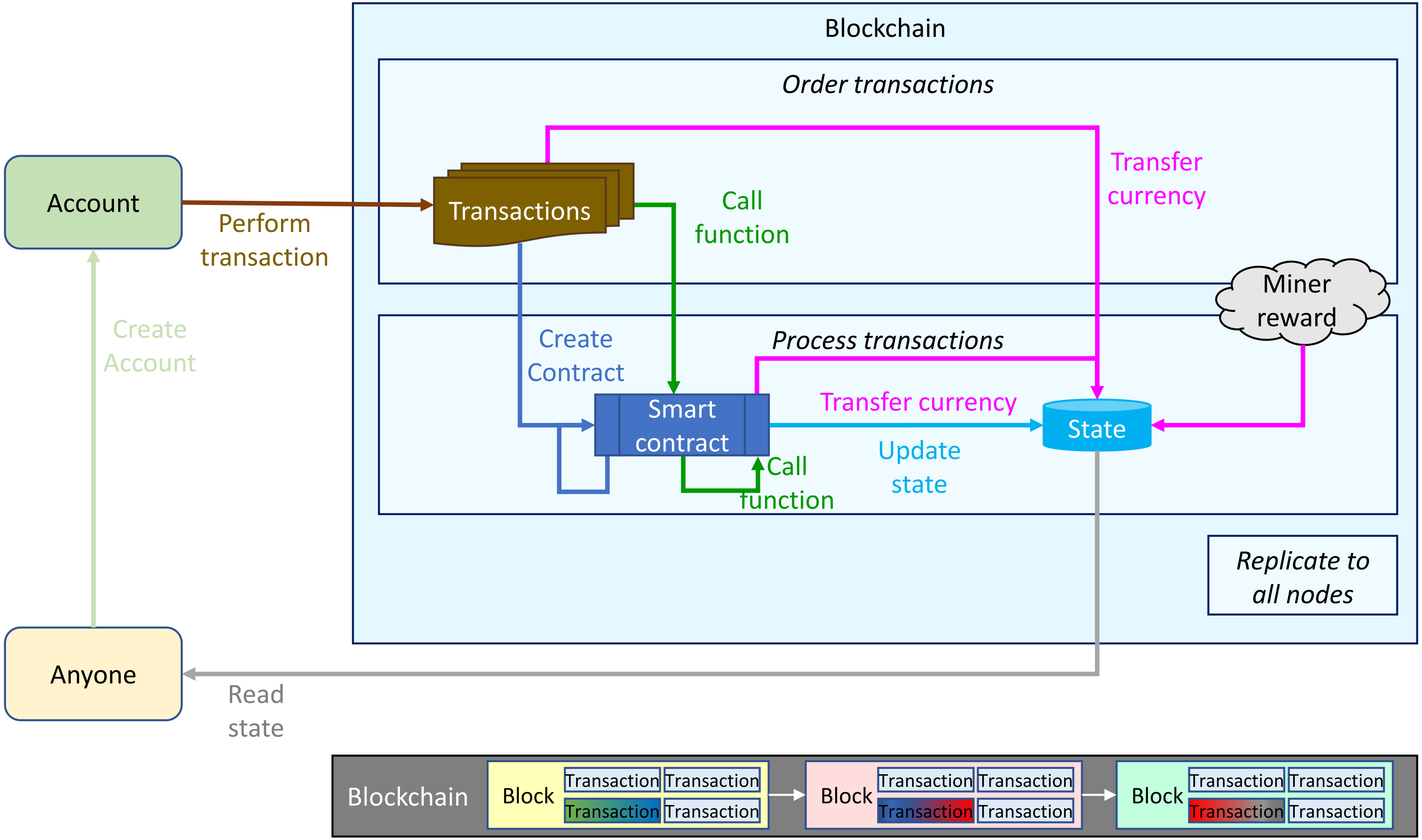
Contract creation

Mempool

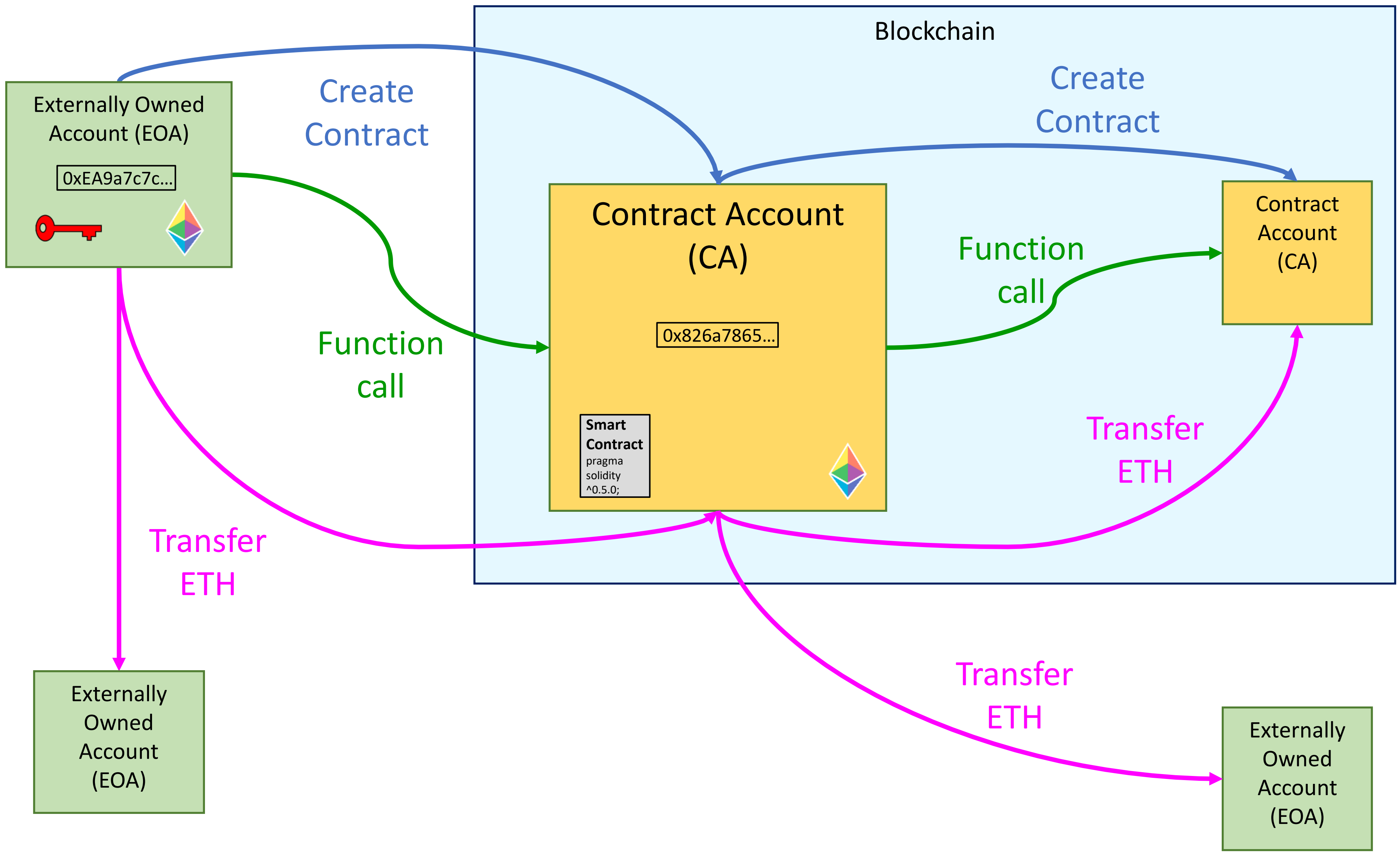
Blockchain

http://ethviewer.live/

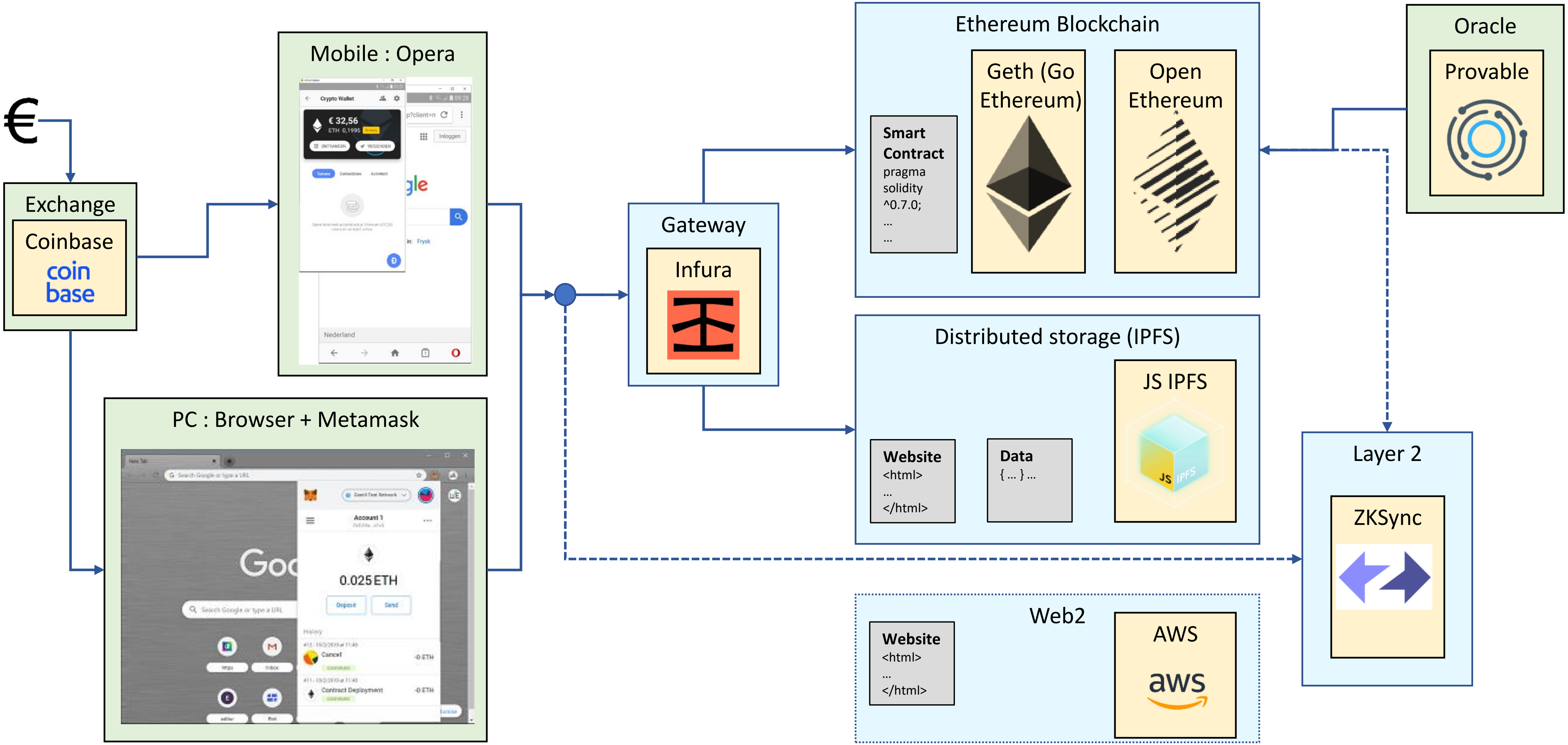
Architecture 2nd generation



Interactions between addresses



DAPP architecture



€

Exchange

Coinbase

coin base

Mobile : Opera

PC : Browser + Metamask

Gateway

Infura

Ethereum Blockchain

Smart Contract
pragma solidity ^0.7.0;
…
…

Geth (Go Ethereum)

Open Ethereum

Distributed storage (IPFS)

Website
<html>
…
</html>

Data
{ … } …

JS IPFS

Web2

Website
<html>
…
</html>

AWS

aws

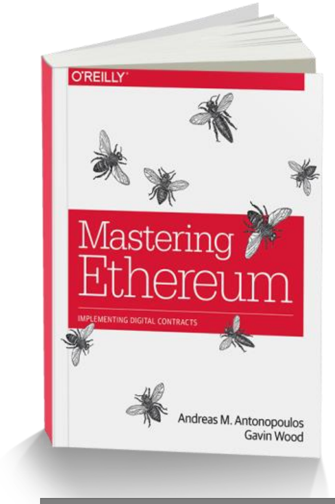
Oracle

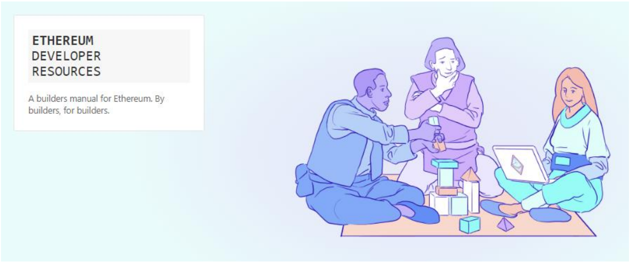
Provable

Layer 2

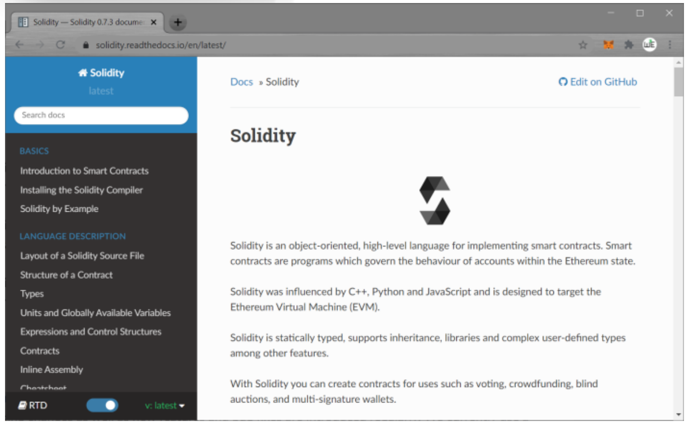
ZKSync

2. How to get started with the Ethereum SDK




ETHEREUM DEVELOPER RESOURCES

A builders manual for Ethereum. By builders, for builders.


Solidity — Solidity 0.7.3 docume
solidity.readthedocs.io/en/latest/
Solidity
latest
Search docs
BASICS
Introduction to Smart Contracts
Installing the Solidity Compiler
Solidity by Example
LANGUAGE DESCRIPTION
Layout of a Solidity Source File
Structure of a Contract
Types
Units and Globally Available Variables
Expressions and Control Structures
Contracts
Inline Assembly
Cheatsheet
RTD
v: latest
Docs » Solidity
Edit on GitHub

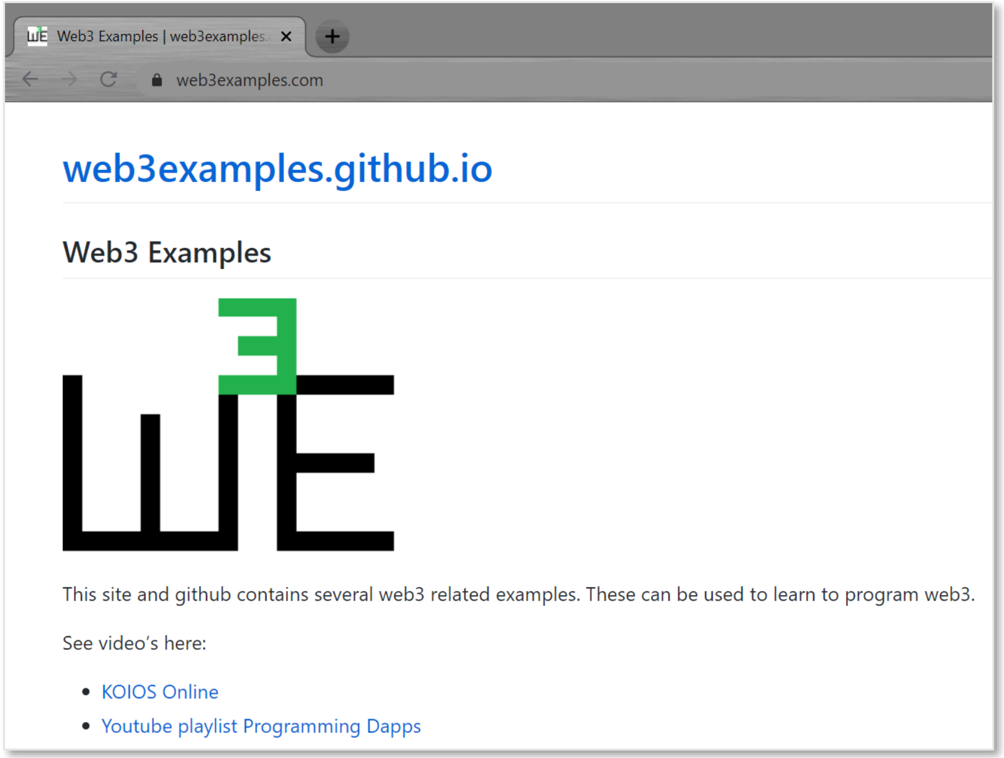
Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state.

Solidity was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM).

Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.



web3examples.github.io

Web3 Examples

This site and github contains several web3 related examples. These can be used to learn to program web3.

See video's here:

