

Introdução ao blockchain (Parte II)

Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

Blockchain vs. Google Docs

- Um só documento
- Uma mesma base de dados replicada

- Vários escritores e leitores
- Vários nodos lendo e atualizando

- Tempo para atualização do documento
- Tempo para sincronizar o ledger em todos os nodos

- Descentralizado:
 - O controle não é mais centralizado a um nodo
 - O controle e a administração difere do modo cliente/servidor (centralizado)



Explaining the Blockchain via a Google Docs ...
medium.com

Potenciais mercados

- Startups
 - Verificar lista na angel.co
- Empresas de tecnologia
 - IBM (Fabric), Facebook (Libra), Microsoft, Amazon
- Bancos
 - Bancos globais ver exemplos na blocktribe.co
- Governo
 - Coindesk UK vai rastrear financiamentos de estudantes (*student loans*) com o blockchain

blocktribe.com



Log in

Sign up

[Blockchain Jobs](#)

[Blockchain Companies](#)

[Post a Blockchain Job](#)

[Applicant Search](#)

[Pricing](#)

[Blog](#)

[FAQs](#) ▾

BLOCKCHAIN JOBS

Search 3,030 blockchain jobs

FIND JOBS

South Beach Florida

Miami votes to study using Bitcoin for employee salaries and payments to City Hall

BY JOEY FLECHAS AND ROB WILE

FEBRUARY 12, 2021 12:12 AM, UPDATED FEBRUARY 12, 2021 10:33 PM



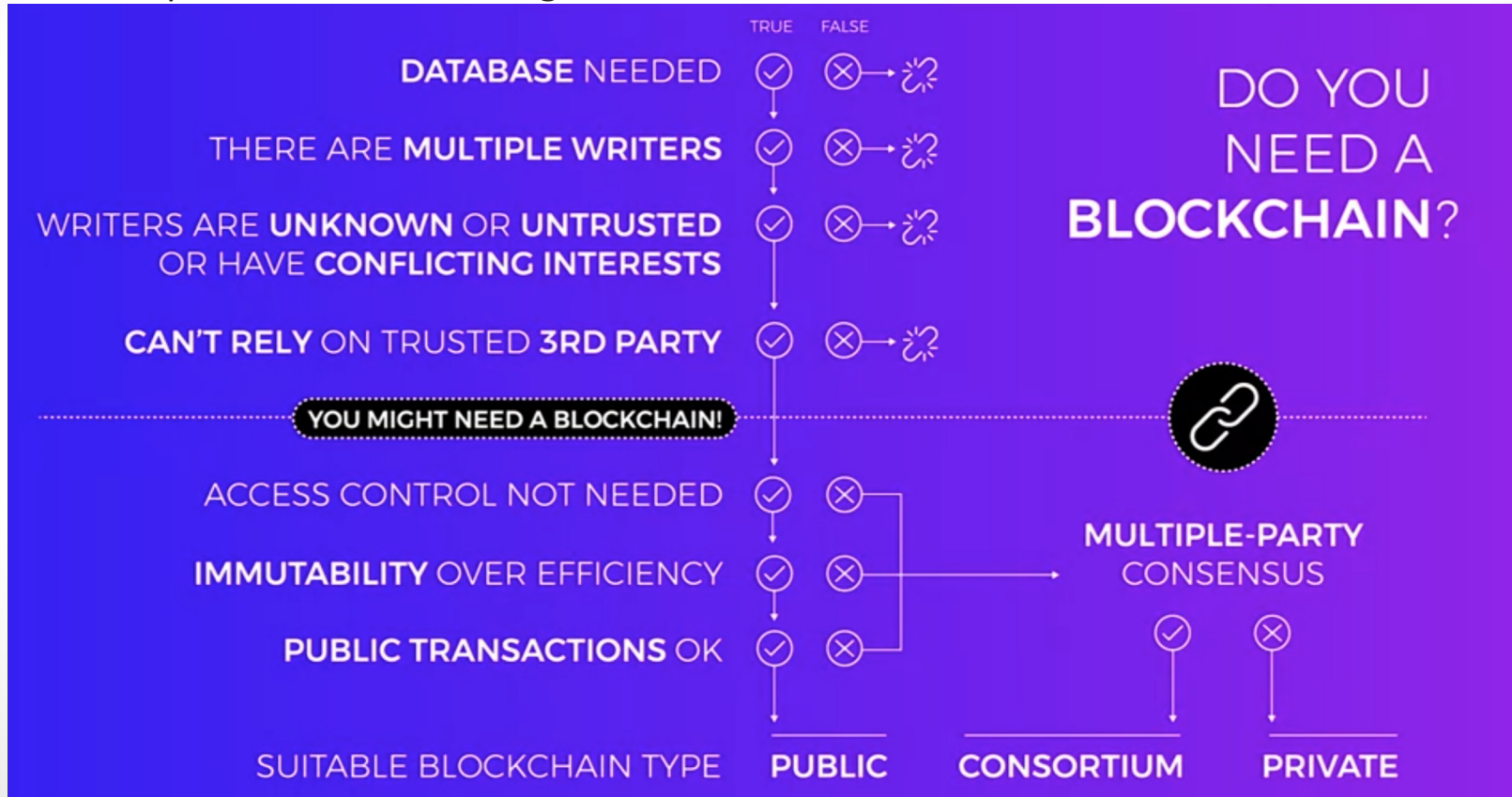
Ações em alta

Trending Tickers >

Symbol	Last Price	Change	% Change
COIN Coinbase Global, Inc.	328.28	+78.28	+31.31%
BAC Bank of America Corporation	39.88	+0.56	+1.42%
SPCE Virgin Galactic Holdings, Inc.	26.68	-0.20	-0.74%
PEP PepsiCo, Inc.	142.11	-0.94	-0.66%
C Citigroup Inc.	72.91	+0.85	+1.18%

Você precisa mesmo de blockchain?

Fonte: <https://www.coursera.org/>



Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

Transação na blockchain

- É uma ação que representa a transferência de um bem (*asset*) de um proprietário para outro
- Tal transferência é registrada no blockchain
- Na blockchain, cada proprietário é identificado pela sua chave pública



Asset Transfer Penalties -
medicaidanswers.net



Asset Transfer – Build Wealth with Duo
buildwealthwithduo.com

Transação na blockchain

- Ovelha Dolly foi clonada
- Mas a clonagem não pode ocorrer na blockchain
- Problema do gasto duplo

- Como evitar o gasto duplo?
- Uso da transação e da característica imutável
- Impossível alterar o ledger por conta da função hash
- Histórico da transação

Fonte: www.wikipedia.org



Teorema de CAP das Transações

Blockchain é baseado em:

- Peer to Peer
- Banco de dados distribuído
- Banco de dados do estilo *append only*

Mas a blockchain também é baseado no Teorema de CAP

O que diz este teorema?

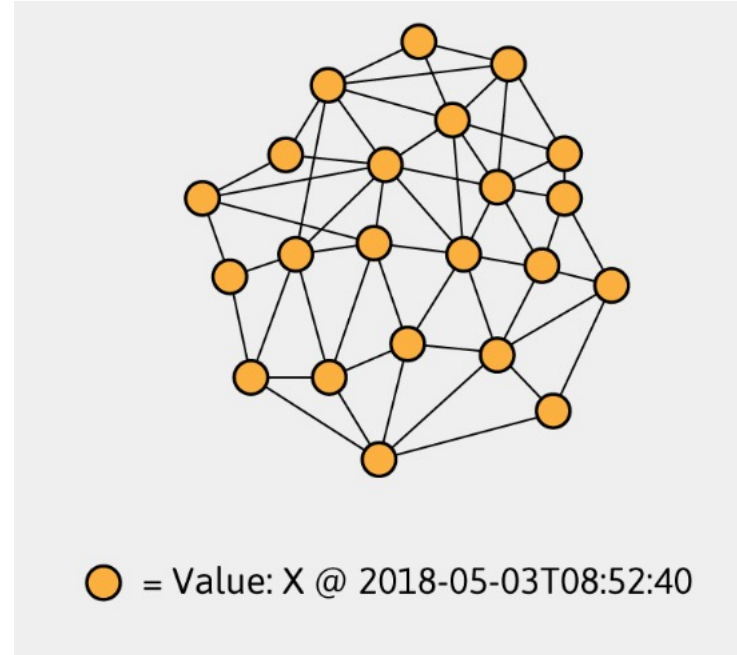
Teorema de CAP

Propriedades do Teorema:

- *Consistency*
- *Availability*
- *Partition Tolerance*

Teorema de CAP

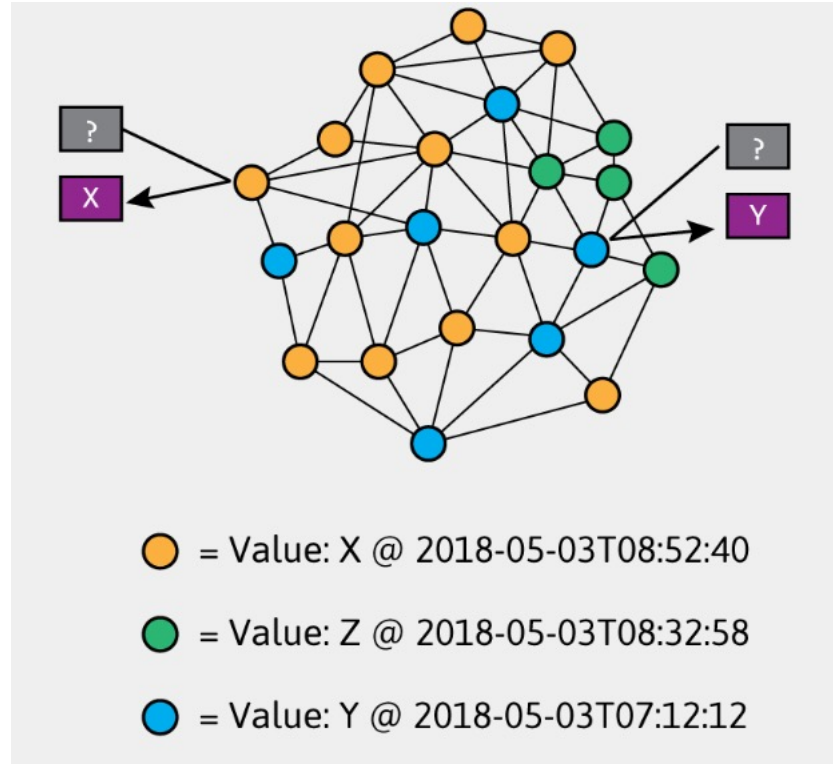
Consistency: *A qualquer momento, todos os nós da rede têm exatamente o mesmo valor (mais recente).*



Teorema de CAP

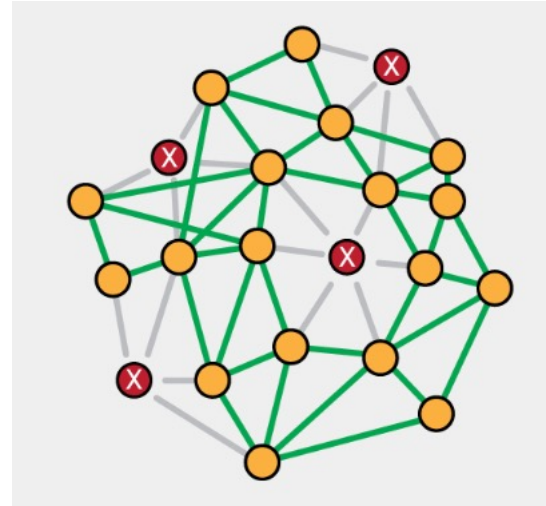
Availability

(disponibilidade): Toda solicitação à rede recebe uma resposta, embora sem nenhuma garantia de que os dados retornados sejam os mais recentes.



