#### PD-2.0.0 First smart contract

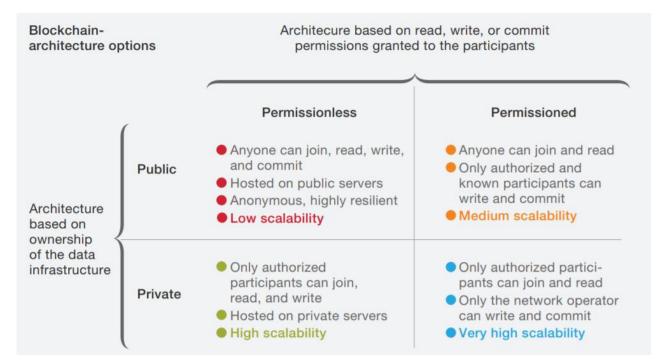
- PD-2.1 Architecture
- PD-2.2 Reading material
- PD-2.3 Prepare to use the play editor
- PD-2.4 Solidity

#### PD-2.1.0 Architecture

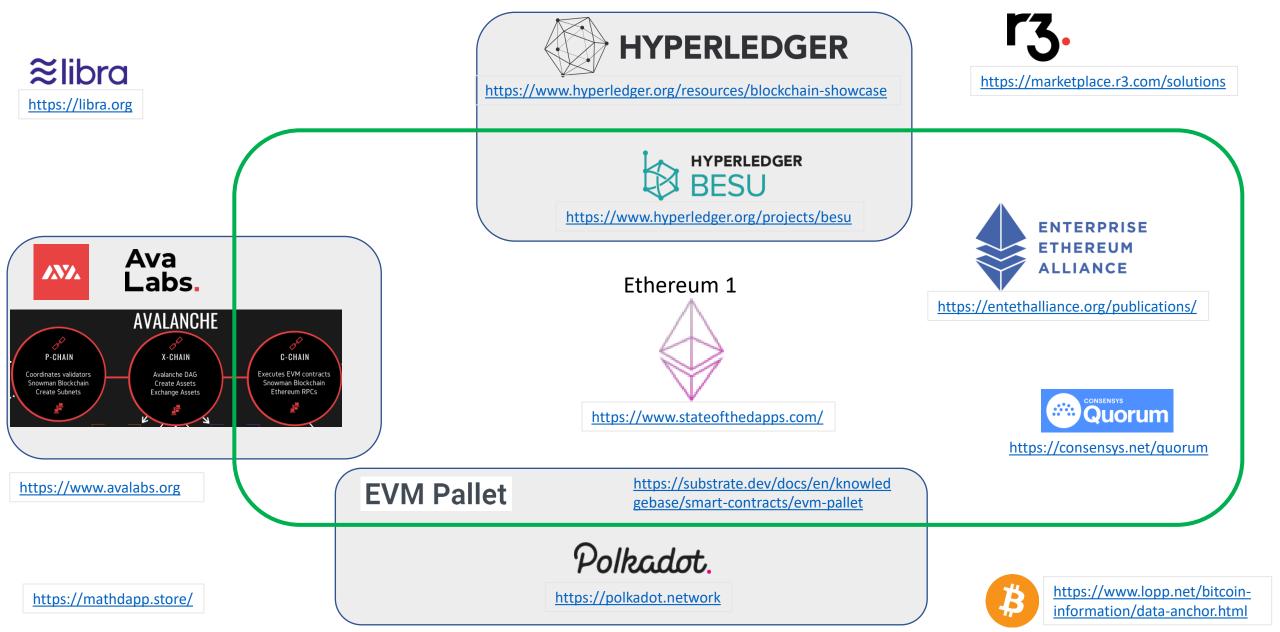
- PD-2.1.1 Types of blockchains
- PD-2.1.2 Characteristics of blockchains
- PD-2.1.3 First generation blockchains
- PD-2.1.4 Second generation blockchains
- PD-2.1.5 Third generation blockchains
- PD-2.1.6 Objects and interactions
- PD-2.1.7 DAPP architecture

## PD-2.1.1 Types of blockchains

	Public	Private Permissioned	Public (read) Permissioned (write)
1 <sup>st</sup> gen	Bitcoin		
2 <sup>nd</sup> gen Smart contracts	Ethereum	Ethereum enterprise Hyperledger	Hyperledger Fabric
3 <sup>rd</sup> gen Multichain & upgradability	Polkadot Ethereum 2.0 Avalanche		



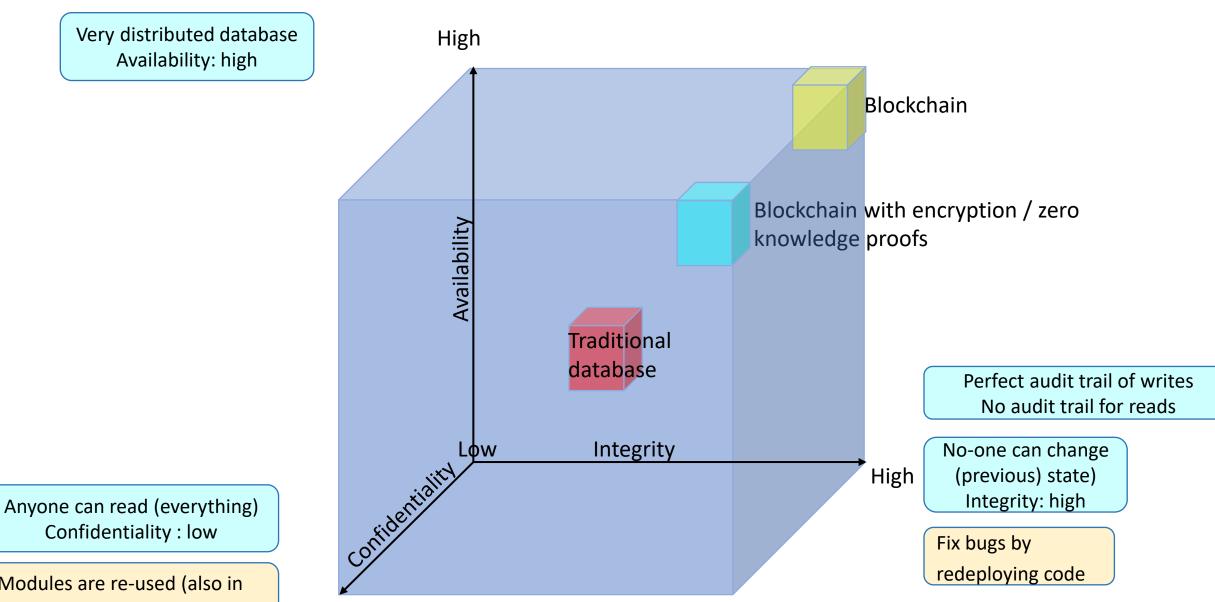
### PD-2.1.1 Different blockchains



### PD-2.1.1 Why Ethereum?

- Permissionless & open
- Most used chain
- Reference chain (everyone compares to Ethereum 1)
- Other chain incorporate EVM or connect
- Network effects / money lego
- Disadvantage: high fees
  - Accelerates layer 2 solutions