- KOIOS Online
- Youtube playlist Programming Dapps

https://web3examples.com

https://ethereumbook.info

https://cryptozombies.io/en/lesson/1/chapter/1

https://solidity.readthedocs.io/en/latest

https://ethereum.org/en/developers

https://docs.ethhub.io

https://consensys.net/developers

Install Metamask

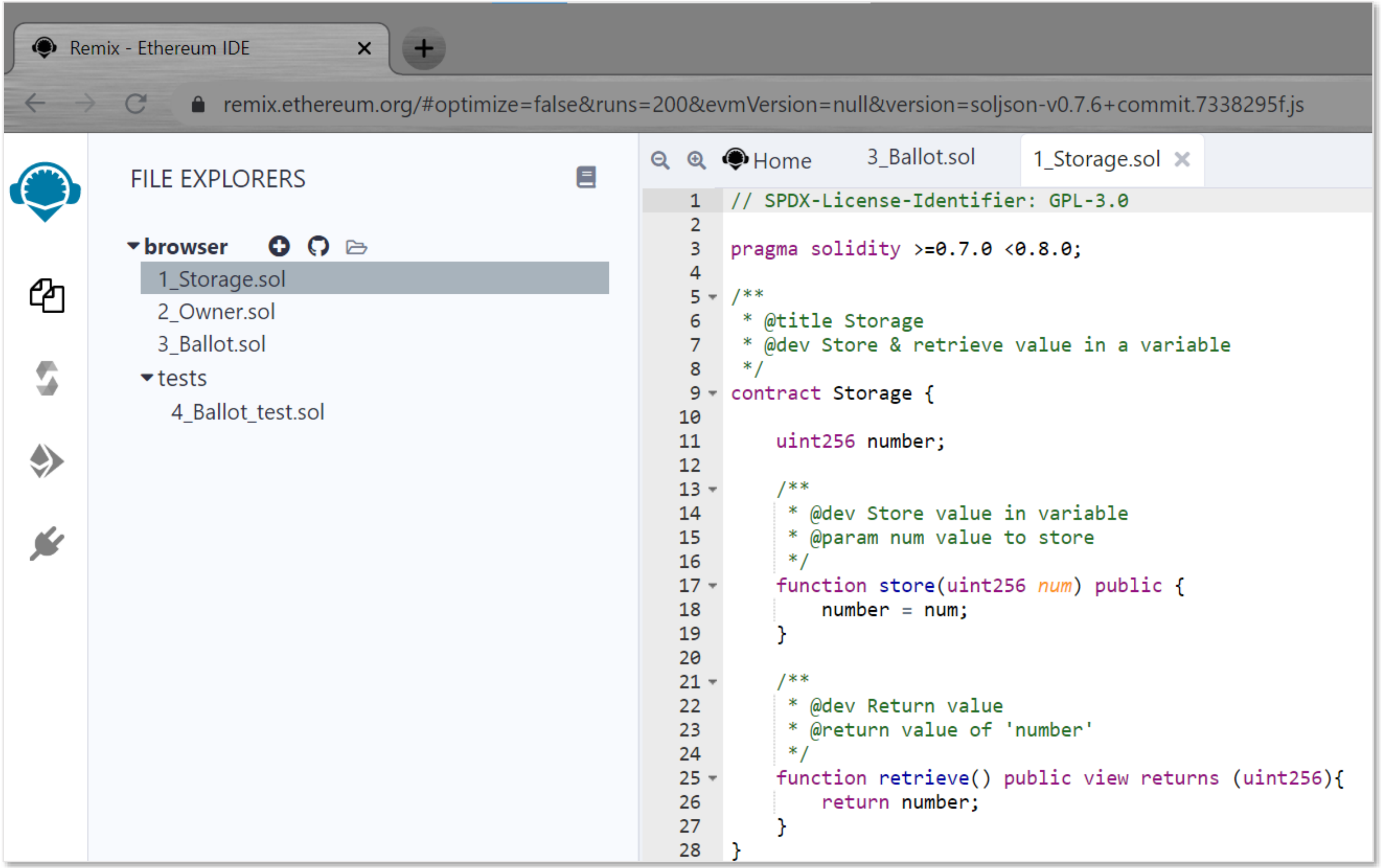
Location	Action	Object
https://www.google.com – Search bar	Enter	metamask
https://www.google.com/search?q=metamask	Click	MetaMask
https://metamask.io	Click	get chrome extension
https://chrome.google.com/webstore/...	Click	Add to Chrome
Popup Add “MetaMask”?	Click	Add extension
chrome-extension://nkbi../home.html#initialize/welcome	Click	Get Started
chrome-extension://nkbi…/home.html#initialize/select-action	Click	Create a wallet
chrome-extension://nkbi…/home.html#initialize/metametrics-opt-in	Click	I agree
Start menu	Start	{password manager}
Password manager	Do	Create random password
Password manager	Copy	Password
chrome-extension:… field: New password	Paste	{password}
chrome-extension:… field: Confirm password	Paste	{password}
chrome-extension:… checkbox: I have read …	Click	{checkbox}
chrome-extension://nkbi…/home.html#initialize/seed-phrase	Click	Click here to reveal…
{ paper}	Write	{seed phrase}
	Click	Next
chrome-extension://nkbi…/home.html#initialize/seed-phrase/confirm	Click	{ All the words}
	Click	Confirm
chrome-extension://nkbi…/home.html#initialize/end-of-flow	Click	All Done
chrome-extension://nkbi…/home.html#	Close	{windows}