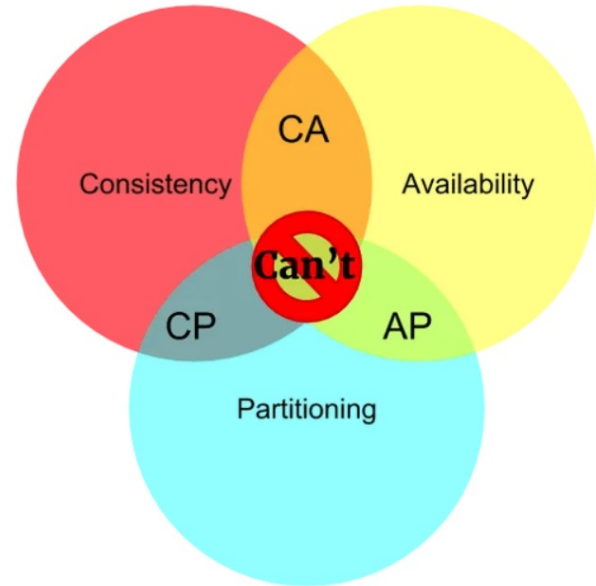
Teorema de CAP

Partition Tolerance: A rede continua operando, mesmo se um número arbitrário de nós estiver falhando



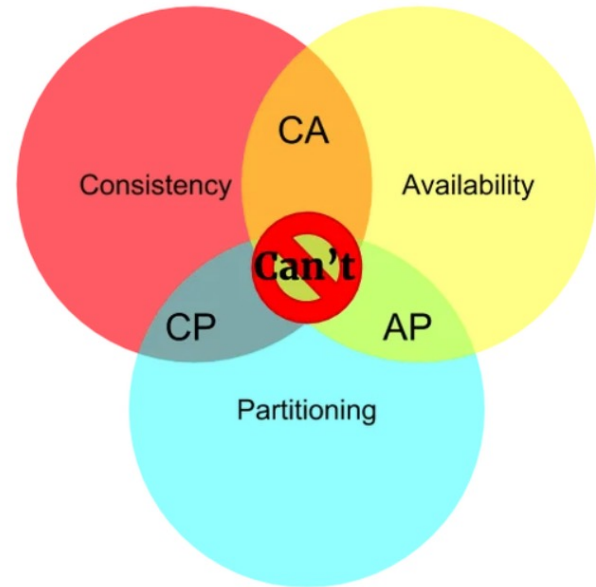
Teorema de CAP

“De acordo com o teorema da CAP, em qualquer rede distribuída é impossível fornecer mais de duas dessas três propriedades como um recurso garantido”.



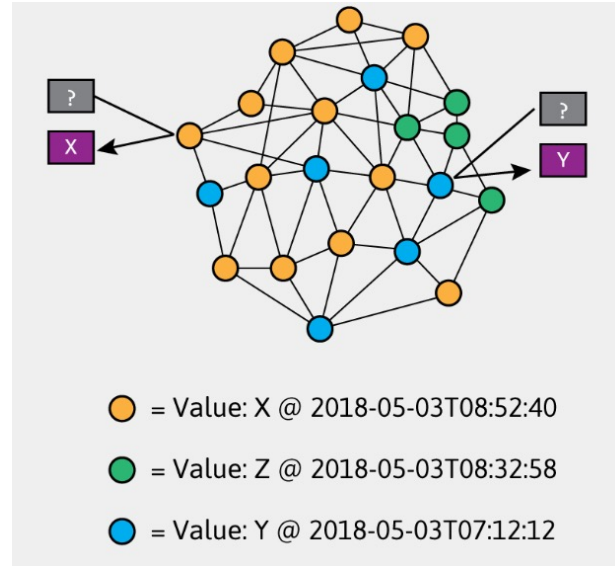
Teorema de CAP em blockchain

*Devido à natureza do armazenamento distribuído, a tolerância a falhas é um fato; sempre haverá nós com falha e/ou inacessíveis na rede (instabilidade da Internet). O teorema do CAP afirma que é preciso escolher entre **C** ou **A** quando na presença de **P** (Partição):*



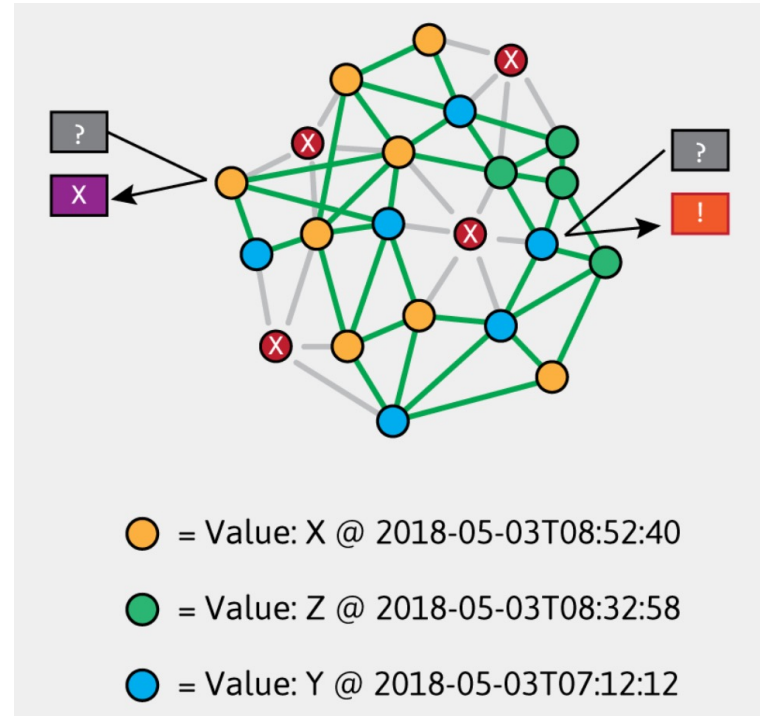
Disponibilidade sobre consistência (A + P)

- Toda solicitação à rede recebe uma resposta;
- mesmo que não haja garantia que ela esteja atualizada;
- devidos nós com falhas.



Consistência sobre disponibilidade (C + P)

- O sistema retornará um erro ou um tempo limite;
- se não for possível garantir a atualização de informações específicas;
- devido a falhas na rede



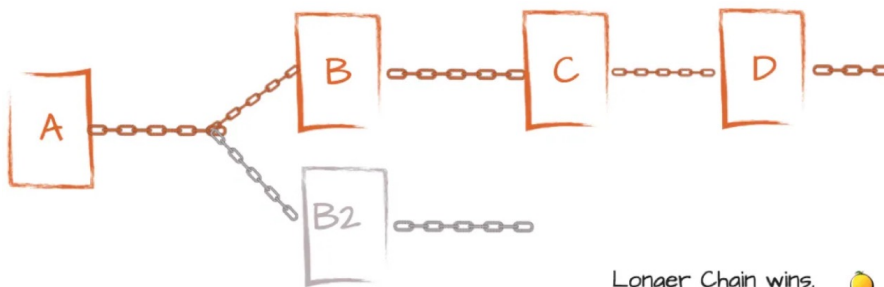
CAP em BD centralizados

- Podem usar **C + A**:
 - pois não precisam se preocupar com a tolerância da partição
 - apenas podem falhar como um todo

Observe que a disponibilidade termina assim que se conecta ao banco de dados distribuído na Internet.

CAP no blockchain do Bitcoin?

- Como as redes blockchain (como Bitcoin) são sistemas descentralizados;
- elas precisam lidar com a tolerância de partição;
- das duas opções restantes, eles escolhem **A** em vez de **C**;
- ou seja, Disponibilidade em vez de Consistência;



Longer Chain wins.
Shorter is "orphaned" 

CAP no blockchain do Bitcoin?

- Se, por exemplo, o Bitcoin preferisse escolher consistência;
- isso significaria que, no caso de um problema de conectividade;
- você não seria capaz de usar, enviar e nem receber o Bitcoin.

Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

Bitcoin vs. Ethereum

Ouro digital →

Valoriza com
auxílio
emergencial



Bitcoin vs Ethereum : Trendy Competition of ...
techbriefstuff.com

← **Plataforma de
aplicações
Descentralizadas**

e.g. NFT

Ethereum e Ether

- Ethereum é a rede que acomoda e executa as aplicações descentralizadas
- É composta de:
 - Main network, a rede Ethereum propriamente dita
 - Test network
 - Rapsten network
 - Kovan network
 - Rinkeby network
 - **Goreli network**
 - Localhost

Redes Ethereum

- Todas
 - Mesma forma de armazenar dados
 - Mesma forma de acessar dados
- Main network
 - Moeda “real”
 - Uma única moeda
- Test network
 - Testar os contratos inteligentes
 - Testar atualizações de protocolos
- Redes privadas
 - Usadas para os próprios blockchains
 - Consorciados

Main networks

- Persistentes
- Blockchain “real”
- Há um custo, o Gas

Test networks

- São persistentes, mas os dados podem ser excluídos
- Blockchain “real”, i.e., está acomodada em diversos nodos
- Explorada para software beta release

Redes de desenvolvedores - Ganache

- É um ambiente de teste também
- Mas muito mais rápido, pois é local
- Não há retardo da rede
- Normalmente não é persistente

Ether?

- O combustível (Gas) existe para incentivar a mineração
- Ethereum não pode ser comprado ou vendido
- Ether é:
 - uma criptomoeda,
 - um bem digital que pode ser comercializado
- Ethereum possui várias aplicações
- Gas é usado para atenuar a flutuação

Ganhos do Ether de 01/01 a 15/04

- Mostrar no Google Finance



Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

Prática I

- Instalar o Metamask
 - Carteira do Ethereum
 - Interface da rede Ethereum
- Criar a sua conta no metamask
- Configurar a chave secreta
- Verificar as redes existentes de teste
- Selecione a rede de teste Goerli
- Adicionar Ether na sua conta 1
- Criar a conta 2
- Transferir valor da conta 1 para a conta 2
- Veja que o saldo total não pode ser transferido à conta 2
 - Por quê? Porque existe a taxa do Gas, o qual é cobrado por transação

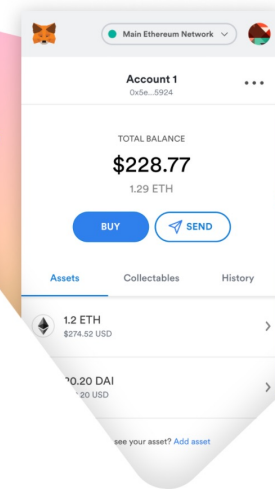
Instalando o Metamask

- Vá ao endereço <https://metamask.io> para baixar o plugin do seu browser

A crypto wallet & gateway to blockchain apps

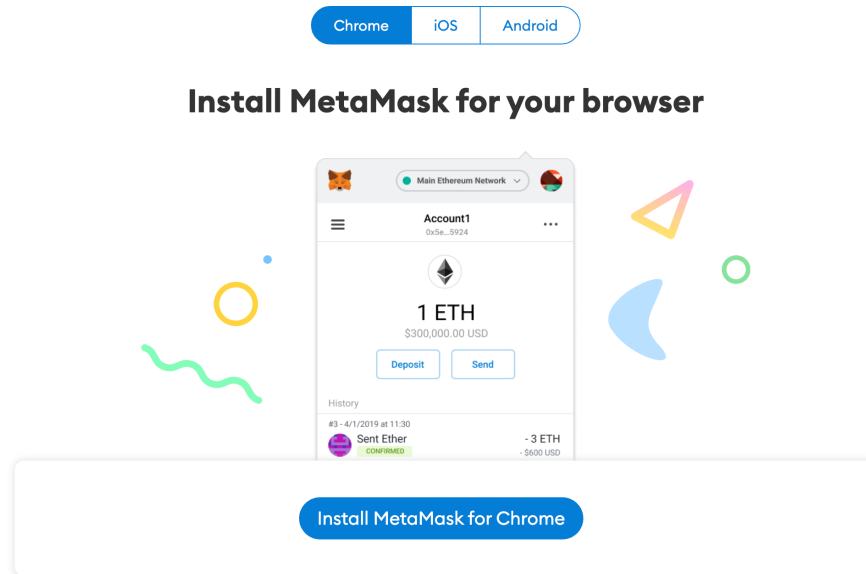
Start exploring blockchain applications in seconds. Trusted by over 1 million users worldwide.