### PD-2.1.2 Characteristics of blockchains

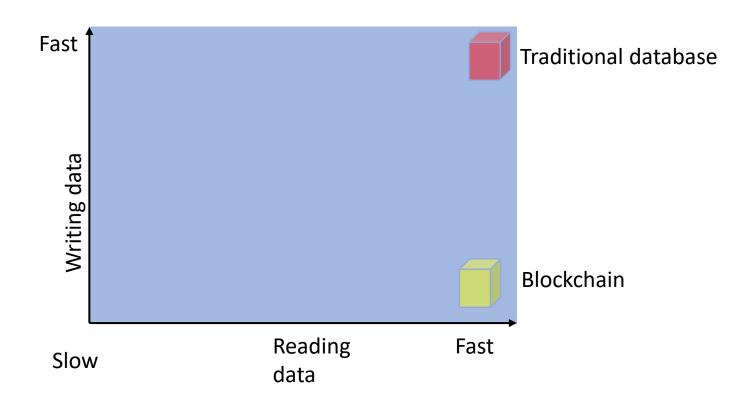


Modules are re-used (also in

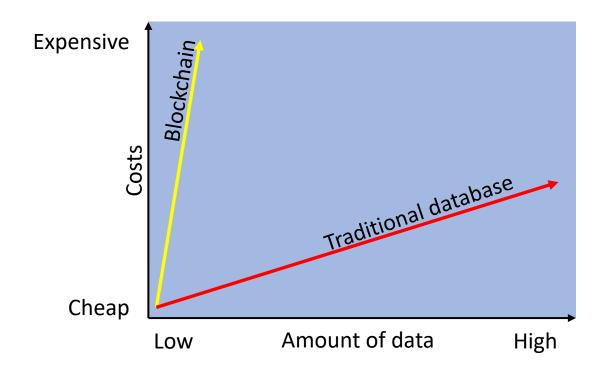
High

unexpected ways)

### PD-2.1.2 Performance blockchain



### PD-2.1.2 Amounts of data vs Costs



### PD-2.1.2 Other characteristics

Money/value involved => bugs quickly security bugs Anyone can deploy code

Anyone can interact with smart contract

Anyone can copy the entire chain (fork)

Shared infrastructure & pay for usage

Hindrance by others

Denial of service possible (gas)

Key management important

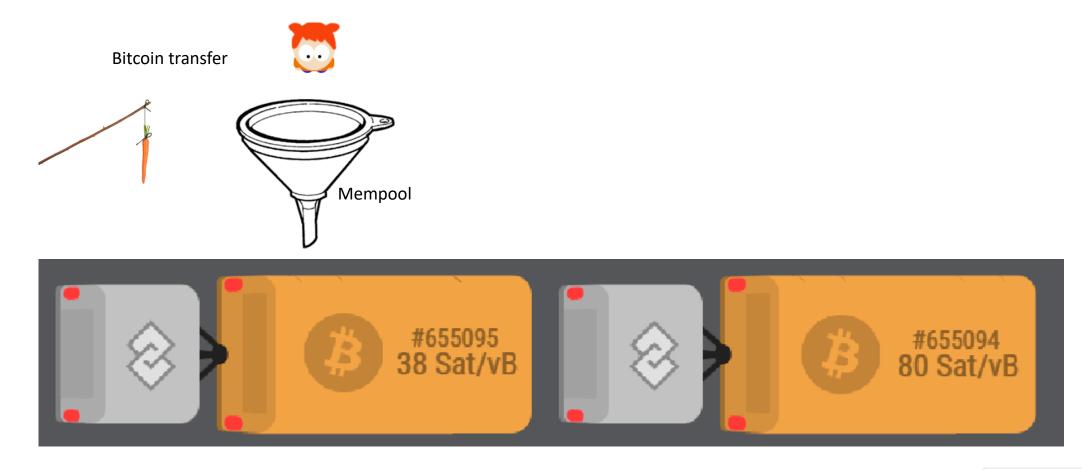
Immature, complex, changing rapidly => lots of bugs