https://www.youtube.com/watch?v=Wc-Hgn1QUjA

https://metamask.io/

http://web3examples.com/ethereum/install/Install_MetaMask_Windows.html

PD-3.1 Remix IDE - online

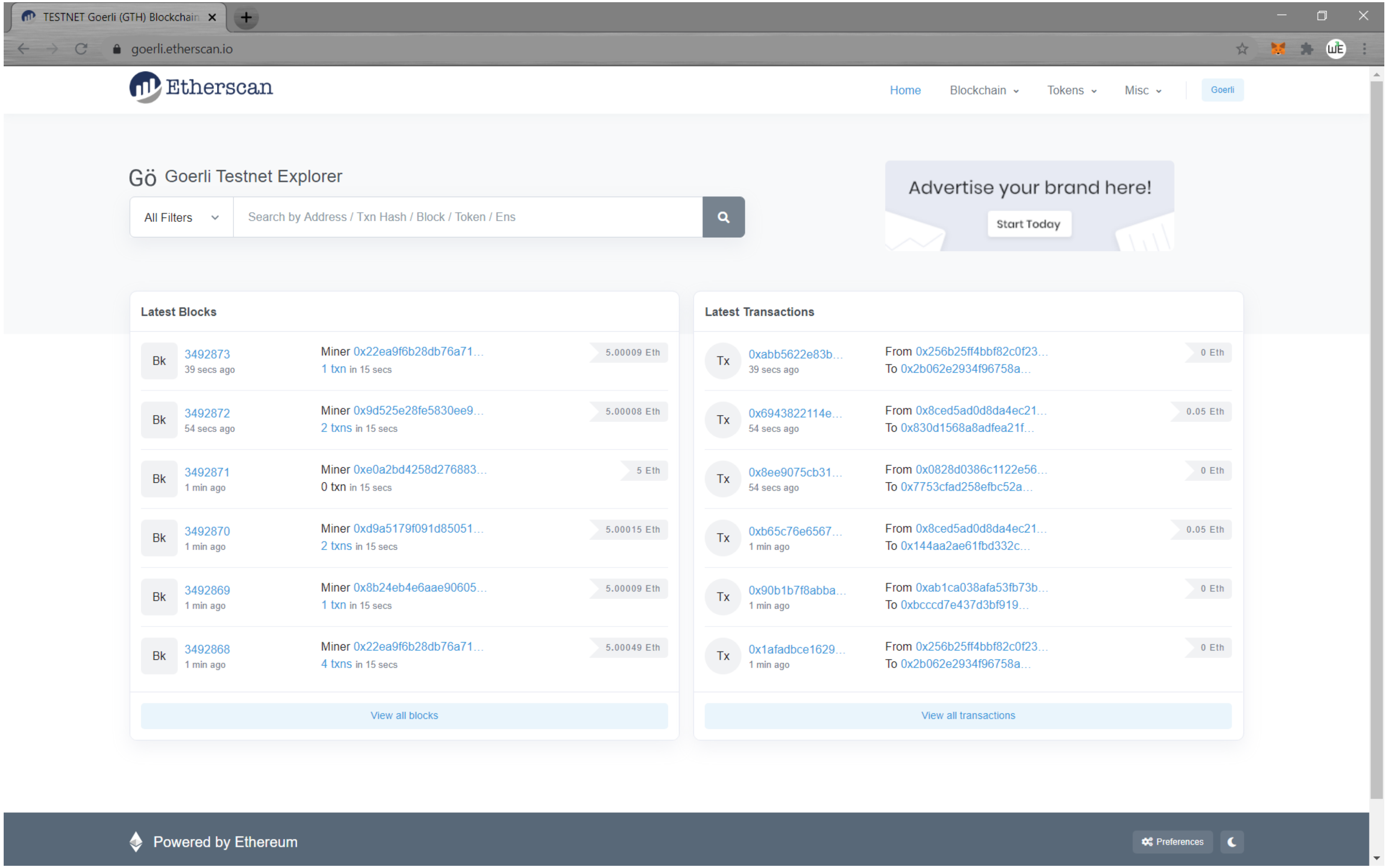


```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.8.0;

/**
 * @title Storage
 * @dev Store & retrieve value in a variable
 */
contract Storage {

    uint256 number;

    /**
     * @dev Store value in variable
     * @param num value to store
     */
    function store(uint256 num) public {
        number = num;
    }

    /**
     * @dev Return value
     * @return value of 'number'
     */
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

https://remix.ethereum.org/

https://remix-ide.readthedocs.io/en/latest/

PD-2.3.4 Etherscan



Gö Goerli Testnet Explorer

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Latest Blocks

Bk	3492873 39 secs ago	Miner 0x22ea9f6b28db76a71... 1 txn in 15 secs	5.00009 Eth
Bk	3492872 54 secs ago	Miner 0x9d525e28fe5830ee9... 2 txns in 15 secs	5.00008 Eth
Bk	3492871 1 min ago	Miner 0xe0a2bd4258d276883... 0 txn in 15 secs	5 Eth
Bk	3492870 1 min ago	Miner 0xd9a5179f091d85051... 2 txns in 15 secs	5.00015 Eth
Bk	3492869 1 min ago	Miner 0x8b24eb4e6aae90605... 1 txn in 15 secs	5.00009 Eth
Bk	3492868 1 min ago	Miner 0x22ea9f6b28db76a71... 4 txns in 15 secs	5.00049 Eth

View all blocks