Download now



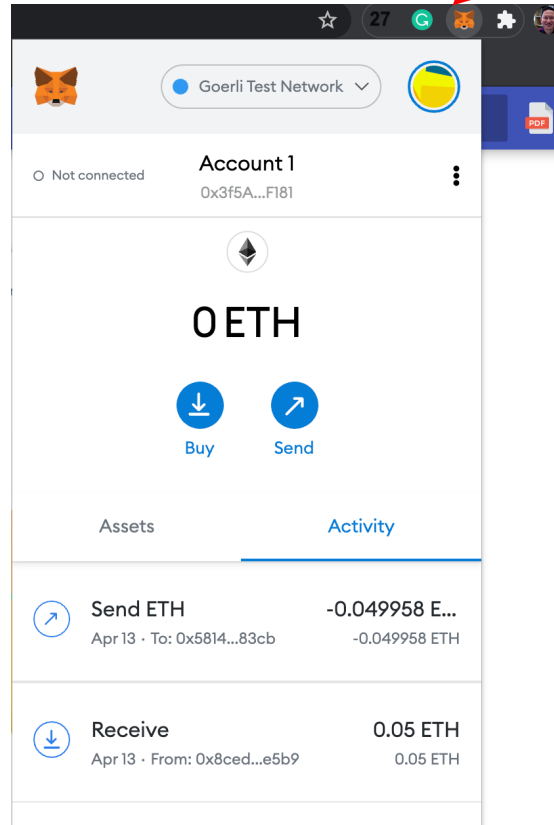
Instalando o Metamask

- Vá ao endereço <https://metamask.io> para baixar o plugin do seu browser



Instalando o Metamask

- Clicar no ícone do Metamask



Criando uma carteira



New to MetaMask?



No, I already have a seed phrase

Import your existing wallet using a 12 word seed phrase

Import wallet



Yes, let's get set up!

This will create a new wallet and seed phrase

Create a Wallet



Criando uma carteira



Help Us Improve MetaMask

MetaMask would like to gather usage data to better understand how our users interact with the extension. This data will be used to continually improve the usability and user experience of our product and the Ethereum ecosystem.

MetaMask will..

- ✓ Always allow you to opt-out via Settings
- ✓ Send anonymized click & pageview events
- ✗ **Never** collect keys, addresses, transactions, balances, hashes, or any personal information
- ✗ **Never** collect your full IP address
- ✗ **Never** sell data for profit. Ever!

No Thanks

I Agree

This data is aggregated and is therefore anonymous for the purposes of General Data Protection Regulation (EU) 2016/679. For more information in relation to our privacy practices, please see our [Privacy Policy here](#).

Crie uma senha para a carteira

- A carteira pode possuir várias contas:
 - Conta corrente
 - Poupança
 - Aposentadoria, etc.
 - São alguns exemplos



< Back

Create Password

New password (min 8 chars)

Confirm password

I have read and agree to the [Terms of Use](#)

Create

Armazenando a frase secreta

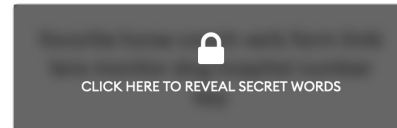
- A frase secreta é formada por 12 palavras
- As 12 palavras formam a sua chave privada e pública
- É a identificação da sua carteira
- Perdeu, já Elvis 😞
- Deve ser mantido em segurança e SECRETAMENTE



Secret Backup Phrase

Your secret backup phrase makes it easy to back up and restore your account.

WARNING: Never disclose your backup phrase. Anyone with this phrase can take your Ether forever.



[Remind me later](#)

[Next](#)

Tips:

Store this phrase in a password manager like 1Password.

Write this phrase on a piece of paper and store in a secure location. If you want even more security, write it down on multiple pieces of paper and store each in 2 - 3 different locations.

Memorize this phrase.

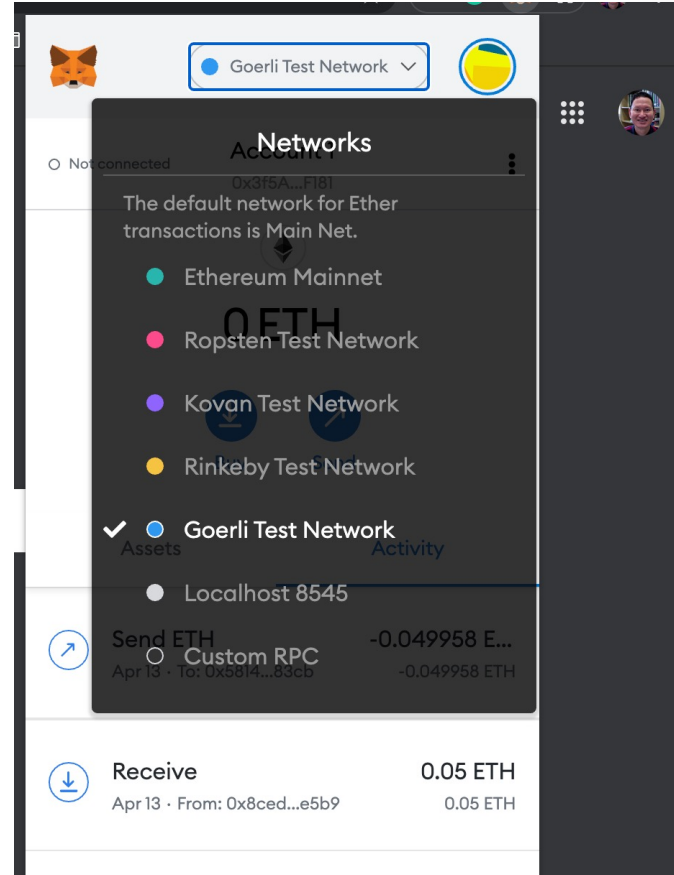
[Download this Secret Backup Phrase and keep it stored safely on an external encrypted hard drive or storage medium.](#)

Sumário

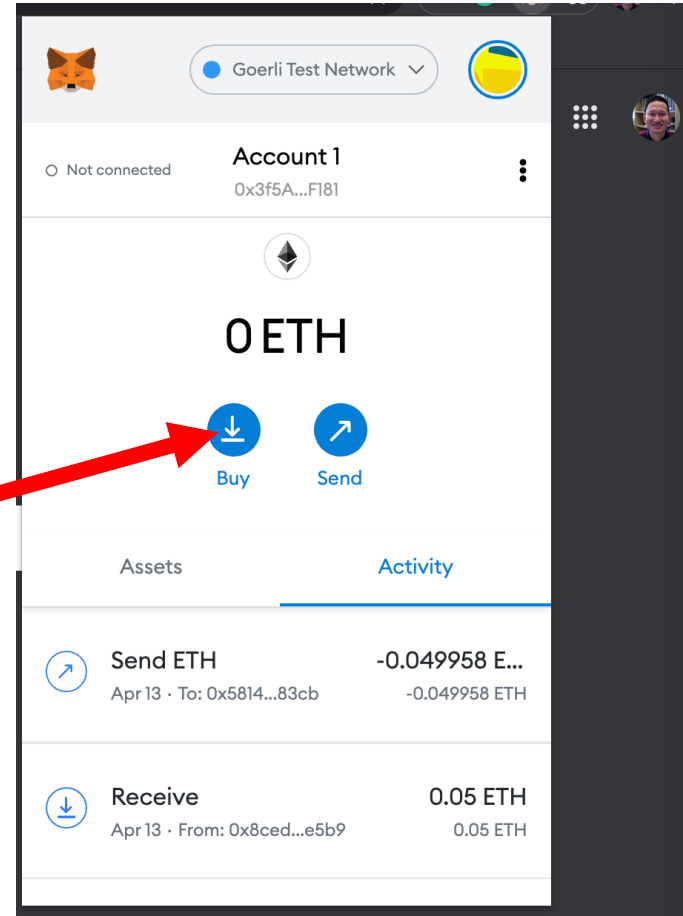
- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

Executando uma transação

- Entre no Goerli test network
- A rede Ropsten teve alguns bugs e por isso a rede Goerli foi selecionada



Comprando Ether



Comprando Ether


Deposit Ether ×

To interact with decentralized applications using MetaMask, you'll need Ether in your wallet.

Directly Deposit Ether

If you already have some Ether, the quickest way to get Ether in your new wallet by direct deposit.

[View Account](#)



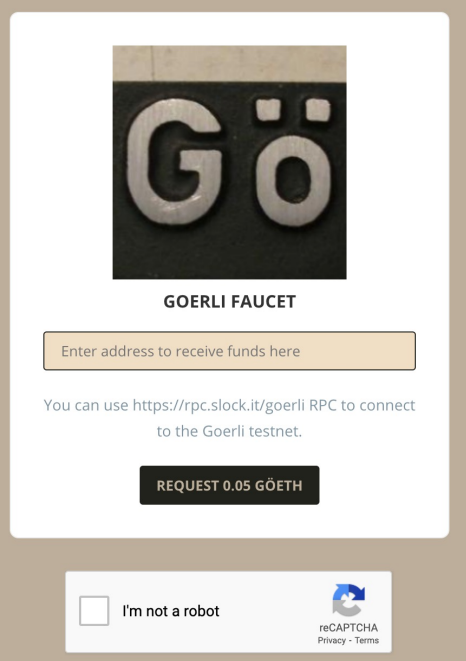
Test Faucet

Get Ether from a faucet for the Goerli

[Get Ether](#)

Comprando Ether

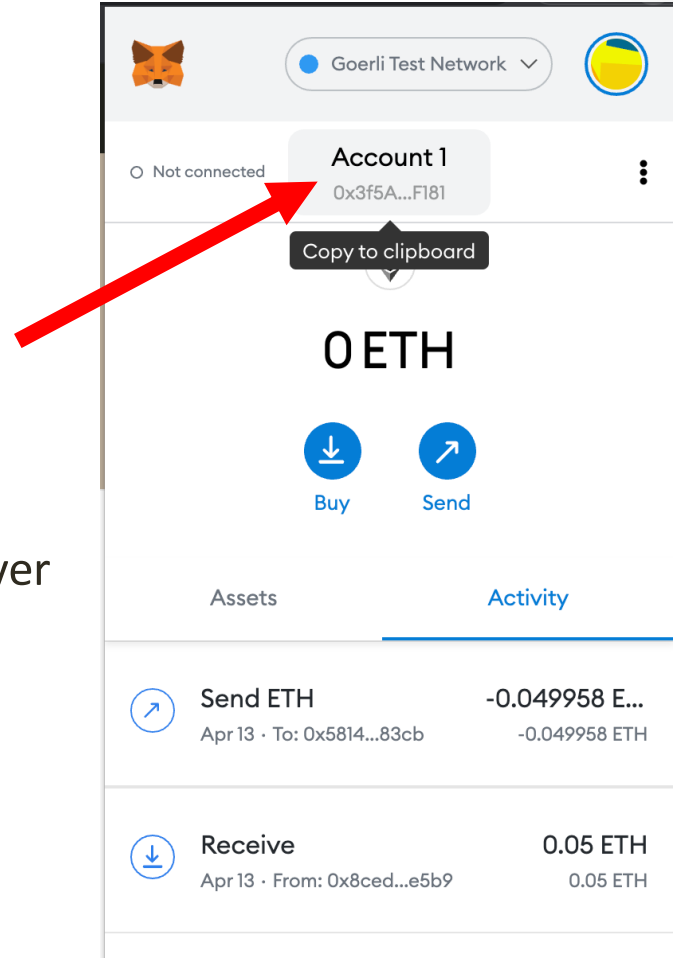
- Uma página da rede de teste é exibida solicitando a compra de Ether de teste
- Pegar a sua identificação na carteira



The screenshot shows the Goerli Faucet interface. At the top, there is a large image of the letters 'Gö' in a stylized font. Below this, the text 'GOERLI FAUCET' is displayed. A text input field contains the placeholder text 'Enter address to receive funds here'. Below the input field, there is a line of text: 'You can use <https://rpc.slock.it/goerli> RPC to connect to the Goerli testnet.' At the bottom of the main content area, there is a dark button with the text 'REQUEST 0.05 GÖETH'. At the very bottom of the page, there is a reCAPTCHA widget with the text 'I'm not a robot' and the reCAPTCHA logo.