Need to trust cryptography, protocols, software, network, incentive mechanisms

Trust is gained by proving all possible interactions

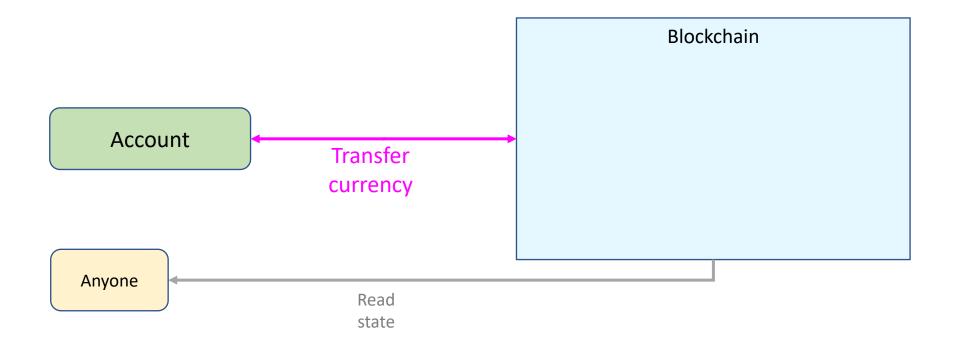
Incentive design important

## PD-2.1.3 First generation blockchains

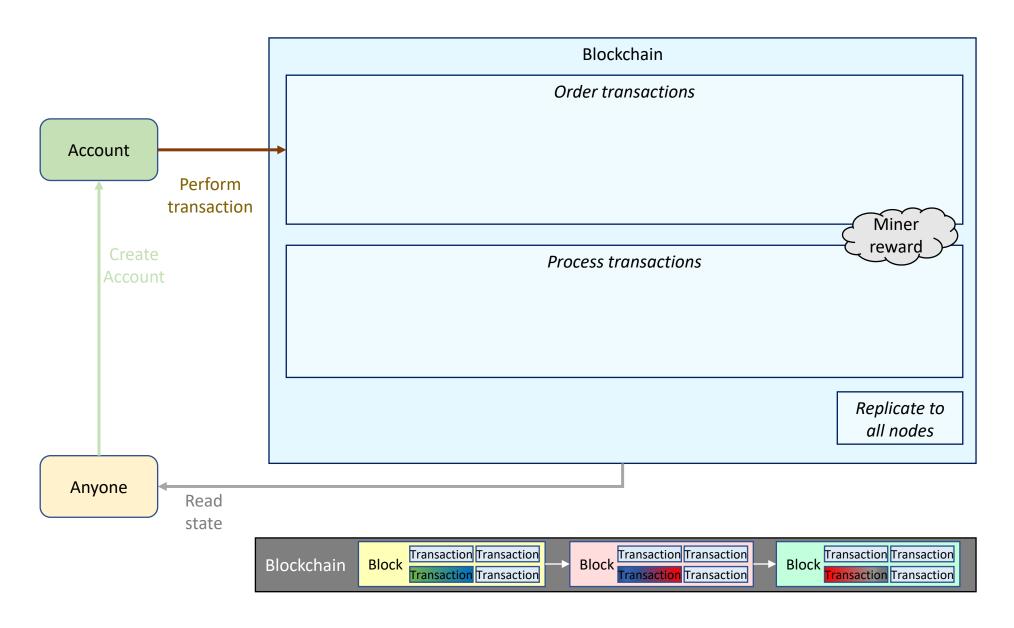


https://txstreet.com/v/btc

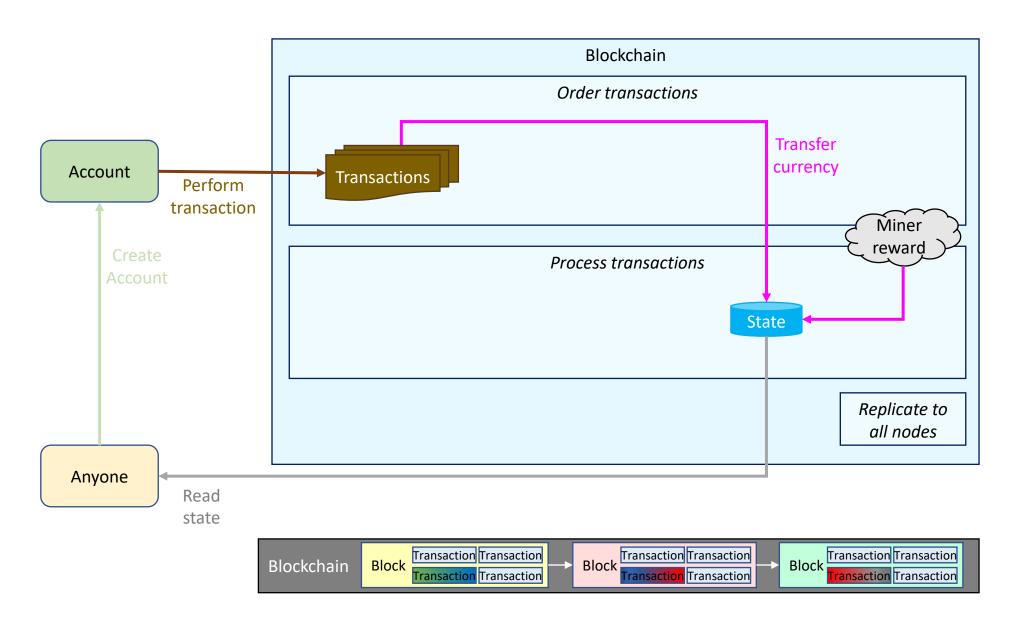
## PD-2.1.3 Black box 1<sup>st</sup> generation



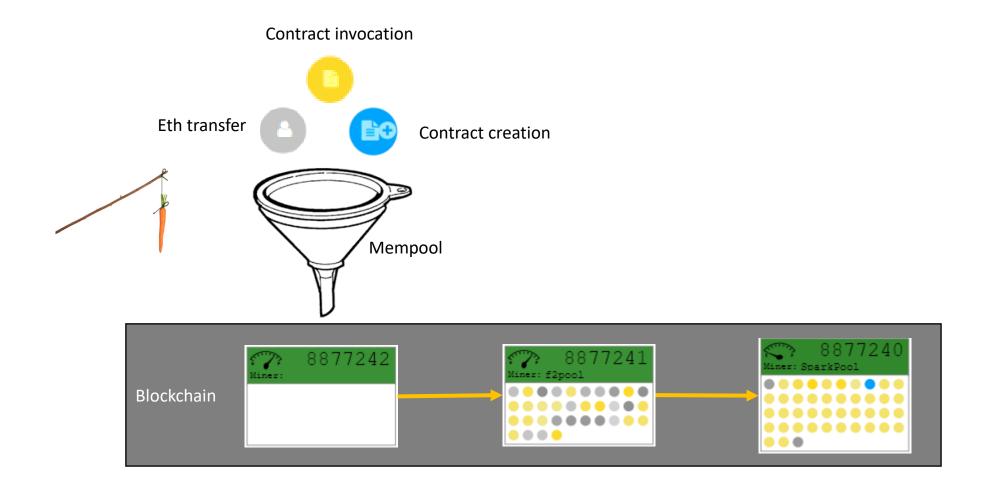
## PD-2.1.3 Architecture 1<sup>st</sup> generation



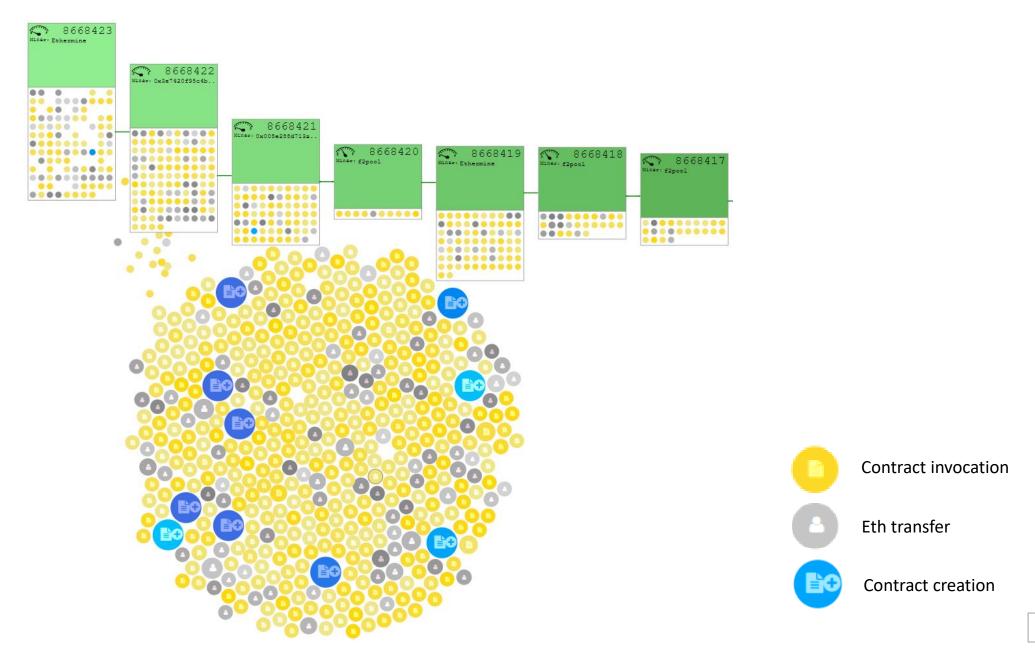
## PD-2.1.3 Architecture 1<sup>st</sup> generation