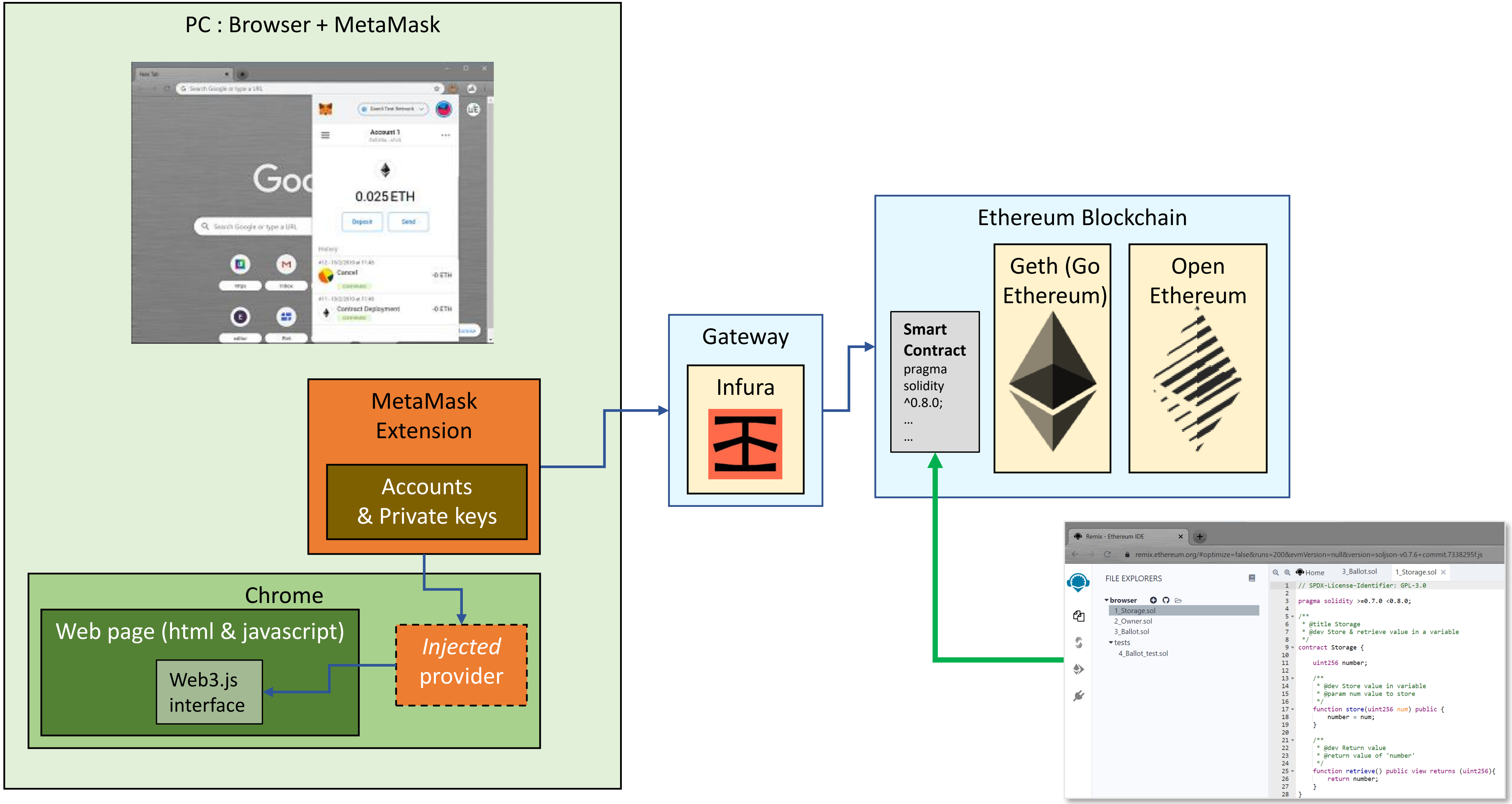
Latest Transactions

Tx	0xabb5622e83b... 39 secs ago	From 0x256b25ff4bbf82c0f23... To 0x2b062e2934f96758a...	0 Eth
Tx	0x6943822114e... 54 secs ago	From 0x8ced5ad0d8da4ec21... To 0x830d1568a8adfea21f...	0.05 Eth
Tx	0x8ee9075cb31... 54 secs ago	From 0x0828d0386c1122e56... To 0x7753cfad258efbc52a...	0 Eth
Tx	0xb65c76e6567... 1 min ago	From 0x8ced5ad0d8da4ec21... To 0x144aa2ae61fbd332c...	0.05 Eth
Tx	0x90b1b7f8abba... 1 min ago	From 0xab1ca038afa53fb73b... To 0xbcccd7e437d3bf919...	0 Eth
Tx	0x1afadbce1629... 1 min ago	From 0x256b25ff4bbf82c0f23... To 0x2b062e2934f96758a...	0 Eth

View all transactions

https://goerli.etherscan.io

DAPP architecture

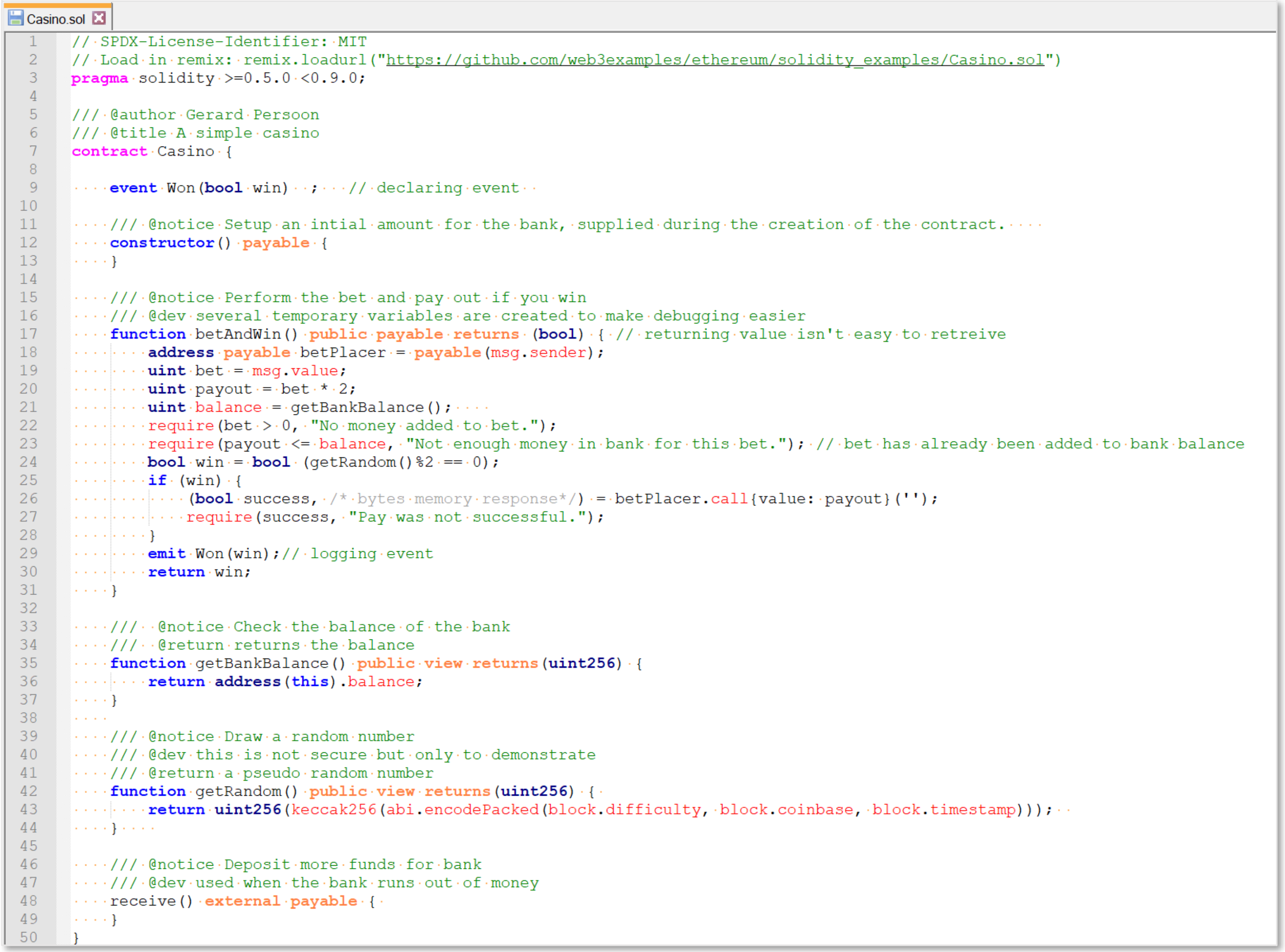


remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.7.6+commit.7338295f.js

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.8.0;

/**
 * @title Storage
 * @dev Store & retrieve value in a variable
 */
contract Storage {

    uint256 number;

    /**
     * @dev Store value in variable
     * @param num value to store
     */
    function store(uint256 num) public {
        number = num;
    }

    /**
     * @dev Return value
     * @return value of 'number'
     */
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

3. Write a basic smart contract

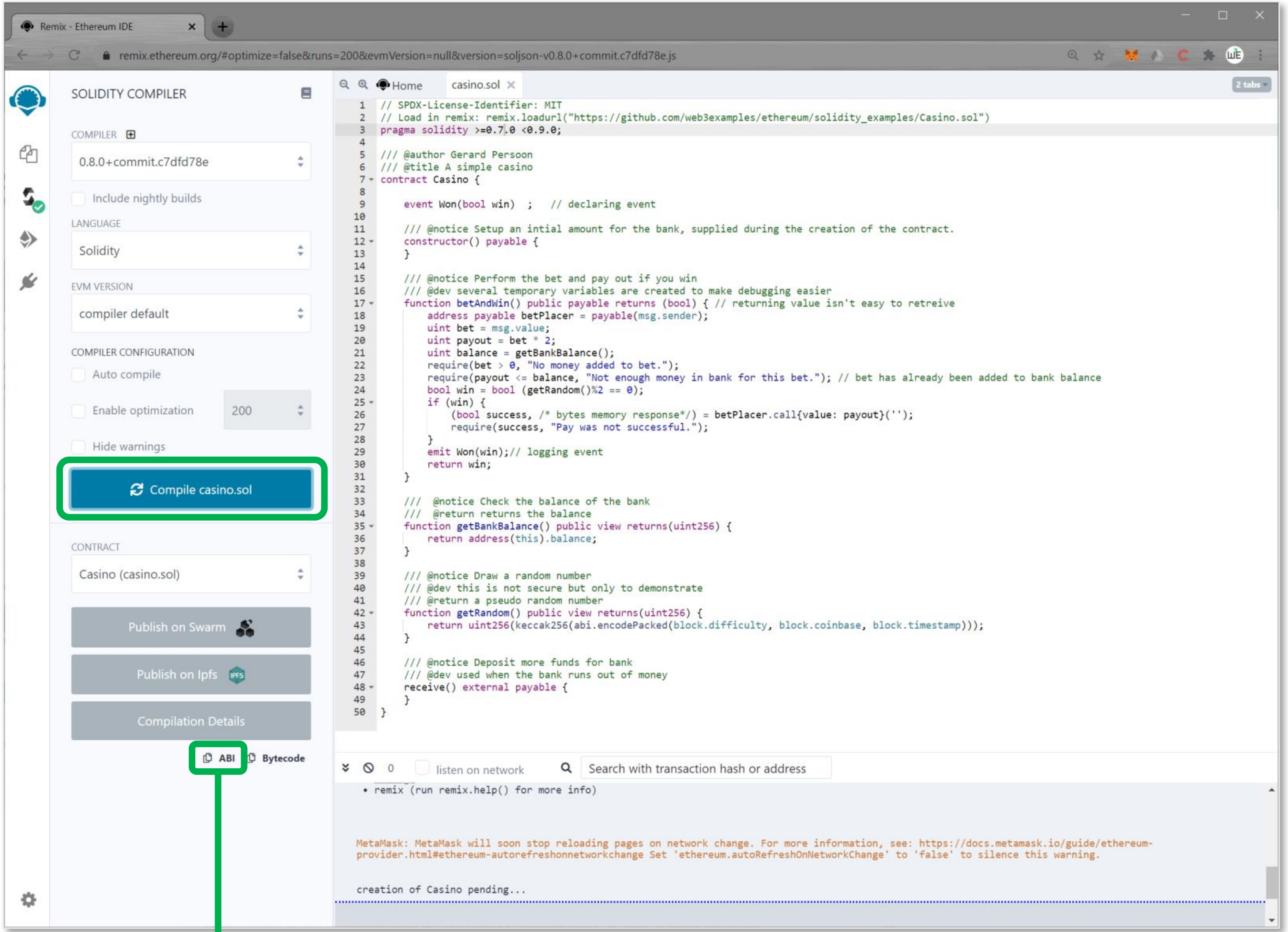
Casino Solidity