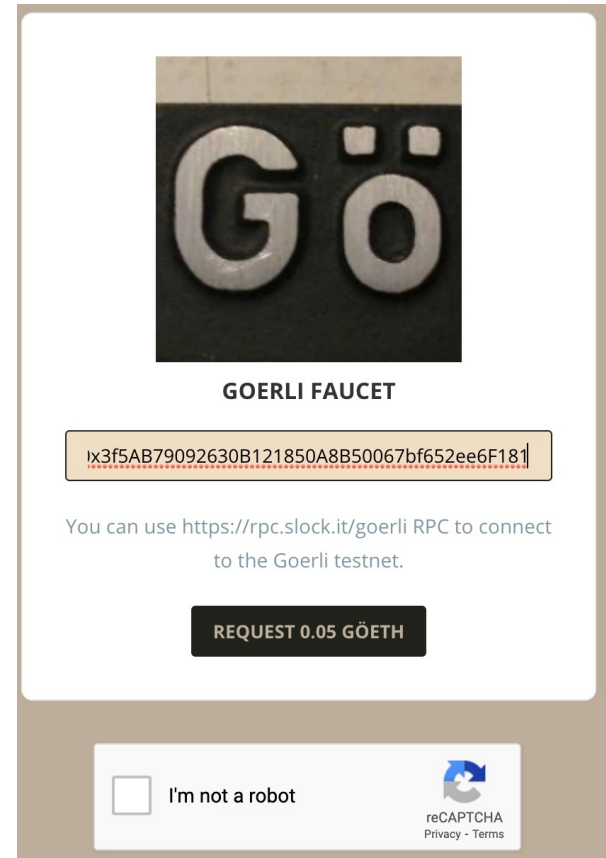
Comprando Ether

- Pegar a sua identificação na carteira
- Copiar o endereço
 - Chave pública
 - Identificação da conta
 - Lembrando que em uma carteira pode haver várias contas



Comprando Ether

- Colar o endereço da conta copiado do Metamask
- Solicitar ao Goerli
- Demora um pouco porque o valor é gerado e atualizado em toda rede Goerli



GOERLI FAUCET

ix3f5AB79092630B121850A8B50067bf652ee6F18

You can use <https://rpc.slock.it/goerli> RPC to connect to the Goerli testnet.

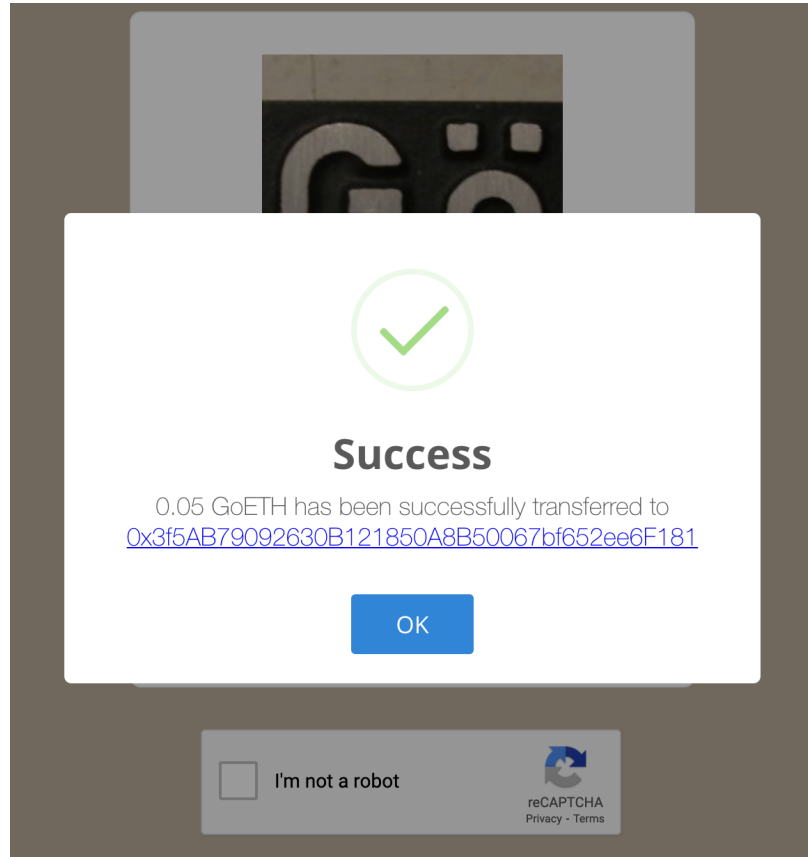
REQUEST 0.05 GÖETH

I'm not a robot

reCAPTCHA
Privacy - Terms

Comprando Ether

- Pronto! Compra efetuada.



Comprando ETH no Goerli

<https://cutt.ly/pXXX9zt>

<https://goerli-faucet.pk910.de/>

Comprando ETH no Sepolia

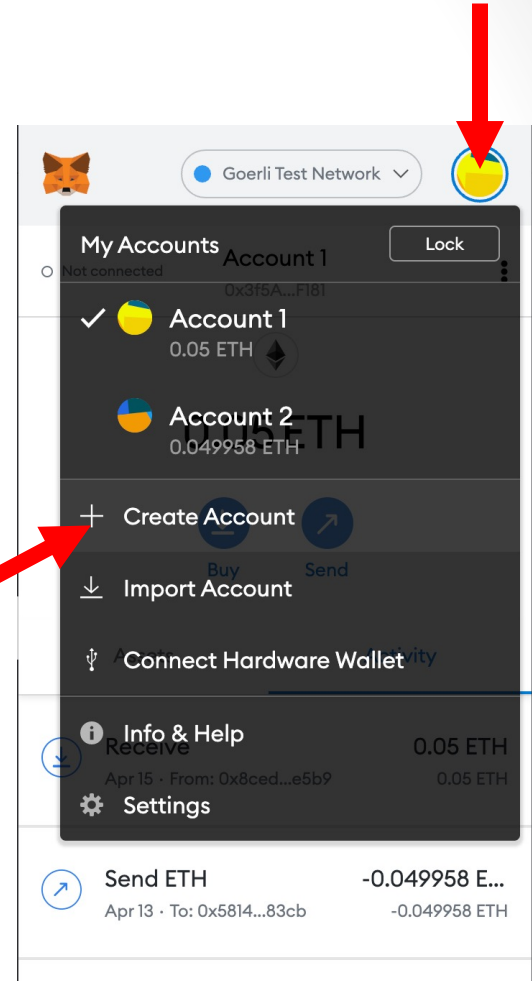
<https://sepoliafaucet.com/>

Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V

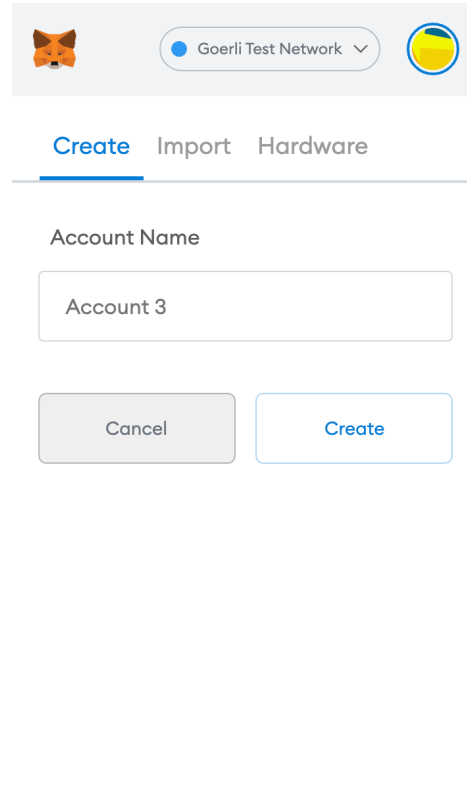
Abrindo uma segunda conta

- Criando uma segunda conta
- A primeira já vem com a carteira
- Abra o Metamask e clique em criar conta



Criando a conta Account 3

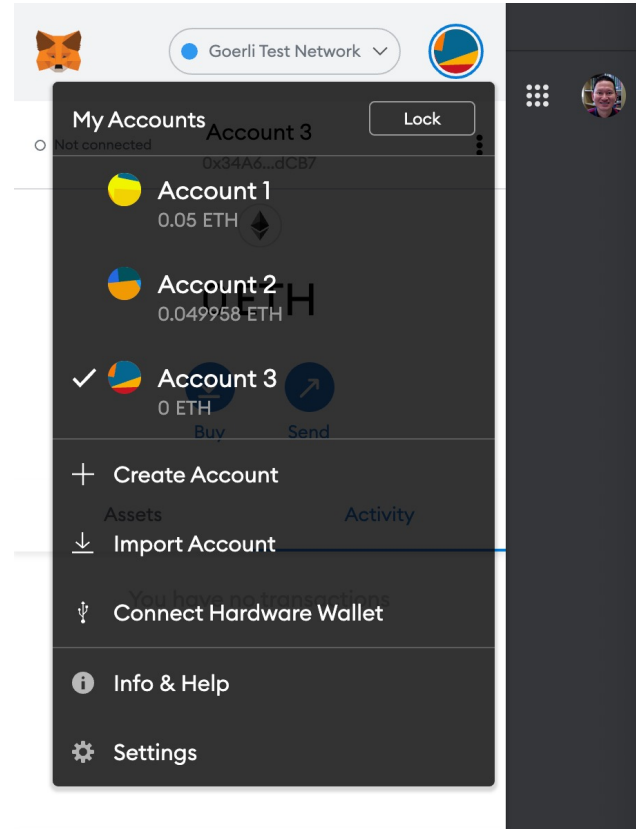
- Crie a conta Account 3



The screenshot shows a web interface for creating an account. At the top, there is a header with a fox icon on the left, a dropdown menu labeled "Goerli Test Network" with a downward arrow, and a yellow circular icon on the right. Below the header, there are three tabs: "Create" (which is active and underlined), "Import", and "Hardware". Under the "Create" tab, there is a label "Account Name" above a text input field containing the text "Account 3". At the bottom of the form, there are two buttons: a grey "Cancel" button on the left and a blue "Create" button on the right.