## PD-2.1.4 Second generation blockchains

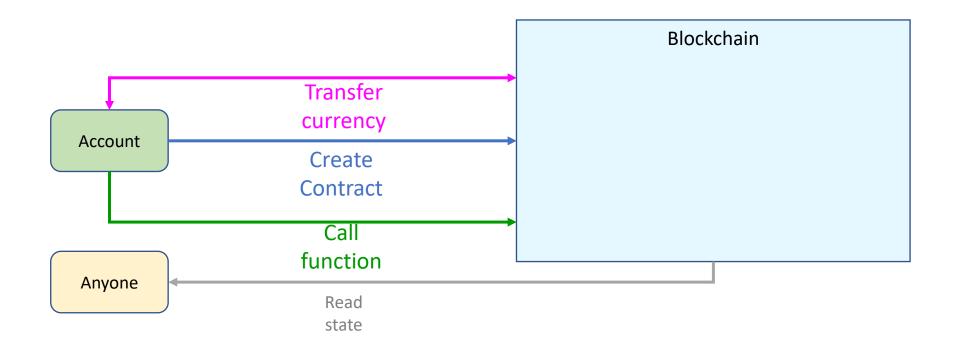


### PD-2.1.4 EthViewer

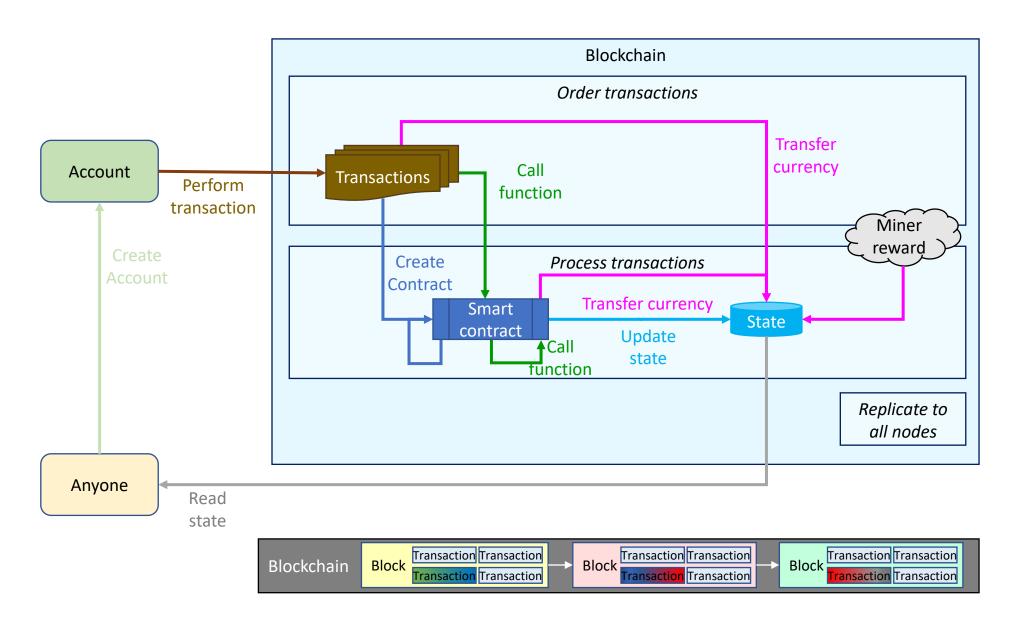


http://ethviewer.live/

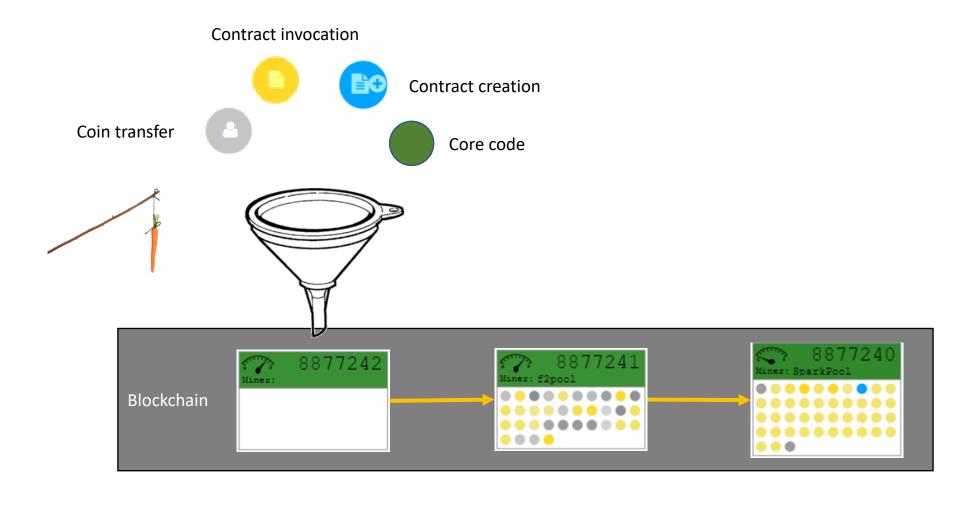
## PD-2.1.4 Black box 2<sup>nd</sup> generation



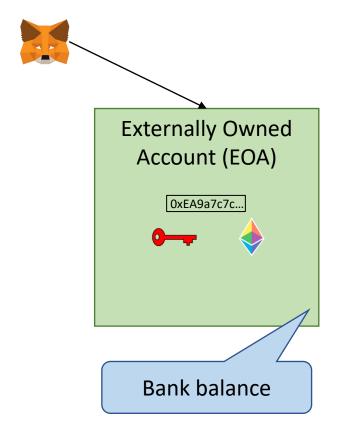
# PD-2.1.4 Architecture 2<sup>nd</sup> generation