```solidity
// SPDX-License-Identifier: MIT
// Load in remix: remix.loadurl("https://github.com/web3examples/ethereum/solidity_examples/Casino.sol")
pragma solidity >=0.5.0 <0.9.0;

/// @author Gerard Persoon
/// @title A simple casino
contract Casino {

    event Won(bool win)  ;   // declaring event  

    /// @notice Setup an intial amount for the bank, supplied during the creation of the contract.    
    constructor() payable {
    }

    /// @notice Perform the bet and pay out if you win
    /// @dev several temporary variables are created to make debugging easier
    function betAndWin() public payable returns (bool) { // returning value isn't easy to retreive
        address payable betPlacer = payable(msg.sender);
        uint bet = msg.value;
        uint payout = bet * 2;
        uint balance = getBankBalance();    
        require(bet > 0, "No money added to bet.");
        require(payout <= balance, "Not enough money in bank for this bet."); // bet has already been added to bank balance
        bool win = bool (getRandom()%2 == 0);
        if (win) {
            (bool success, /* bytes memory response*/) = betPlacer.call{value: payout}('');
            require(success, "Pay was not successful.");
        }
        emit Won(win);// logging event
        return win;
    }

    ///  @notice Check the balance of the bank
    ///  @return returns the balance
    function getBankBalance() public view returns(uint256) {
        return address(this).balance;
    }
    
    /// @notice Draw a random number
    /// @dev this is not secure but only to demonstrate
    /// @return a pseudo random number
    function getRandom() public view returns(uint256) { 
        return uint256(keccak256(abi.encodePacked(block.difficulty, block.coinbase, block.timestamp)));  
    }    

    /// @notice Deposit more funds for bank
    /// @dev used when the bank runs out of money
    receive() external payable { 
    }
}
```

https://github.com/web3examples/ethereum/blob/master/solidity_examples/Casino.sol

Compile via Remix


Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js
Home
casino.sol
2 tabs
Compile casino.sol
Publish on Swarm
Publish on Ipfs
Compilation Details
ABI
Bytecode
listen on network
Search with transaction hash or address

SOLIDITY COMPILER

COMPILER: 0.8.0+commit.c7dfd78e

□ Include nightly builds

LANGUAGE: Solidity

EVM VERSION: compiler default

COMPILER CONFIGURATION

□ Auto compile

□ Enable optimization 200

□ Hide warnings

CONTRACT: Casino (casino.sol)

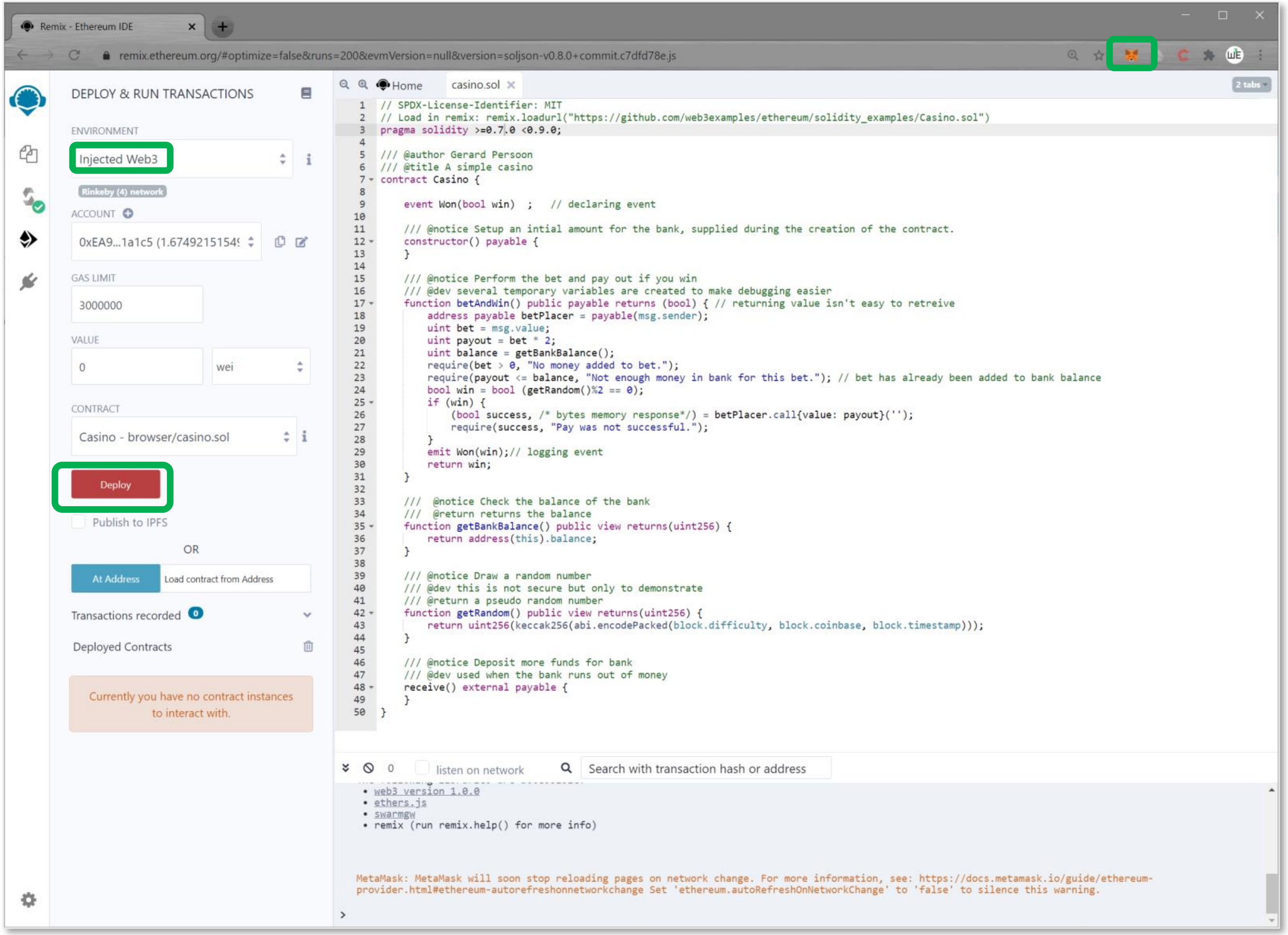
```
// SPDX-License-Identifier: MIT
// Load in remix: remix.loadurl("https://github.com/web3examples/ethereum/solidity_examples/Casino.sol")
pragma solidity >=0.7.0 <0.9.0;

/// @author Gerard Persoon
/// @title A simple casino
contract Casino {

    event Won(bool win)  ;   // declaring event

    /// @notice Setup an intial amount for the bank, supplied during the creation of the contract.
    constructor() payable {
    }