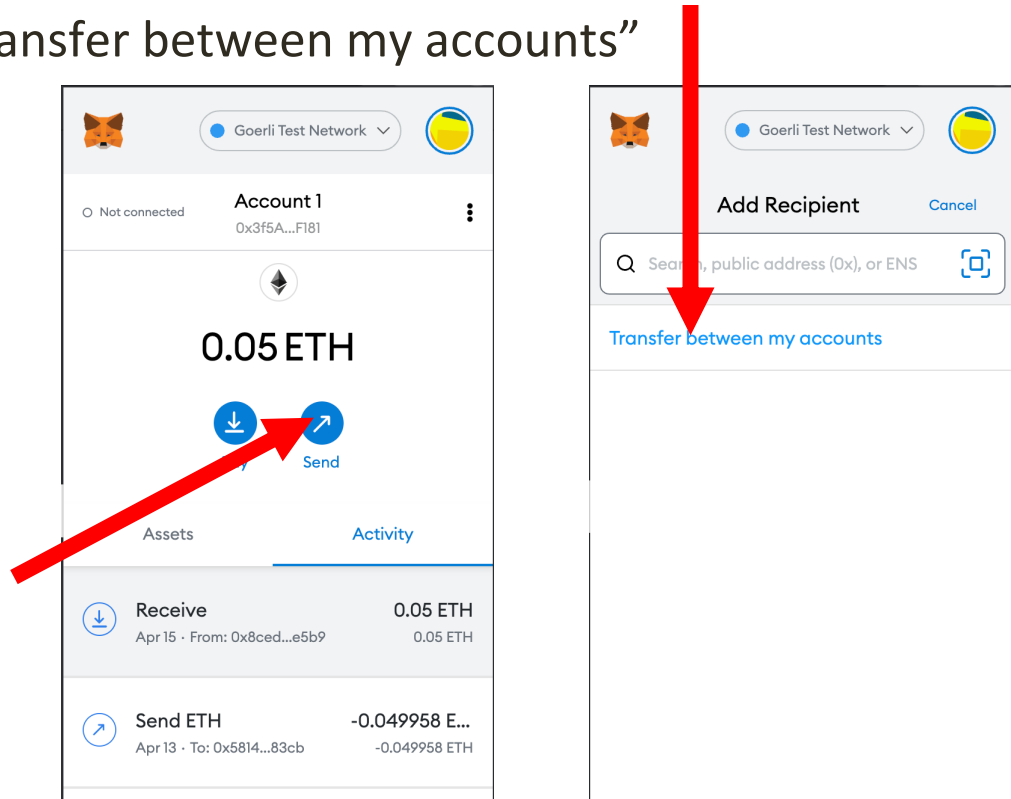
Criando a conta Account 3

- Agora você terá três contas
- Estas contas foram criadas porque realizei vários testes
- Você irá criar a conta Account 2
- Sem saldo apenas no Account 3



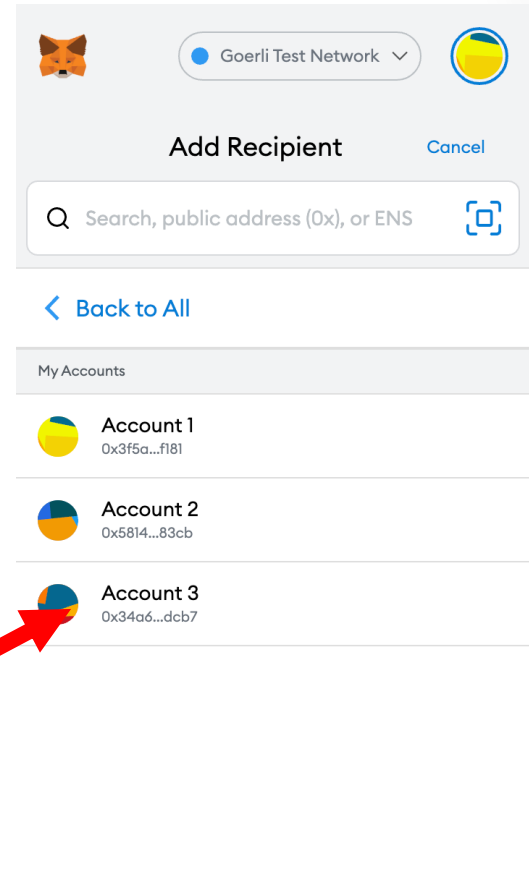
Transferindo valores

- Clique no “Send” e no “Transfer between my accounts”



Transferindo valores

- Selecione o “Account 2” como a conta de crédito



Transferindo valores

- Clique no “Max” para indicar o valor máximo a ser transferido
- Depois Clique “Next” e confirme a transação

Goerli Test Network

Send ETH Cancel

Account 3
0x34a611d00e2a3349bb055a0c3f2ee9bb51e1dcb7

Asset: ETH Balance: 0.05 ETH

Amount: 0 ETH No Conversion Rate Available

Transaction Fee: Gas Price (GWEI) 2,0267 Gas Limit 21000

Cancel Next

Goerli Test Network

Account 1 → Account 3

SENT ETHER

0.049957

GAS FEE 0.000043 No Conversion Rate Available

Gas Price (GWEI) 2,0267 Gas Limit 21000

AMOUNT + GAS FEE

TOTAL 0.05 No Conversion Rate Available

Reject Confirm

Transferindo valores

- Transferindo...
- Toma tempo por conta da mineração
- Na rede de teste Goerli
 - Rede blockchain real

The screenshot displays a mobile wallet interface for the Goerli Test Network. At the top, there is a fox icon and a dropdown menu set to 'Goerli Test Network'. Below this, the account is identified as 'Account 1' with the address '0x3f5A...F181'. The current balance is shown as '0.05 ETH'. There are two buttons: 'Buy' (with a download icon) and 'Send' (with an arrow icon). The 'Activity' tab is selected, showing a 'Queue (1)' with one pending transaction: 'Send ETH' for -0.049957 ETH to address '0x34a6...dcb7'. The transaction is marked as 'Pending' and has 'Speed Up' and 'Cancel' buttons. A red arrow points to the 'Send ETH' transaction icon.

Tranferindo valores

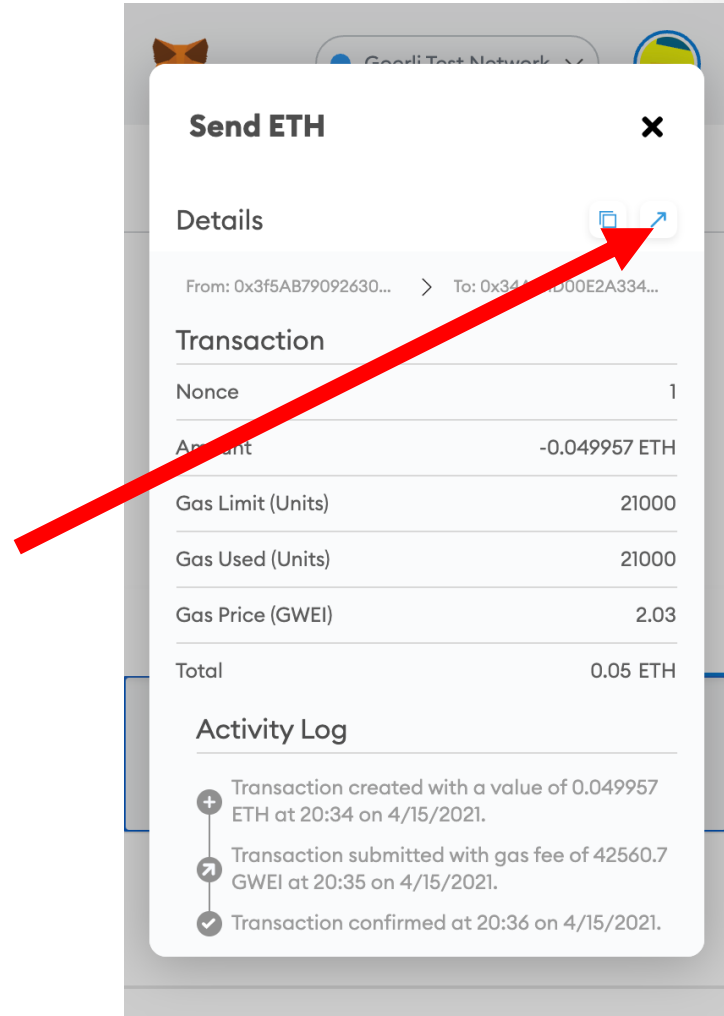
- Transação realizada com sucesso
- Clicar na transação

The screenshot displays a mobile wallet interface for the Goerli Test Network. At the top, there is a fox logo and a dropdown menu set to 'Goerli Test Network'. Below this, the account is identified as 'Account 1' with the address '0x3f5A...F181'. The main display shows '0 ETH' with a diamond icon above it. There are two buttons: 'Buy' (with a downward arrow) and 'Send' (with an upward arrow). Below the main display, there are two tabs: 'Assets' and 'Activity'. The 'Activity' tab is selected, showing a list of transactions:

Transaction Type	Date	Details	Amount
Send ETH	Apr 15	To: 0x34a6...dcb7	-0.049957 ETH
Receive	Apr 15	From: 0x8ced...e5b9	0.05 ETH

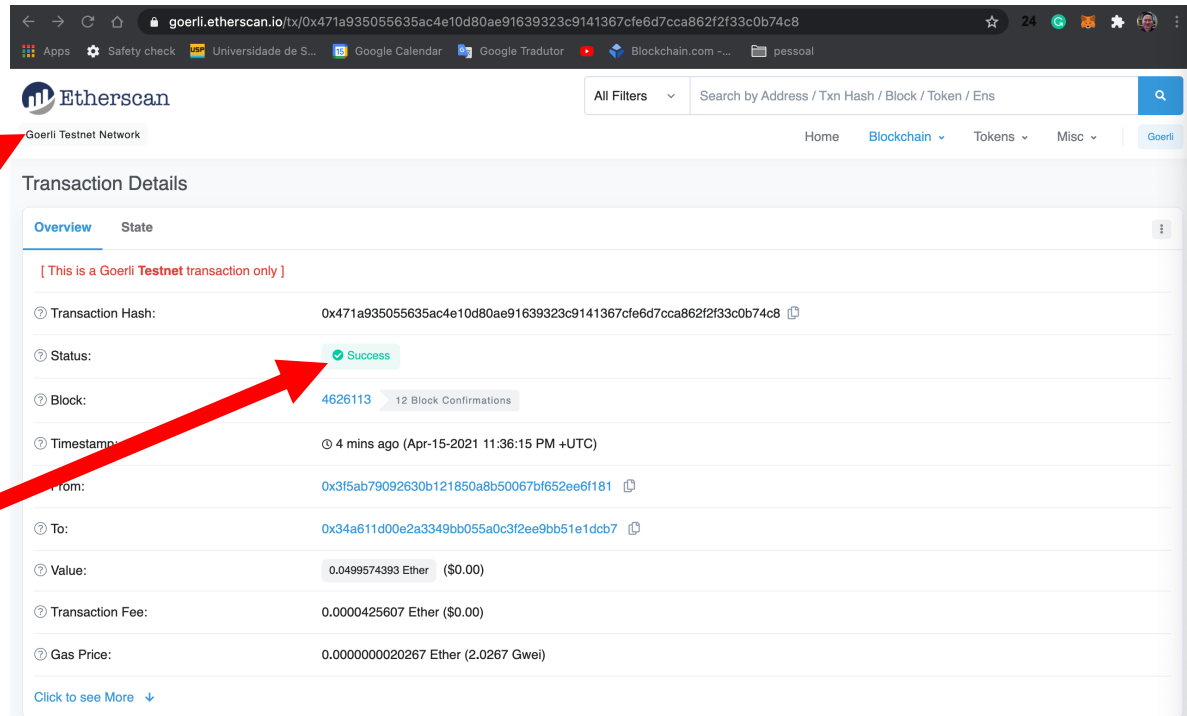
Transferindo valores

- Transação realizada com sucesso
- Clicar na transação
- Vamos abrir a transação no Etherscan



Transferindo valores

- Confirmação da transação efetuada



The screenshot shows the Etherscan interface for a transaction on the Goerli Testnet. The transaction is confirmed as successful. Two red arrows point to the 'Goerli Testnet Network' label and the 'Success' status.