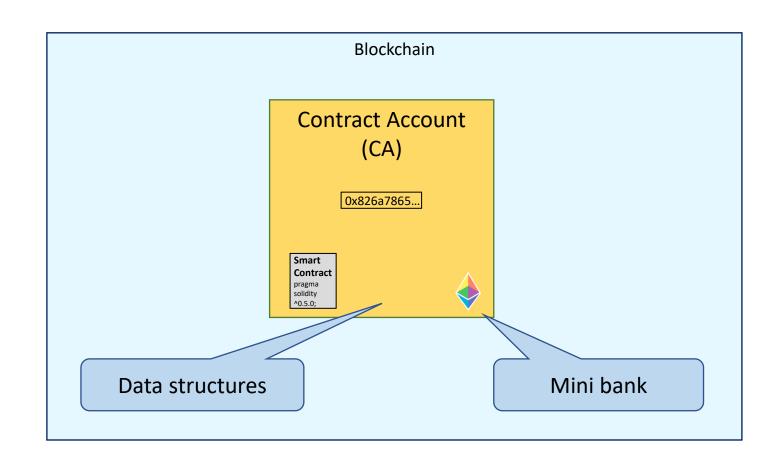


## PD-2.1.5 Third generation blockchains

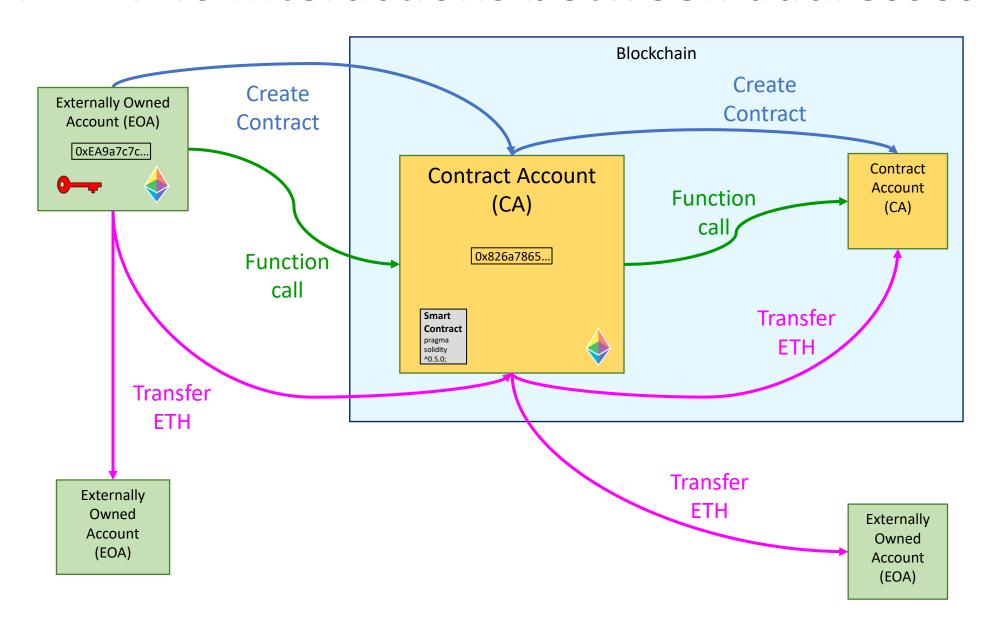


## PD-2.1.6 Objects and interactions

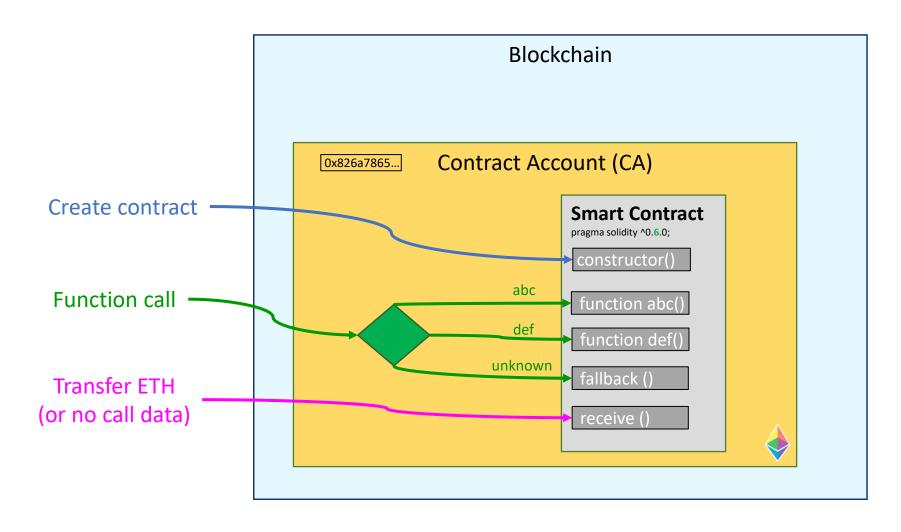




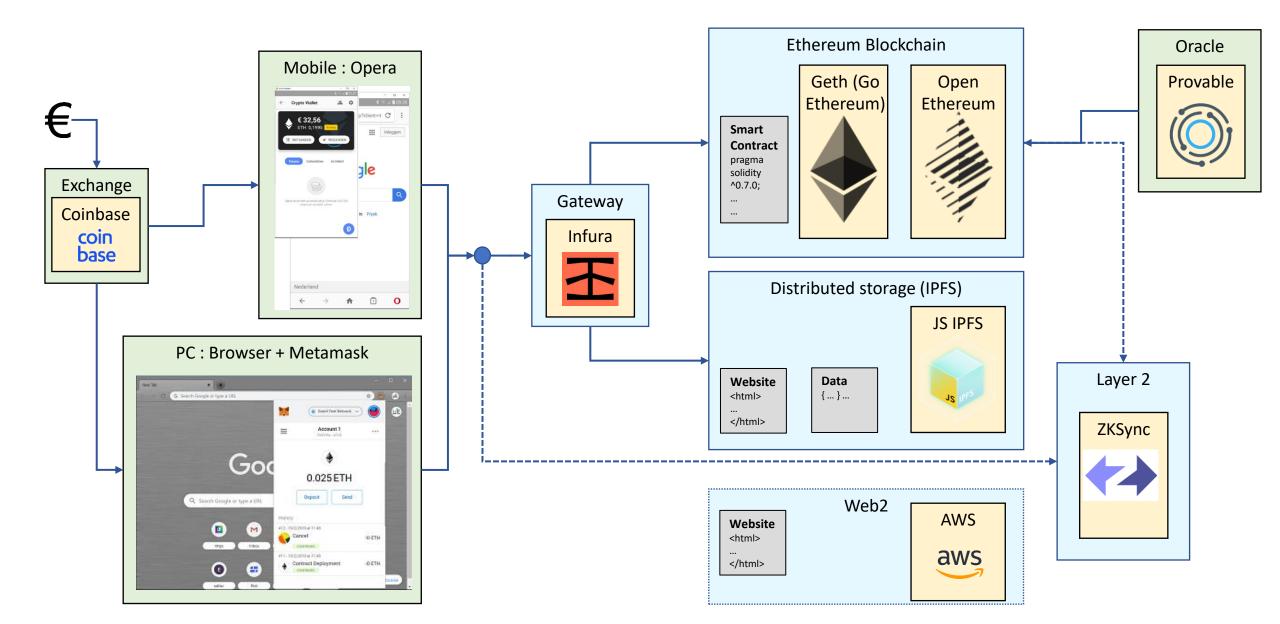
### PD-2.1.6 Interactions between addresses



### PD-2.1.6 Functions of a smart contract



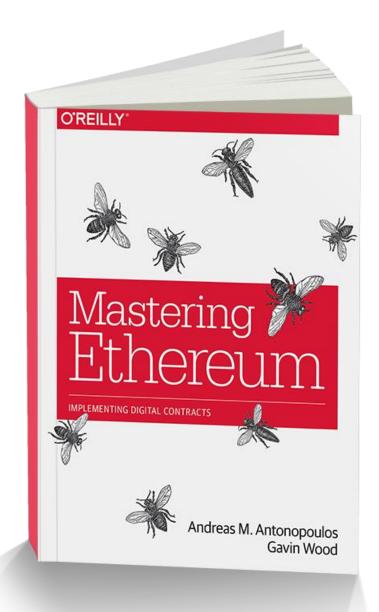
### PD-2.1.7 DAPP architecture



### PD-2.2 Reading material

- Mastering Ethereum (mandatory)
- Crypto Zombies (mandatory)
- Solidity manual (mandatory)
- Ethereum.org
- EthHub
- Consensys developer portal

## PD-2.2.1 Mastering Ethereum



https://ethereumbook.info

https://github.com/ethereumbook/ethereumbook/blob/develop/01what-is.asciidoc

https://github.com/ethereumbook/ethereumbook/blob/develop/book.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/02intro.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/03clients.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/04keys-addresses.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/05wallets.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/06transactions.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/07smart-contracts-solidity.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/09smart-contracts-security.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/10tokens.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/11oracles.asciidoc

https://github.com/ethereumbook/ethereumbook/tree/develop/12dapps.asciidoc

https://github.com/ethereumbook/ethereumbook/blob/develop/13evm.asciidoc#turing-completeness-and-gas

https://github.com/ethereumbook/ethereumbook/tree/develop/14consensus.asciidoc

## PD-2.2.2 Crypto Zombies



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

https://cryptozombies.io/en/lesson/2/chapter/1

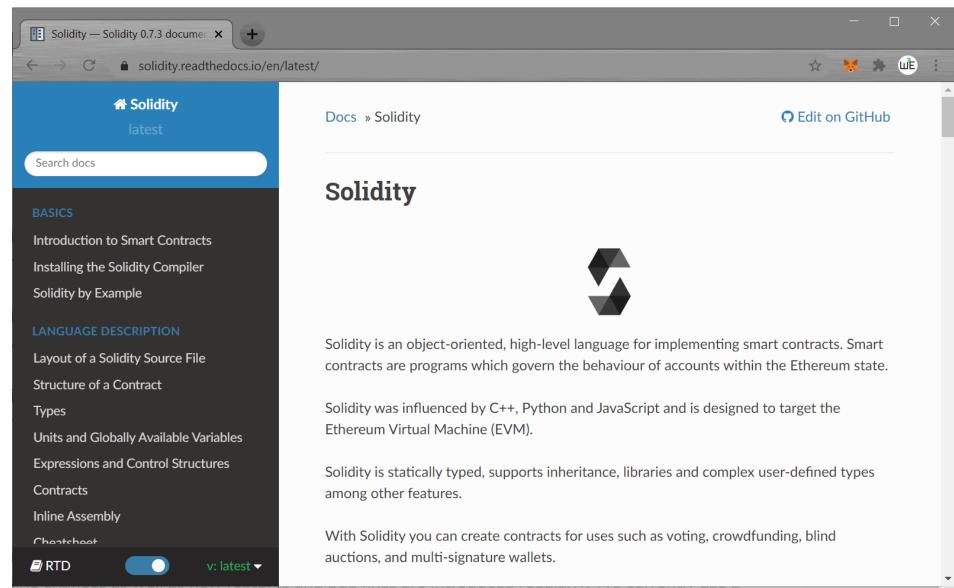
https://cryptozombies.io/en/lesson/3/chapter/1