    /// @notice Perform the bet and pay out if you win
    /// @dev several temporary variables are created to make debugging easier
    function betAndWin() public payable returns (bool) { // returning value isn't easy to retreive
        address payable betPlacer = payable(msg.sender);
        uint bet = msg.value;
        uint payout = bet * 2;
        uint balance = getBankBalance();
        require(bet > 0, "No money added to bet.");
        require(payout <= balance, "Not enough money in bank for this bet."); // bet has already been added to bank balance
        bool win = bool (getRandom()%2 == 0);
        if (win) {
            (bool success, /* bytes memory response*/) = betPlacer.call{value: payout}('');
            require(success, "Pay was not successful.");
        }
        emit Won(win);// logging event
        return win;
    }

    ///  @notice Check the balance of the bank
    ///  @return returns the balance
    function getBankBalance() public view returns(uint256) {
        return address(this).balance;
    }

    /// @notice Draw a random number
    /// @dev this is not secure but only to demonstrate
    /// @return a pseudo random number
    function getRandom() public view returns(uint256) {
        return uint256(keccak256(abi.encodePacked(block.difficulty, block.coinbase, block.timestamp)));
    }

    /// @notice Deposit more funds for bank
    /// @dev used when the bank runs out of money
    receive() external payable {
    }
}
```

```
• remix (run remix.help() for more info)

MetaMask: MetaMask will soon stop reloading pages on network change. For more information, see: https://docs.metamask.io/guide/ethereum-
provider.html#ethereum-autorefreshonnetworkchange Set 'ethereum.autoRefreshOnNetworkChange' to 'false' to silence this warning.

creation of Casino pending...
```

```
[
…
   {
      "inputs": [],
      "name": "betAndWin",
      "outputs": [
         {
            "internalType": "bool",
            "name": "",
            "type": "bool"
         }
      ],
      "stateMutability": "payable",
      "type": "function"
   },
…
]
```

https://remix.ethereum.org

Deploy via Remix



Remix - Ethereum IDE
remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js
Home
casino.sol
2 tabs
DEPLOY & RUN TRANSACTIONS
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 0
Deployed Contracts
listen on network
Search with transaction hash or address

ENVIRONMENT: Injected Web3

Rinkeby (4) network

ACCOUNT: 0xEA9...1a1c5 (1.67492151545

GAS LIMIT: 3000000

VALUE: 0 wei

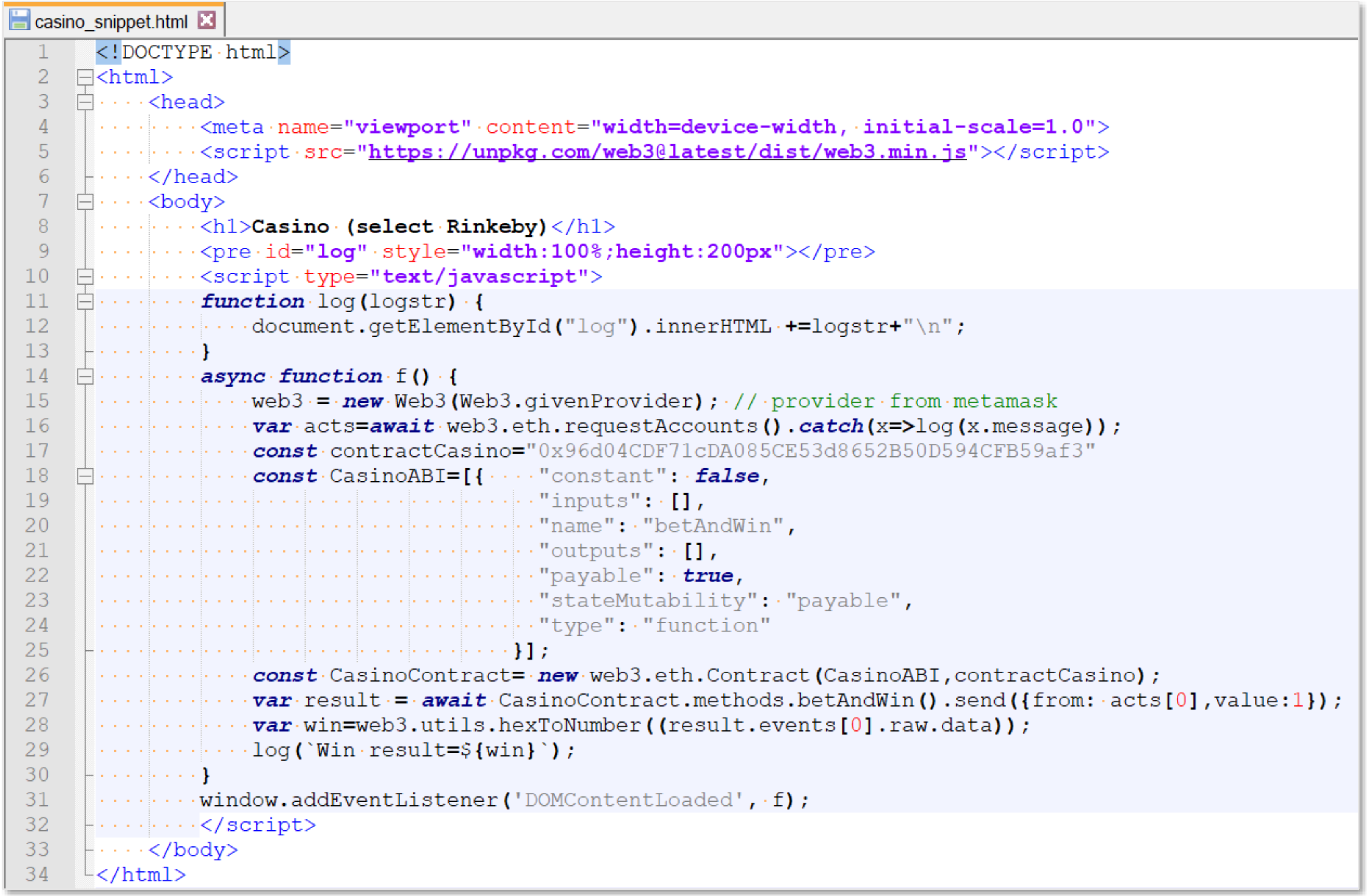
CONTRACT: Casino - browser/casino.sol

Currently you have no contract instances to interact with.

```
// SPDX-License-Identifier: MIT
// Load in remix: remix.loadurl("https://github.com/web3examples/ethereum/solidity_examples/Casino.sol")
pragma solidity >=0.7.0 <0.9.0;

/// @author Gerard Persoon
/// @title A simple casino
contract Casino {

    event Won(bool win)  ;   // declaring event

    /// @notice Setup an intial amount for the bank, supplied during the creation of the contract.
    constructor() payable {
    }

    /// @notice Perform the bet and pay out if you win
    /// @dev several temporary variables are created to make debugging easier
    function betAndWin() public payable returns (bool) { // returning value isn't easy to retreive
        address payable betPlacer = payable(msg.sender);
        uint bet = msg.value;
        uint payout = bet * 2;
        uint balance = getBankBalance();
        require(bet > 0, "No money added to bet.");
        require(payout <= balance, "Not enough money in bank for this bet."); // bet has already been added to bank balance
        bool win = bool (getRandom()%2 == 0);
        if (win) {
            (bool success, /* bytes memory response*/) = betPlacer.call{value: payout}('');
            require(success, "Pay was not successful.");
        }
        emit Won(win);// logging event
        return win;
    }

    ///  @notice Check the balance of the bank
    ///  @return returns the balance
    function getBankBalance() public view returns(uint256) {
        return address(this).balance;
    }

    /// @notice Draw a random number
    /// @dev this is not secure but only to demonstrate
    /// @return a pseudo random number
    function getRandom() public view returns(uint256) {
        return uint256(keccak256(abi.encodePacked(block.difficulty, block.coinbase, block.timestamp)));
    }

    /// @notice Deposit more funds for bank
    /// @dev used when the bank runs out of money
    receive() external payable {
    }
}
```

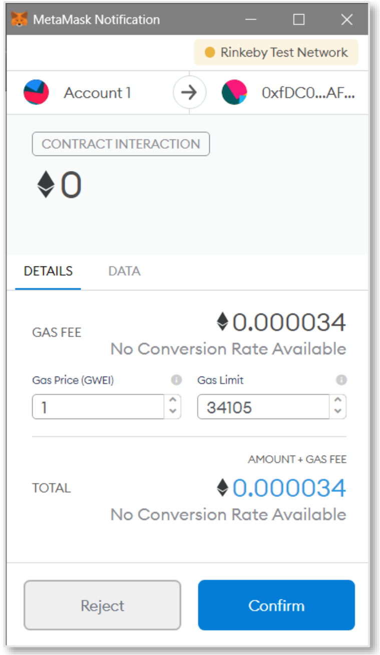
```
 • web3 version 1.0.0
 • ethers.js
 • swarmgw
 • remix (run remix.help() for more info)

MetaMask: MetaMask will soon stop reloading pages on network change. For more information, see: https://docs.metamask.io/guide/ethereum-
provider.html#ethereum-autorefreshonnetworkchange Set 'ethereum.autoRefreshOnNetworkChange' to 'false' to silence this warning.