Transaction Details	
Overview	State
[This is a Goerli Testnet transaction only]	
Transaction Hash:	0x471a935055635ac4e10d80ae91639323c9141367cfe6d7cca862f2f33c0b74c8
Status:	Success
Block:	4626113 12 Block Confirmations
Timestamp:	4 mins ago (Apr-15-2021 11:36:15 PM +UTC)
From:	0x3f5ab79092630b121850a8b50067b6f52ee6f181
To:	0x34a611d00e2a3349bb055a0c3f2ee9bb51e1dcb7
Value:	0.0499574393 Ether (\$0.00)
Transaction Fee:	0.0000425607 Ether (\$0.00)
Gas Price:	0.0000000020267 Ether (2.0267 Gwei)

Como os blocos inter-relacionam - Etherscan

- Entre no <https://etherscan.io>
- Clique no último bloco
- Veja como os blocos inter-relacionam
 - Veja que os hashes devem ser iguais
 - É a ligação entre os blocos

Block #12284284

Flashbots Unconventional Ordering

Sponsored: CryptoGames -The best gaming site to play with your Ether! [Have fun!](#)

Overview Comments

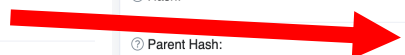
Block Height:	12284284
Timestamp:	2 mins ago (Apr-21-2021 03:07:53 PM +UTC)
Transactions:	230 transactions and 36 contract internal transactions in this block
Mined by:	0x5a0b54d5dc17e0aacd383d2db43b0a0d3e029c4c (Spark Pool) in 7 secs
Block Reward:	4.93650666103815497 Ether (2 + 2.93650666103815497)
Uncles Reward:	0
Difficulty:	6,892,868,222,436,416
Total Difficulty:	23,586,276,423,505,505,666,750
Size:	55,912 bytes
Gas Used:	14,595,721 (99.93%)
Gas Limit:	14,606,163
Extra Data:	eth-pro-hzo-1006 (Hex:0x6574682d70726f2d687a6f2d74303036)
Hash:	0x62254469696a8a66550839155116754caaf84cc29e4710f953f5ad50a0f0742f
Parent Hash:	0xfbb30a5ac15cbec84cd40b438c548fb528cd7efb6e6b5cd8e02a8b23c4ed8fb75
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6cc41ad312451b948a7413f0a142fd40d49347
StateRoot:	0x1db922f5b8c8fab021e2570c77b0f234a469899c4463b907ea648c54bffa442f
Nonce:	0x9cdc5a1ddb9b1981

Block #12284285

Sponsored: Convenient & Safe: Join Fairspin to Receive Up to 170 ETH, 170 Free Spins, and 18% Cashback.

Overview Comments

Block Height:	12284285
Timestamp:	3 mins ago (Apr-21-2021 03:08:06 PM +UTC)
Transactions:	242 transactions and 48 contract internal transactions in this block
Mined by:	0x3ecef08d0e2dad803847e052249bb4f8bf2d5bb (MiningPoolHub) in 13 secs
Block Reward:	4.629755875697516804 Ether (2 + 2.629755875697516804)
Uncles Reward:	0
Difficulty:	6,892,869,296,178,240
Total Difficulty:	23,586,283,316,374,801,844,990
Size:	54,801 bytes
Gas Used:	14,575,959 (99.89%)
Gas Limit:	14,591,901
Extra Data:	seo6 (Hex:0x73656f36)
Hash:	0x59f8c68df27a285a3083e7c3b8ae032b26f18b0e614692b388e69fe837f00c5
Parent Hash:	0x62254469696a8a66550839155116754caaf84cc29e4710f953f5ad50a0f0742f
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6cc41ad312451b948a7413f0a142fd40d49347
StateRoot:	0xa4ec06e5e28db0caf6915623b11de436f28e036a25c281cf37b53bde7e8b5f03
Nonce:	0xa278dad3c7a52d4a

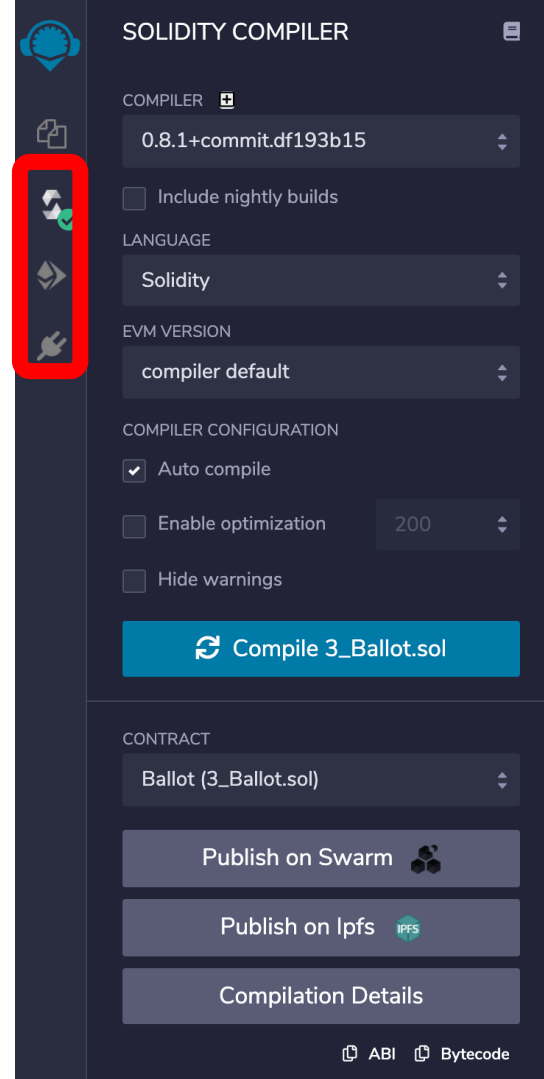


Sumário


- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V
- Prática VI


Configurando Remix

- Remix é uma IDE Solidity para codificar, compilar e executar contratos inteligentes Ethereum
- Entre no Remix Web IDE
<http://remix.ethereum.org>
- O que você precisa no Remix:
 - Compiler
 - Deploy & Run Transaction
 - Plugins




SOLIDITY COMPILER

COMPILER 


0.8.1+commit.df193b15 

Include nightly builds

LANGUAGE


Solidity 

EVM VERSION


compiler default 

COMPILER CONFIGURATION


Auto compile


Enable optimization 200 


Hide warnings

 Compile 3_Ballot.sol



CONTRACT

Ballot (3_Ballot.sol) 

 Publish on Swarm

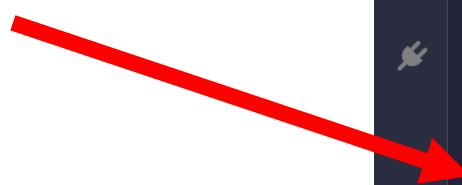
 Publish on Ipfs

Compilation Details

 ABI  Bytecode

Na aba Compiler

- Sugestão: ativar o Auto-compile

The image shows the right-hand sidebar of the Solidity Compiler interface. At the top, it says 'SOLIDITY COMPILER'. Below that, there are several sections: 'COMPILER' with a dropdown menu set to '0.8.1+commit.df193b15'; 'LANGUAGE' with a dropdown menu set to 'Solidity'; 'EVM VERSION' with a dropdown menu set to 'compiler default'; and 'COMPILER CONFIGURATION' which contains three checkboxes: 'Auto compile' (checked), 'Enable optimization' (unchecked, with a dropdown set to '200'), and 'Hide warnings' (unchecked). Below these settings is a large blue button that says 'Compile 3_Ballot.sol'. At the bottom of the sidebar, there is a 'CONTRACT' section with a dropdown menu set to 'Ballot (3_Ballot.sol)', and three buttons: 'Publish on Swarm', 'Publish on Ipfs', and 'Compilation Details'. At the very bottom right, there are links for 'ABI' and 'Bytecode'.

SOLIDITY COMPILER

COMPILER

0.8.1+commit.df193b15

Include nightly builds

LANGUAGE

Solidity

EVM VERSION

compiler default

COMPILER CONFIGURATION

Auto compile

Enable optimization 200

Hide warnings

Compile 3_Ballot.sol

CONTRACT

Ballot (3_Ballot.sol)

Publish on Swarm

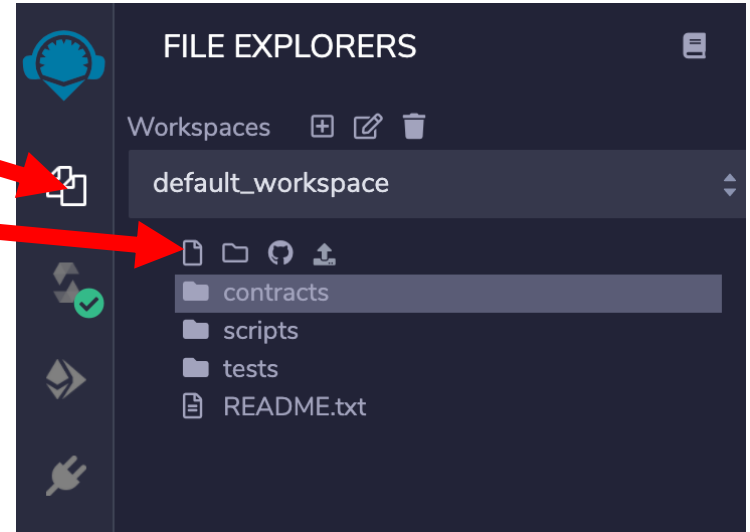
Publish on Ipfs

Compilation Details

ABI Bytecode

Criando o primeiro contrato

- Clicar no “File explorers”
- Depois no ícone do arquivo



Criar o contrato MyContract.sol

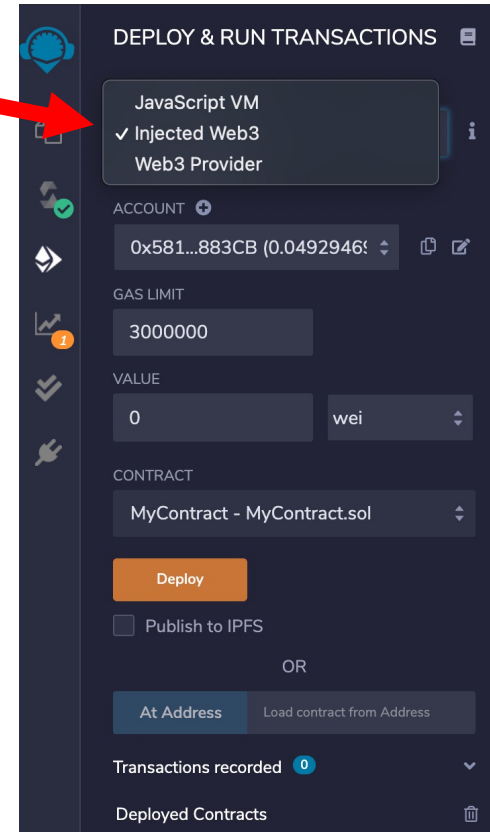
```
// SPDX-License-Identifier: GPL-3.0
```

```
pragma solidity ^0.8.1;
```

```
contract MyContract {  
    string public myString = 'hello world';  
}
```