https://cryptozombies.io/en/lesson/4/chapter/1

https://cryptozombies.io/en/lesson/5/chapter/1

https://cryptozombies.io/en/lesson/6/chapter/1

## PD-2.2.3 Solidity manual



https://soliditylang.org

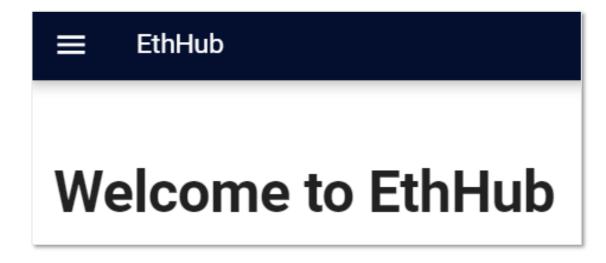
# PD-2.2.4 Ethereum.org

#### ETHEREUM DEVELOPER RESOURCES

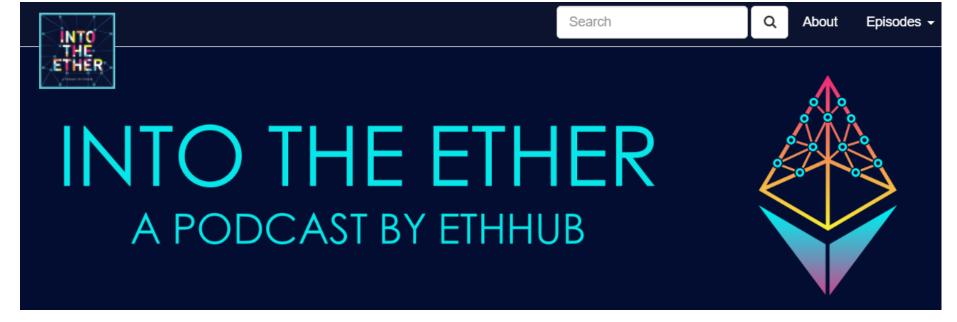
A builders manual for Ethereum. By builders, for builders.



### PD-2.2.5 EthHub



https://docs.ethhub.io



https://podcast.ethhub.io

### PD-2.2.6 Consensys developer portal



## PD-2.3 Prepare to use the play editor

- Install MetaMask
- Select testnetwork
- Get test ETH
- Play editor
- Etherscan
- Avalanche chain

### PD-2.3.1 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	Сору	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}



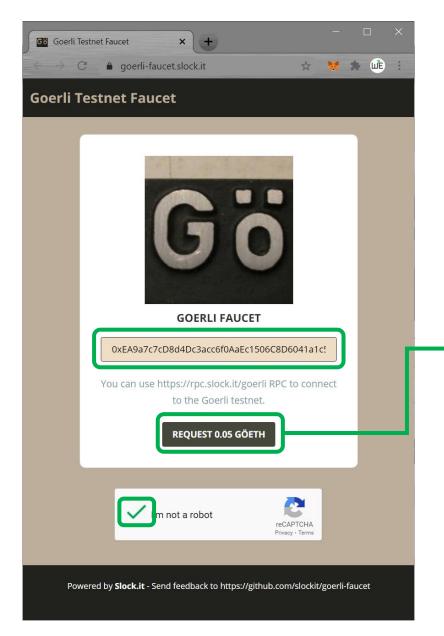
https://www.youtube.com/watch?v=Wc-Hgn1QUjA