>
```

Casino – snippet (Rinkeby)



casino_snippet.html

```
<!DOCTYPE html>
<html>
    <head>
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <script src="https://unpkg.com/web3@latest/dist/web3.min.js"></script>
    </head>
    <body>
        <h1>Casino (select Rinkeby)</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() {
            web3 = new Web3(Web3.givenProvider); // provider from metamask
            var acts=await web3.eth.requestAccounts().catch(x=>log(x.message));
            const contractCasino="0x96d04CDF71cDA085CE53d8652B50D594CFB59af3"
            const CasinoABI=[{    "constant": false,
                                  "inputs": [],
                                  "name": "betAndWin",
                                  "outputs": [],
                                  "payable": true,
                                  "stateMutability": "payable",
                                  "type": "function"
                                }];
            const CasinoContract= new web3.eth.Contract(CasinoABI,contractCasino);
            var result = await CasinoContract.methods.betAndWin().send({from: acts[0],value:1});
            var win=web3.utils.hexToNumber((result.events[0].raw.data));
            log(`Win result=${win}`);
        }
        window.addEventListener('DOMContentLoaded', f);
        </script>
    </body>
</html>
```



MetaMask Notification

Rinkeby Test Network

Account 1 → 0xfDC0...AF...

CONTRACT INTERACTION

♦0

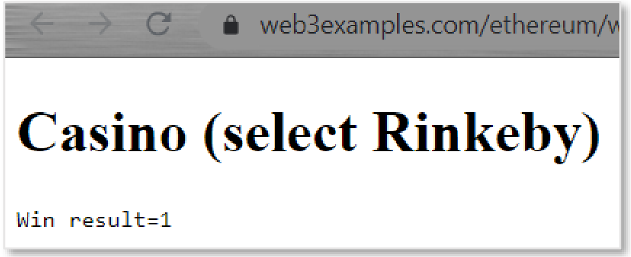
GAS FEE ♦0.000034
No Conversion Rate Available

Gas Price (GWEI): 1

Gas Limit: 34105

AMOUNT + GAS FEE

TOTAL ♦0.000034
No Conversion Rate Available



web3examples.com/ethereum/w

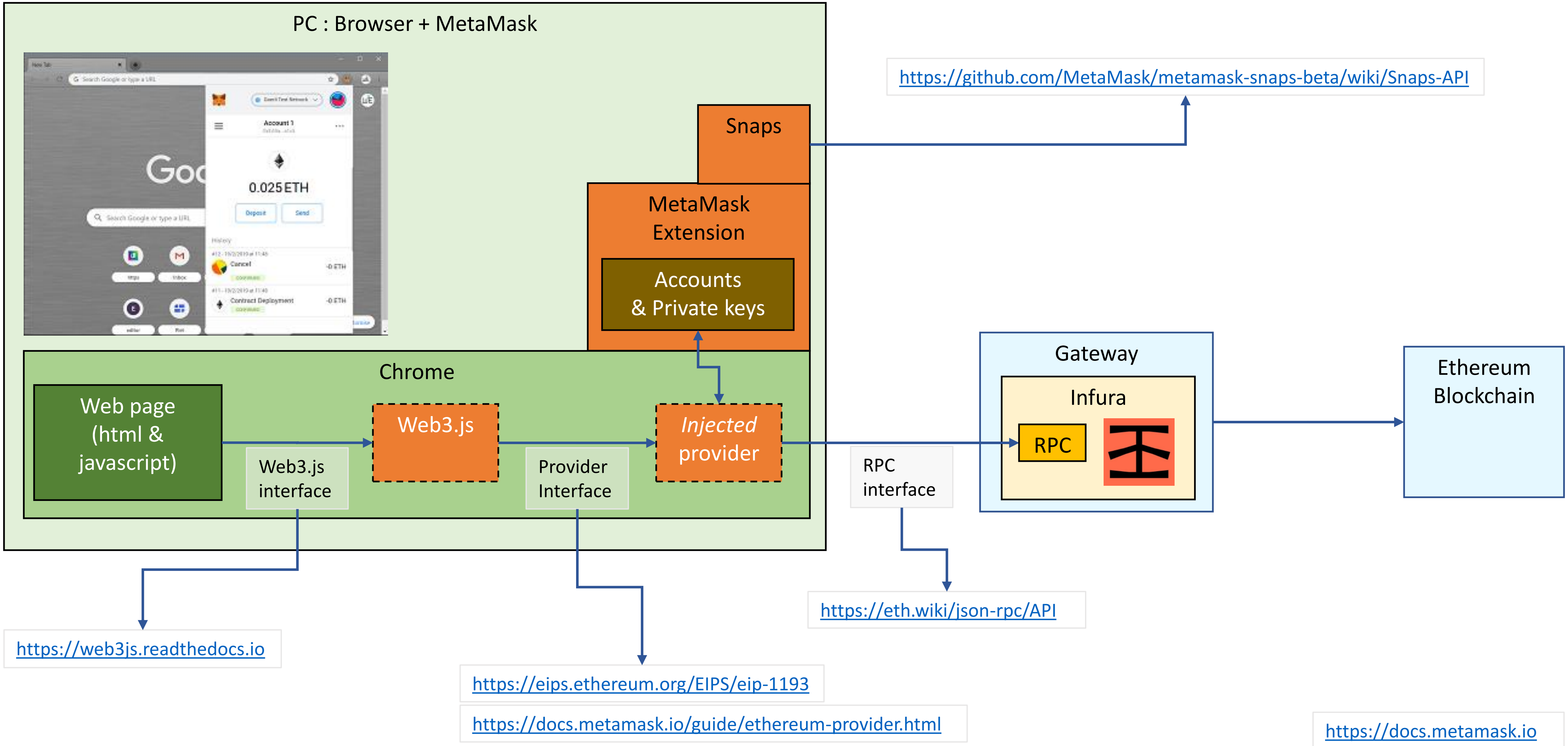
Casino (select Rinkeby)