Carregando o MyContract.sol

- Mudar o ambiente para Injected Web 3



The screenshot shows the 'DEPLOY & RUN TRANSACTIONS' panel. The environment selection dropdown is open, showing the following options:

- JavaScript VM
- ✓ Injected Web3
- Web3 Provider

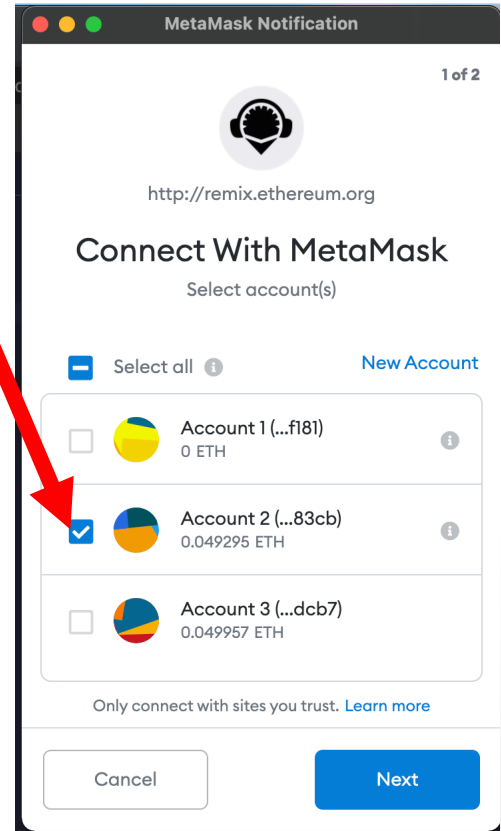
The 'Injected Web3' option is selected, indicated by a checkmark. Below the environment selection, the following fields are visible:

- ACCOUNT: 0x581...883CB (0.0492946)
- GAS LIMIT: 3000000
- VALUE: 0 wei
- CONTRACT: MyContract - MyContract.sol

At the bottom of the panel, there is a 'Deploy' button, a checkbox for 'Publish to IPFS', and an 'OR' separator. Below the separator, there are two buttons: 'At Address' and 'Load contract from Address'. At the very bottom, there is a 'Transactions recorded' section showing 0 transactions and a 'Deployed Contracts' section.

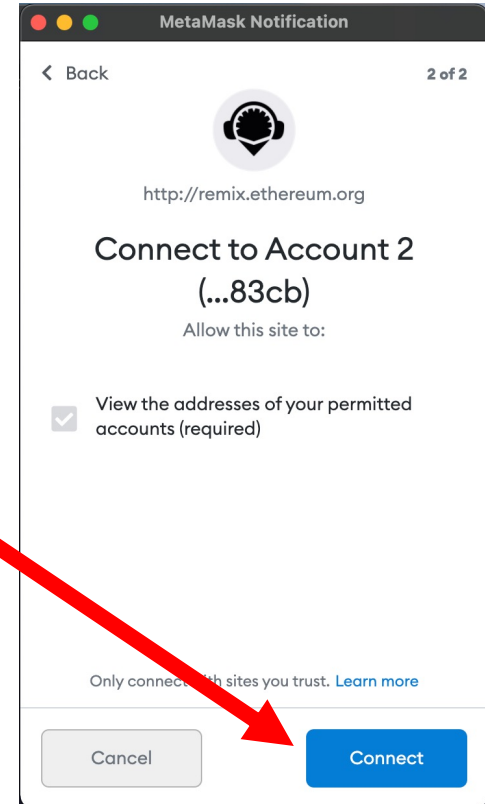
Selecionando a conta do Metamask

- Selecionar a conta que pagará a taxa em Gas
- Depois clicar em “Next”



Selecionando a conta do Metamask

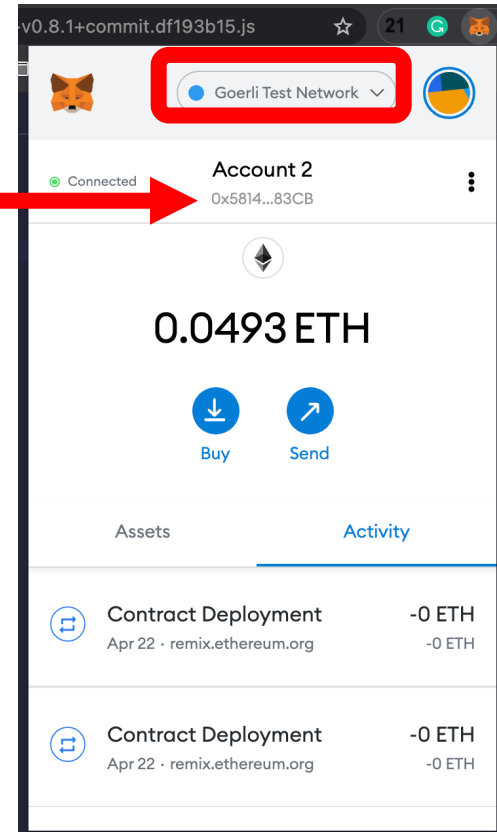
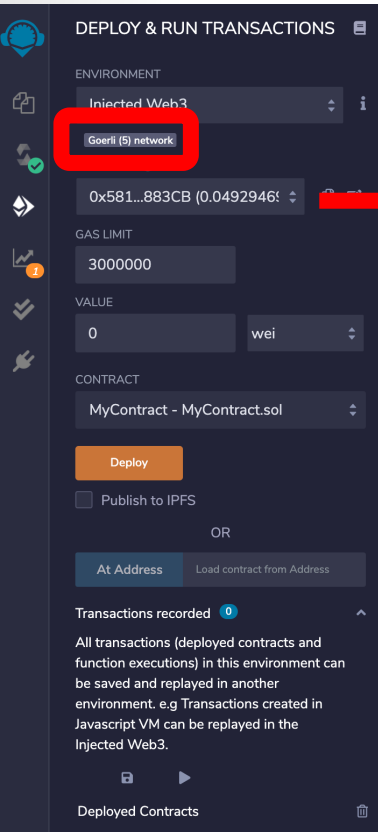
- Conectar à conta



Verificando a identidade da conta

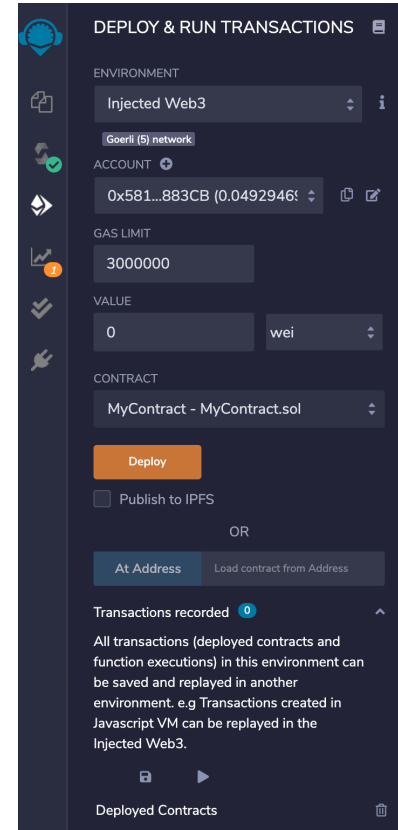
- Certificando que as duas contas são as mesmas

- Verificar o uso da rede Goerli
 - No Metamaks
 - No Remix



Deploy do contrato

- Basta clicar no Deploy do Remix
- Isso ativará o Metamask para confirmar o pagamento da transação em Gas



The screenshot shows the 'DEPLOY & RUN TRANSACTIONS' interface in the Remix IDE. The environment is set to 'Injected Web3'. The account is 'Goerli (5) network' with address '0x581...883CB (0.0492946)'. The gas limit is set to 3,000,000. The value is 0 wei. The contract selected is 'MyContract - MyContract.sol'. There is a 'Deploy' button and a checkbox for 'Publish to IPFS'. Below this, there is an 'OR' section with a button 'At Address' and a sub-label 'Load contract from Address'. At the bottom, it shows 'Transactions recorded 0' and a message: 'All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.' There are also icons for 'Deployed Contracts' and a trash icon.

Confirmando o pagamento da taxa

- Clicar no “Confirm”
- Depois de confirmado, uma mensagem será exibida no Remix



```
0  listen on network Search with transaction hash or address  
[block:4664387 txIndex:4] from: 0x581...883CB to: MyContract.(constructor) value: 0 wei  
data: 0x608...10033 logs: 0 hash: 0x16b...320e1 Debug
```

MetaMask Notification

Goerli Test Network

Account 2 → New Contract

http://remix.ethereum.org

CONTRACT DEPLOYMENT

0

DETAILS DATA

GAS FEE 0.000332
No Conversion Rate Available

Gas Price (GWEI) 1,6533 Gas Limit 200601

AMOUNT + GAS FEE

TOTAL 0.000332
No Conversion Rate Available

Reject Confirm

Interação com o MyContract

- Clicar na caixa dropdown “MyContract”

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT
Injected Web3

Goerli (5) network

ACCOUNT
0x581...883CB (0.0489630)

GAS LIMIT
3000000

VALUE
0 wei

CONTRACT
MyContract - MyContract.sol

Deploy

Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 1

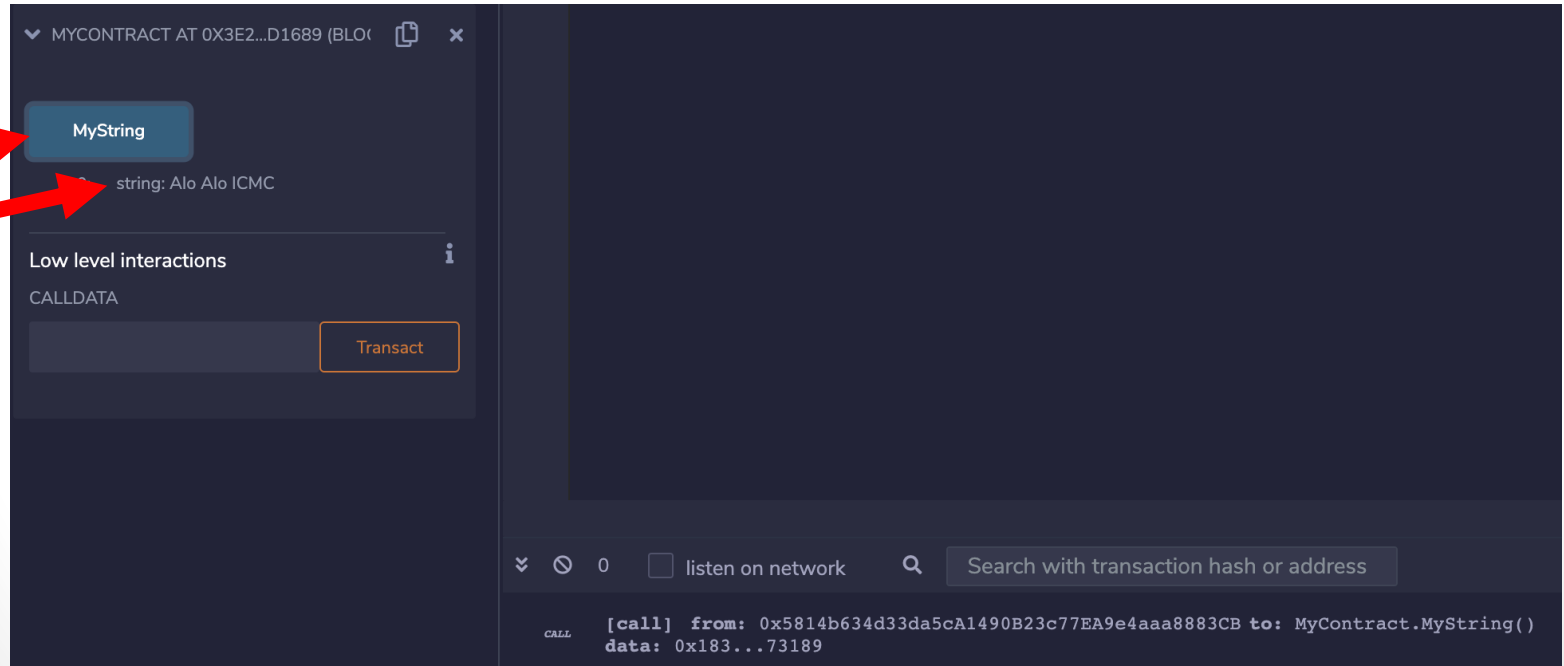
All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.