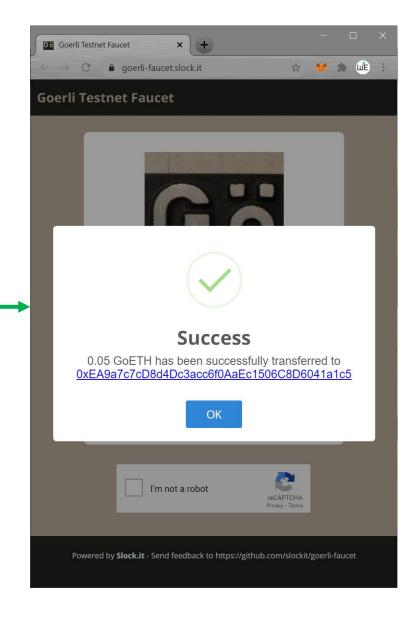
https://metamask.io/

http://web3examples.com/ethereum/install/Install MetaMask Windows.html

#### PD-2.3.2 Goerli test ETH



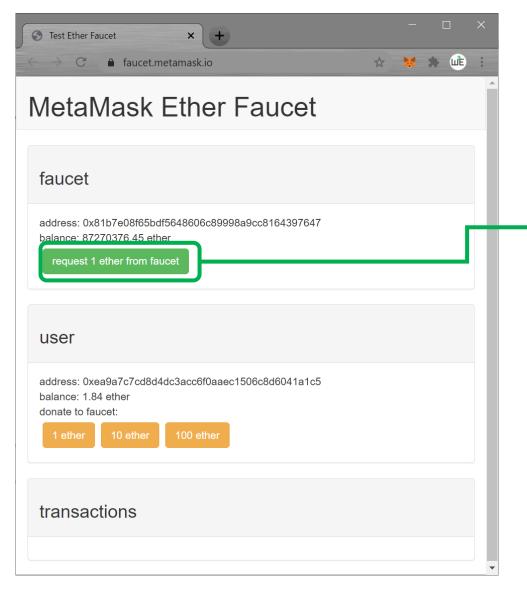


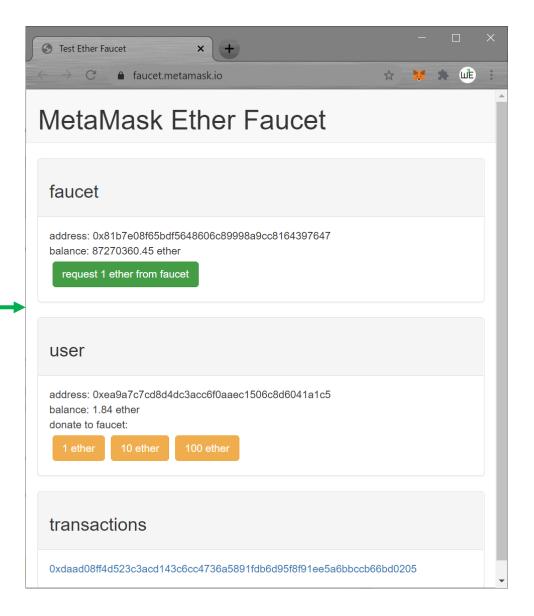


https://goerli-faucet.slock.it

https://faucet.goerli.mudit.blog

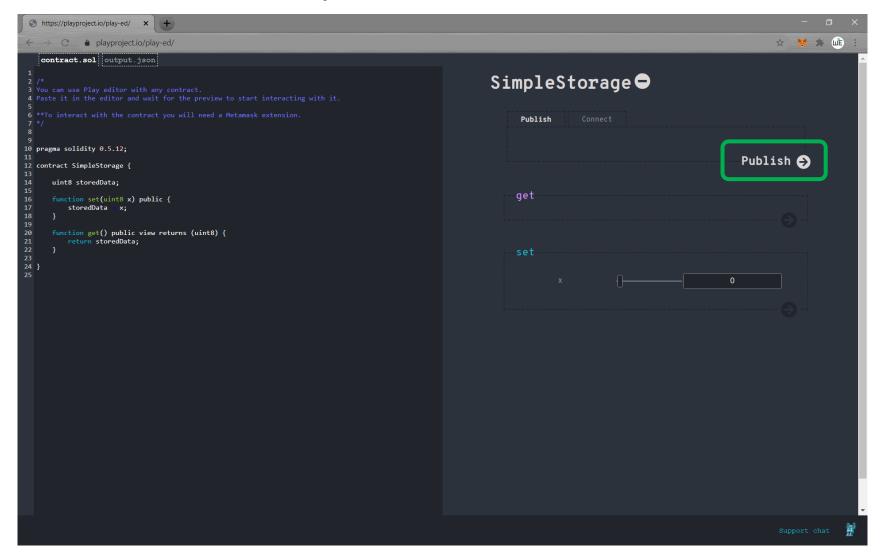
### PD-2.3.2.1 Ropsten test ETH







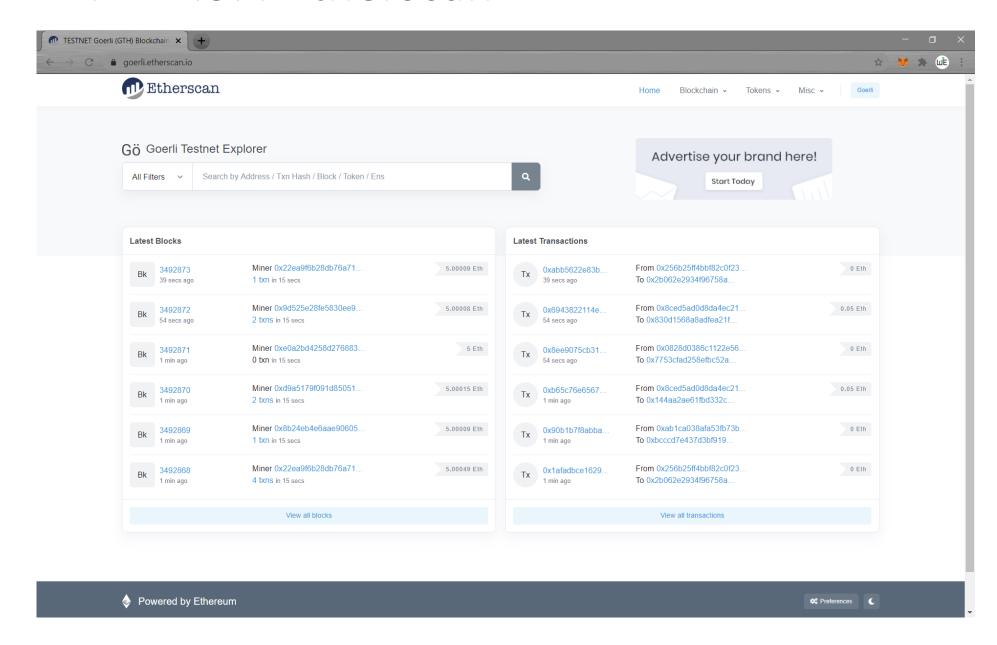
## PD-2.3.3 Play editor



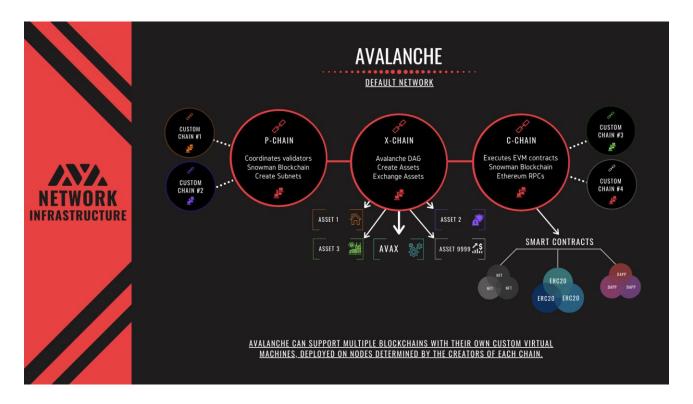
https://playproject.io/play-ed/

https://github.com/playproject-io/play-ed

#### PD-2.3.4 Etherscan



#### PD-2.3.5 Avalanche C-Chain



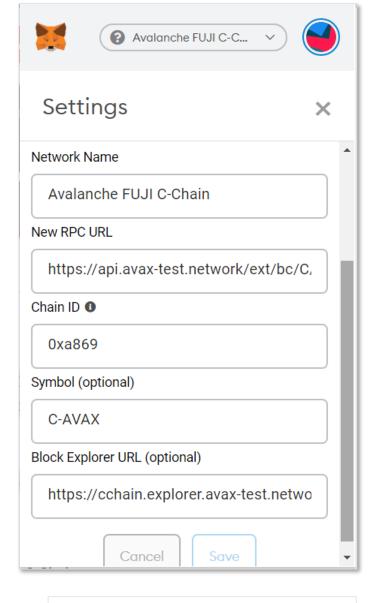
#### **FUJI Testnet Settings:**

•Network Name: Avalanche FUJI C-Chain

•New RPC URL: https://api.avax-test.network/ext/bc/C/rpc

•ChainID: 0xa869 •Symbol: C-AVAX

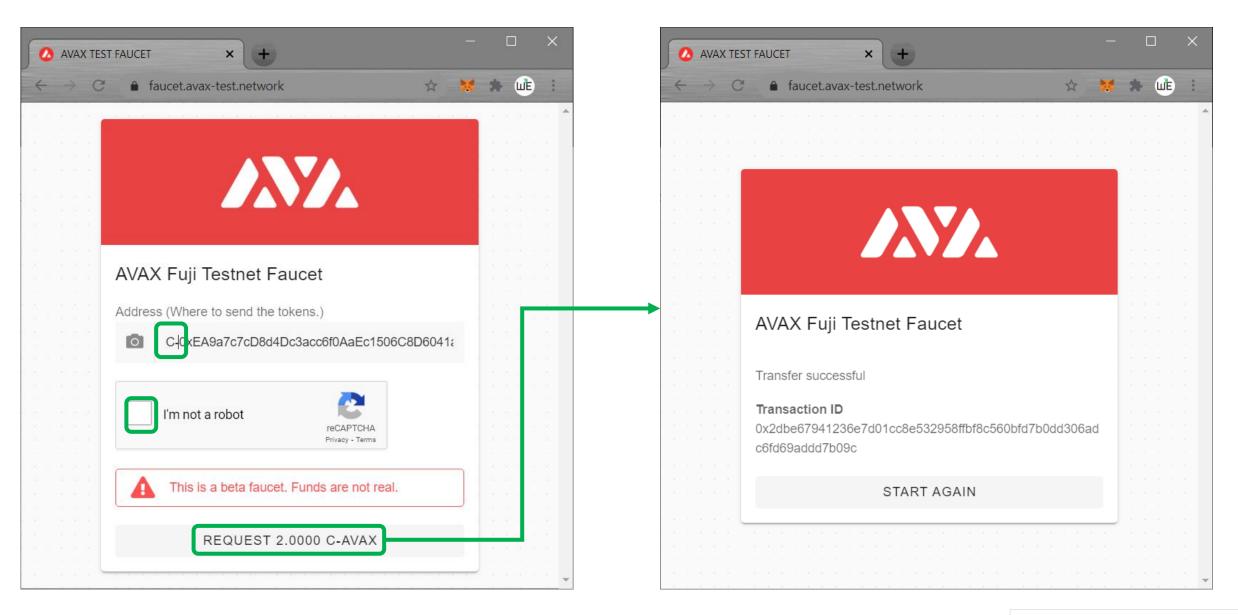
•Explorer: <a href="https://cchain.explorer.avax-test.network">https://cchain.explorer.avax-test.network</a>