```
Win result=1
```

https://web3examples.com/ethereum/web3js_browser/casino_snippet.html

https://github.com/web3examples/ethereum/blob/master/web3js_browser/casino_snippet.html

MetaMask & Web3js



PC : Browser + MetaMask

Snaps

MetaMask Extension

Accounts & Private keys

Chrome

Web page (html & javascript)

Web3.js

Injected provider

Web3.js interface

Provider Interface

RPC interface

Gateway

Infura

RPC

Ethereum Blockchain

https://github.com/MetaMask/metamask-snaps-beta/wiki/Snaps-API

https://eth.wiki/json-rpc/API

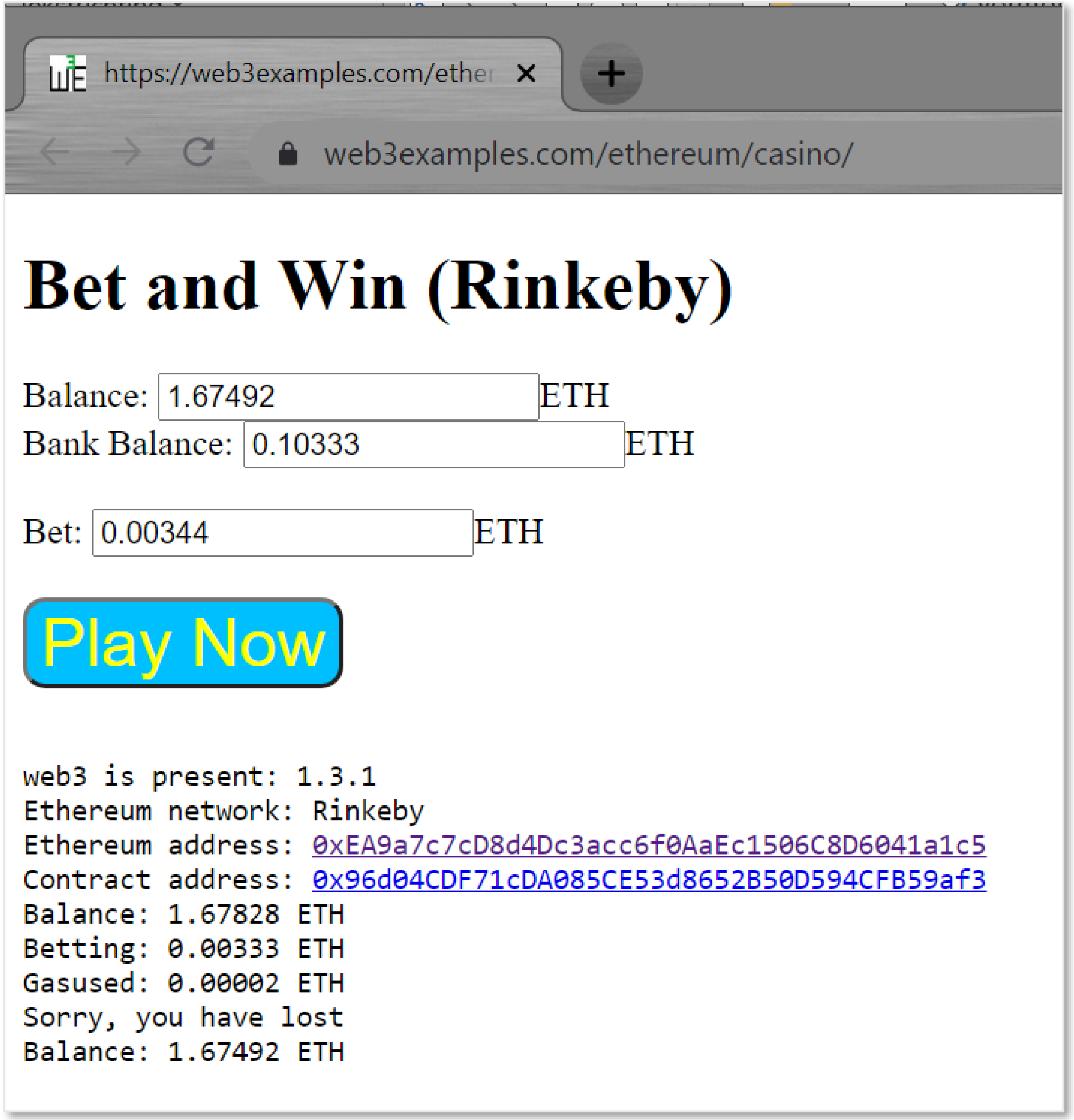
https://web3js.readthedocs.io

https://eips.ethereum.org/EIPS/eip-1193

https://docs.metamask.io/guide/ethereum-provider.html

https://docs.metamask.io

Casino – full version


https://web3examples.com/ether ×
web3examples.com/ethereum/casino/

Bet and Win (Rinkeby)

Balance: 1.67492 ETH
Bank Balance: 0.10333 ETH

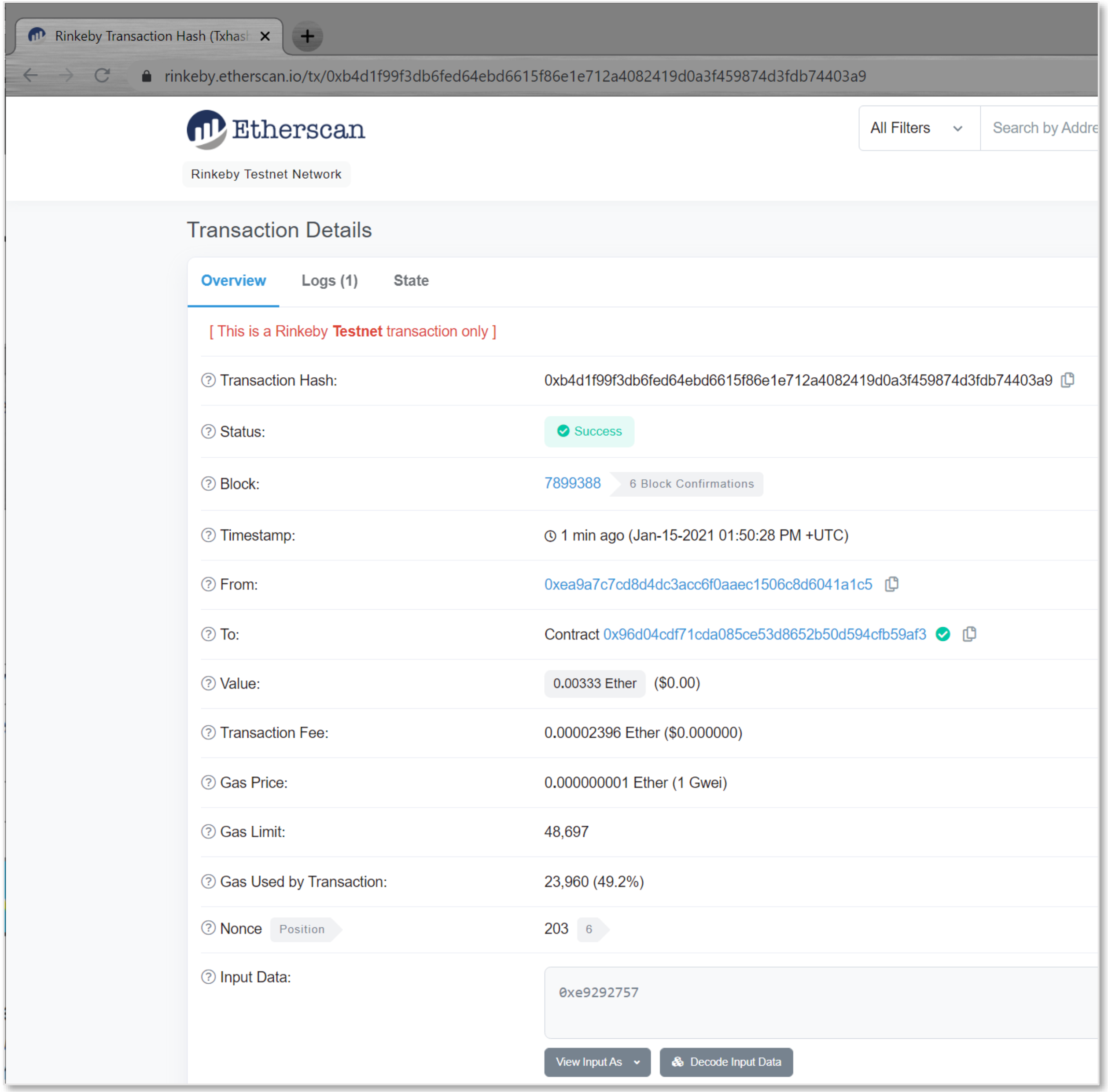
Bet: 0.00344 ETH

```
web3 is present: 1.3.1
Ethereum network: Rinkeby
Ethereum address: 0xEA9a7c7cD8d4Dc3acc6f0AaEc1506C8D6041a1c5
Contract address: 0x96d04CDF71cDA085CE53d8652B50D594CFB59af3
Balance: 1.67828 ETH
Betting: 0.00333 ETH
Gasused: 0.00002 ETH
Sorry, you have lost
Balance: 1.67492 ETH
```

https://web3examples.com/ethereum/casino

https://github.com/web3examples/ethereum/tree/master/casino

Etherscan



Rinkeby Transaction Hash (Txhash
rinkeby.etherscan.io/tx/0xb4d1f99f3db6fed64ebd6615f86e1e712a4082419d0a3f459874d3fdb74403a9
Etherscan
Rinkeby Testnet Network
All Filters
Search by Addre

Transaction Details

Overview | Logs (1) | State

[This is a Rinkeby **Testnet** transaction only]

Transaction Hash: 0xb4d1f99f3db6fed64ebd6615f86e1e712a4082419d0a3f459874d3fdb74403a9

Status: ✓ Success

Block: 7899388 6 Block Confirmations

Timestamp: 1 min ago (Jan-15-2021 01:50:28 PM +UTC)

From: 0xea9a7c7cd8d4dc3acc6f0aaec1506c8d6041a1c5

To: Contract 0x96d04cdf71cda085ce53d8652b50d594cfb59af3 ✓

Value: 0.00333 Ether ($0.00)

Transaction Fee: 0.00002396 Ether ($0.000000)

Gas Price: 0.000000001 Ether (1 Gwei)

Gas Limit: 48,697

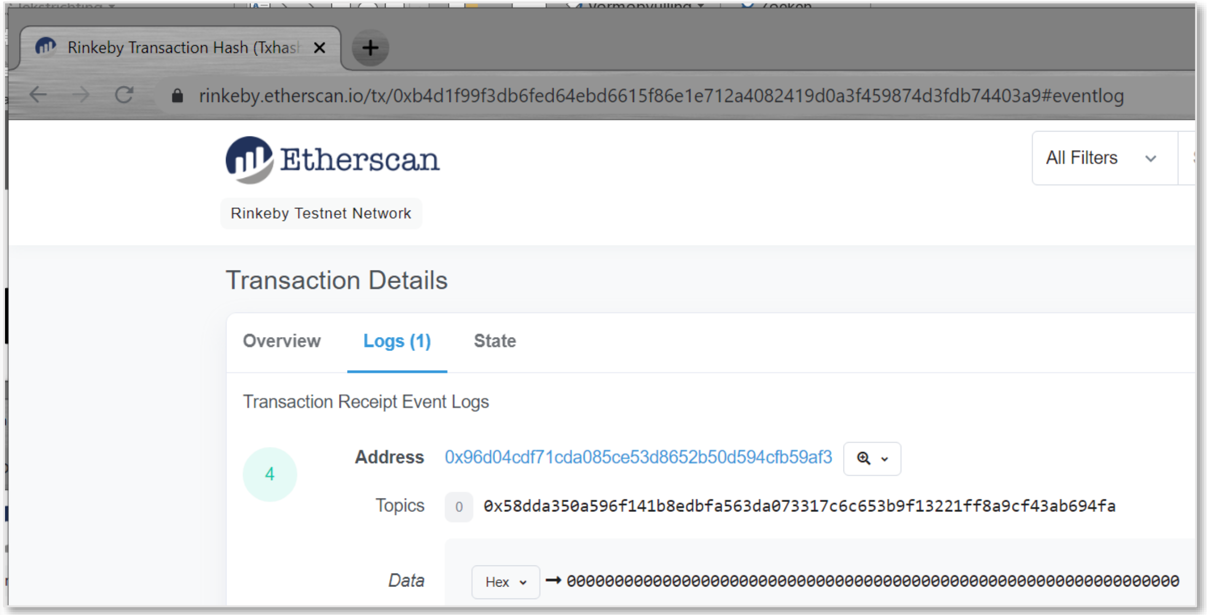
Gas Used by Transaction: 23,960 (49.2%)

Nonce Position: 203 6

Input Data:

```
0xe9292757
```

View Input As
Decode Input Data



Rinkeby Transaction Hash (Txhash
rinkeby.etherscan.io/tx/0xb4d1f99f3db6fed64ebd6615f86e1e712a4082419d0a3f459874d3fdb74403a9#eventlog
Etherscan
Rinkeby Testnet Network
All Filters

Transaction Details

Overview | Logs (1) | State

Transaction Receipt Event Logs

4

Address 0x96d04cdf71cda085ce53d8652b50d594cfb59af3

Topics 0 0x58dda350a596f141b8edbfa563da073317c6c653b9f13221ff8a9cf43ab694fa

Data Hex → 0000000000000000000000000000000000000000000000000000000000000000

https://rinkeby.etherscan.io/tx/0xb4d1f99f3db6fed64ebd6615f86e1e712a4082419d0a3f459874d3fdb74403a9

More examples

https://web3examples.com/ethereum/web3js_browser