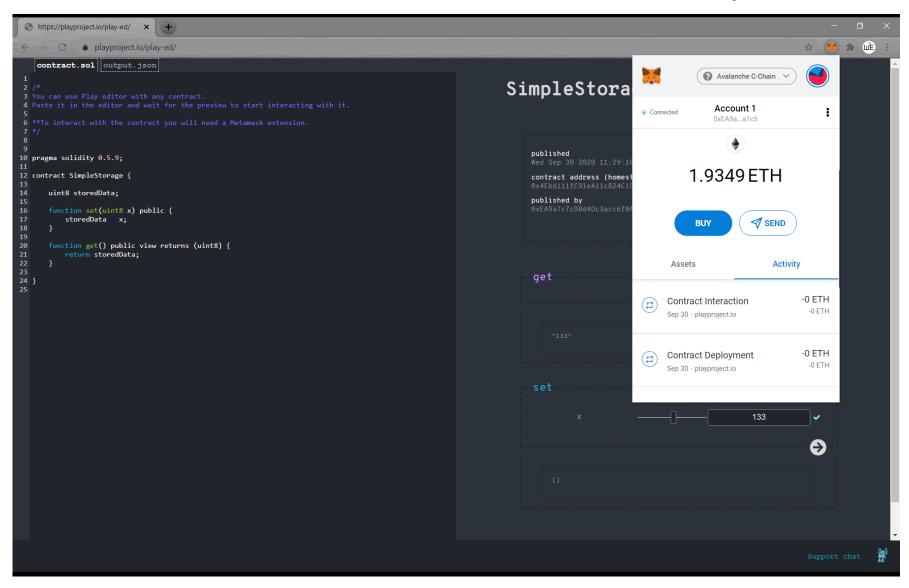
https://api.avax-test.network/ext/bc/C/rpc

https://cchain.explorer.avax-test.network

#### PD-2.3.6 Avalanche C-Chain faucet



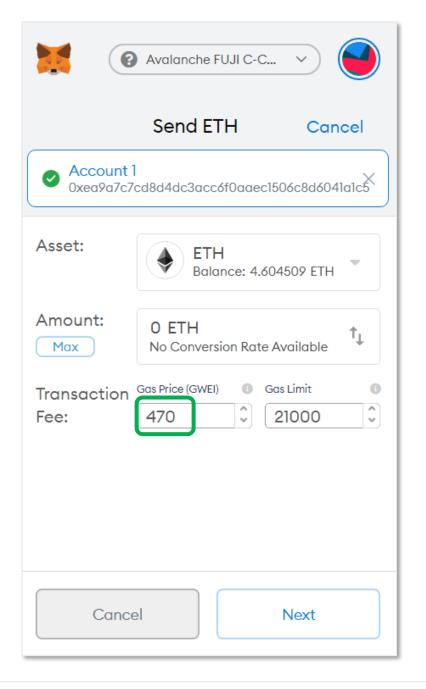
## PD-2.3.7 Avalanche C-Chain Play editor



#### PD-2.3.8 Avalanche GasPrice

The C-Chain gas price is 4.7e-7 AVAX/gas.

The C-Chain gas limit is 10e8.



https://docs.avax.network/learn/platform-overview/transaction-fees

## PD-2.4 Solidity

Try out several examples

http://web3examples.com/ethereum/#solidity

http://web3examples.com/ethereum/solidity\_examples

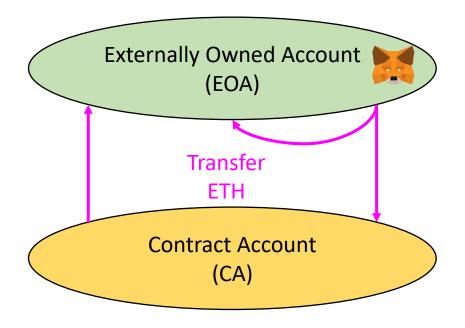
https://solidity-by-example.org

### PD-2.4.1 SimpleStorage

```
SimpleStorage.sol
     =/*
      You can use Play editor with any contract.
       Paste it in the editor and wait for the preview to start interacting with it.
  4
  5
  6
      **To interact with the contract you will need a Metamask extension.
  8
  9
 10
      pragma solidity 0.5.9;
 11
 12
       contract SimpleStorage {
 13
 14
           uint8 storedData;
 15
 16
           function set(uint8 x) public {
 17
               storedData = x;
 18
 19
 20
           function get() public view returns (uint8) {
 21
               return storedData;
 22
 23
 24
```

#### PD-2.4.2 Hello World

#### PD-2.4.3 Transfer ETH





http://web3examples.com/ethereum/demo/Play Transfer eth with contract.html

https://github.com/web3examples/ethereum/blob/master/solidity\_examples/Transfer.sol

### PD-2.4.4 Types

```
pragma solidity ^0.5.11;
    contract Types {
        bool public a; // note: public variables => getter
  4
        int public b1;
  6
      int256 public b256=1;
  7
     vee uint public b2=2;
  8
       // no floating point
        address public c1;
  9
 10
        address payable public c2;
 11
     byte public d0;
 12
     bytes1 public d1; // fixed byte array
 13
     bytes3 public d3;
 14
     bytes32 public d32;
 15
       uint[] public e1=[12,7,6,4];
 16
 17
        function elgetCount() public view returns(uint count) {
      return e1.length;
 18
 19
 20
 21
        string public e2 ="Test";
 22
 23
        enum Choices { A, B, C, D }
 24
        Choices public f1=Choices.D;
 25 }
```

### PD-2.4.5 Arrays

```
Arrays.sol
     5'ragin'aeb3's:opesjetderut/ylidit/@mp5s\Ty1e1s;
     contract TestArray {
     struct member {
     ···· uint data;
     . . . . . . . address sender;
  8
  9
         member[] public List;
 10
         mapping(address => uint) public Map;
 11
 12
         function add(uint x) public {
 13
      member memory temp;
 14
      temp.data=x;
 15
      temp.sender=msg.sender;
 16
      Map[msg.sender] = x;
 17
      List.push (temp);
 18
 19
 20
         function ListLength() public view returns(uint) {
 21
           return List.length;
 22
    23
```

### PD-2.4.6 Mappings

```
Mapping.sol
     pragma solidity ^0.5.11;
      contract RegisterParticipants {
         mapping(address => bool) public MapParticipant;
      ····address[] ·public · ListParticipant;
      · · · · mapping (address · = > · uint) · public · IndexInList;
      ····constructor() ·public · { ·
      ·····ListParticipant.push(address(0)); ·// · "use" · address · 0, · to · make · tests · easier
      . . . . } . .
 10
      ···· function · Participate (bool · Join) · public · {
 11
      .... MapParticipant [msq.sender] = Join;
 12
      ....uint i=IndexInList[msq.sender];
 13
      ····

if (i.>.0) · { · // · Delete · previous · participation · entry
 14
      ·····ListParticipant[i] ·= ·ListParticipant[ListParticipant.length ·-·1]; ·// ·switch
 15
      .... IndexInList [msq.sender]=0;
 16
      17
 18
      .....ListParticipant.pop();
 19
      .....if (Join) . {
 20
      ....ListParticipant.push(msg.sender);
 21
      ······IndexInList[msg.sender]=ListParticipant.length-1;
 23
      2.4
      ····function · NrOfParticipants() · public · view · returns · (uint) · {
 26
      ····· return ListParticipant.length-1;
 27
      . . . . }
 28
```

## PD-2.4.7 Storage / Memory

```
Memory_Storage.sol
      // Shows the difference between memory and storage
      pragma solidity >= 0.5.11;
  3
  4
      contract TicketSystem {
  5
      ····struct · Ticket · {uint · val; }
  6
      ····Ticket[] ·public · ticketArray;
      ····constructor() ·public · { · · · · · ·
  8
  9
      ····· Ticket memory ticket - Ticket (1234);
      ···· ticketArray.push(ticket);
 10
 11
      . . . . }
 12
      ·····function·StoreValue1(uint·value)·public·returns(·uint)·{·······
 13
      ·····Ticket·storage··ticket·=·ticketArray[0]; ·//·pointer
 14
      ····ticket.val·=·value;
      ····· return ticketArray[0].val;// returns the updated val
 15
 16
 17
      ···· function · Store Value 2 (uint · value) · public · returns (· uint) · {
 18
      ·····Ticket·memory·ticket·=·ticketArray[0];·//·copy
 19
      ····ticket.val·=·value;
 20
      ····· return ticketArray[0].val; // does not return the updated val
      . . . . }
 21
 22
```