Deployed Contracts

MYCONTRACT AT 0X3E2...D1689 (BLOC)

Executando o MyContract

- Clique no MyString (na parte inferior da página)
- Isso executará o contrato e exibirá a mensagem



MYCONTRACT AT 0X3E2...D1689 (BLOC)

MyString

string: Alo Alo ICMC

Low level interactions

CALLDATA

Transact

listen on network

Search with transaction hash or address

`CALL [call] from: 0x5814b634d33da5cA1490B23c77EA9e4aaa8883CB to: MyContract.MyString() data: 0x183...73189`

Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V
- Prática VI

Usando Remix VM London

- O JavaScript VM é um ambiente blockchain simulado
- Vantagem
 - É rápido e não precisa se conectar a uma conta
- Desvantagem
 - Só funciona enquanto a aba do browser estiver aberto
 - Não guarda os estados (p.ex., variáveis e pilhas de execução)
 - Se você recarregar o contrato, os estados são perdidos
 - Se fizer um “refresh” da página, os dados serão perdidos
- É ideal para codificar e testar

Iniciando o JavaScript VM

- Clique no ambiente

The screenshot shows the Remix IDE interface. On the left, the 'DEPLOY & RUN TRANSACTIONS' panel is open. The 'ENVIRONMENT' section shows 'JavaScript VM' selected with a checkmark. Below it, 'Injected Web3' and 'Web3 Provider' are listed. The 'GAS LIMIT' is set to 3000000 and 'VALUE' is 0 wei. The 'CONTRACT' section shows 'MyContract - MyContract.sol' selected. A red arrow points to the 'Deploy' button. Below the 'Deploy' button, there is a checkbox for 'Publish to IPFS' and an 'OR' section with 'At Address' and 'Load contract from Address' options. At the bottom, it says 'Transactions recorded 0' and 'Deployed Contracts'.

```
1 // SPDX-License-Identifier: GPL-3.0
2
3 pragma solidity ^0.8.1;
4
5 contract MyContract {
6     string public MyString = 'Alo Alo ICMC';
7 }
```

- Depois no Deploy

Executando no JavaScript VM

- Clique no MyString
- Veja a execução do contrato

MYCONTRACT AT 0XD91...39138 (MEM)

MyString

string: Alo Alo ICMC

Low level interactions

CALLDATA

Transact

listen on network

Search with transaction hash or address

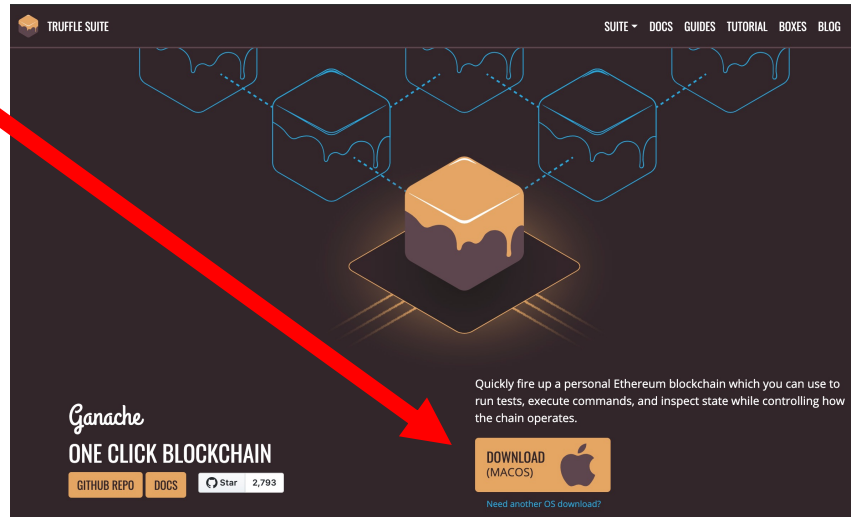
```
[call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: MyContract.MyString()  
data: 0x183...73189
```

Sumário

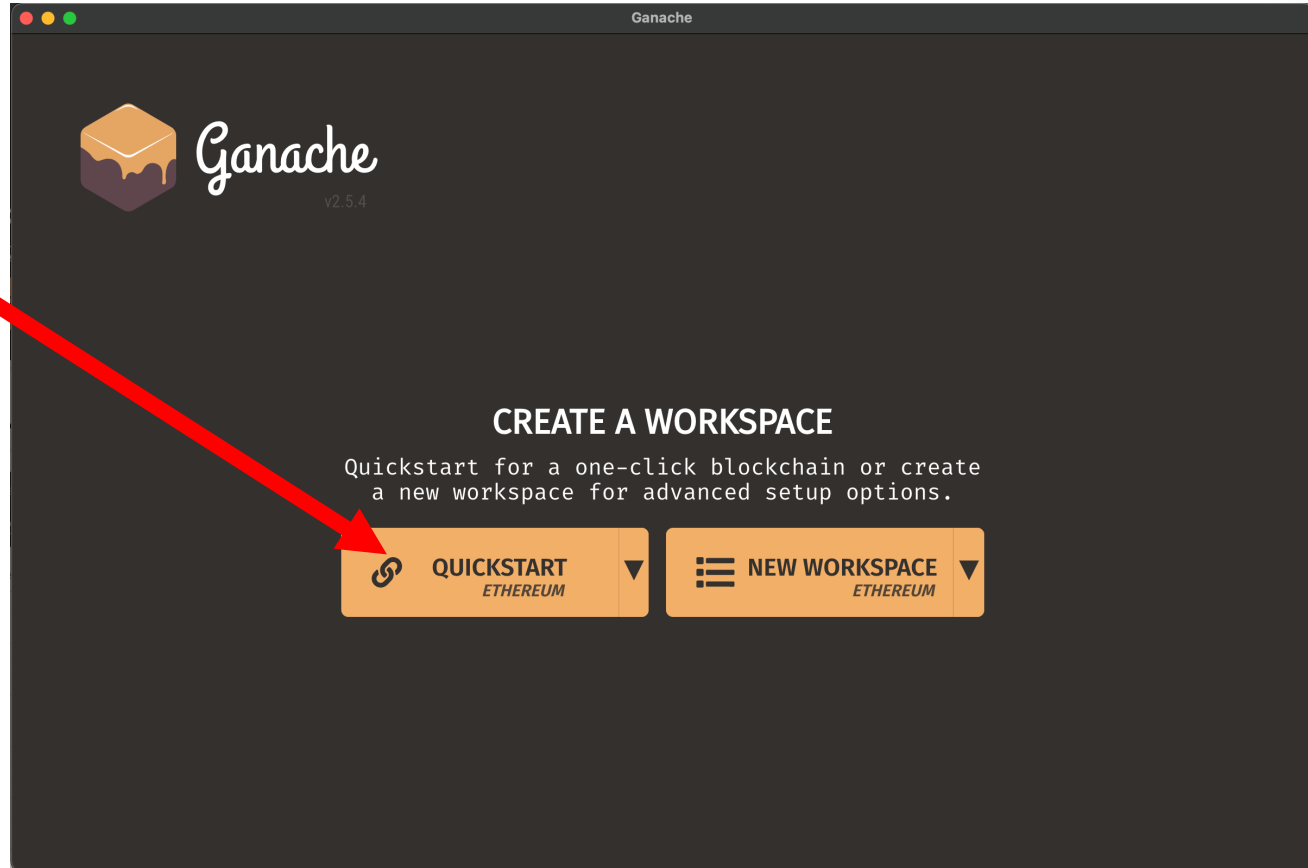
- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V (Usando Ganache Provider)
- Prática VI

Agora usando o Web3 Provider

- Neste método, o ambiente não está no browser
- Usa-se um software que não seja o browser, e.g. Ganache
- Irei usar o Ganache
 - Pode ser baixado do <https://www.trufflesuite.com/ganache>
 - Para vários SOs; eu uso o MAC/OS
- Muito usado para desenvolvimento
- Principalmente para testes

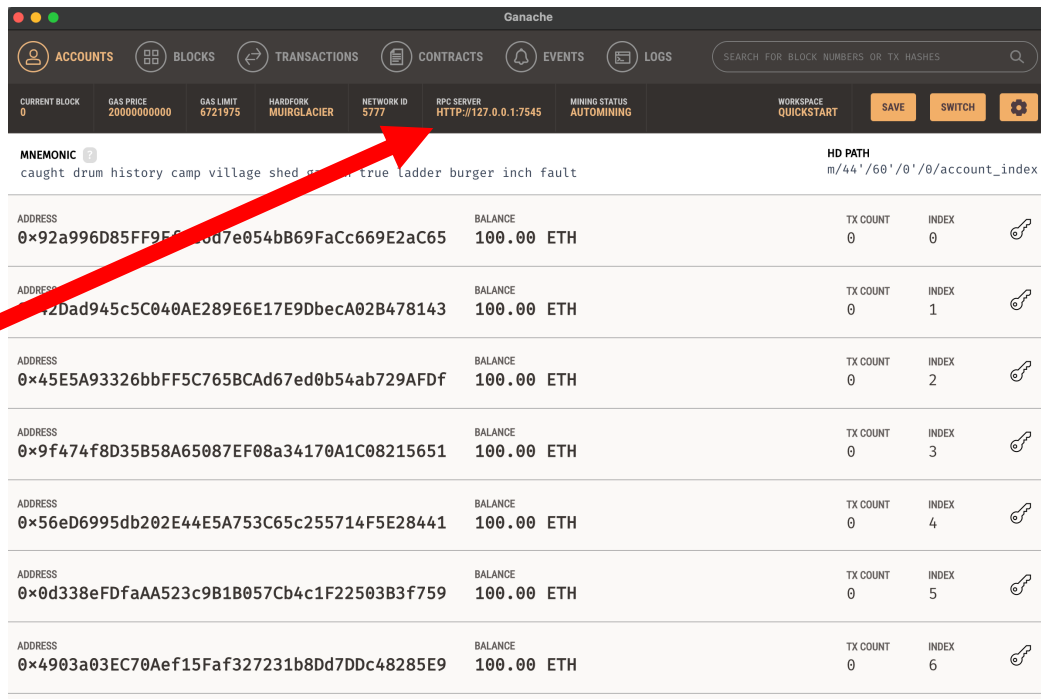


Iniciando o Ganache



Abrindo o Ganache (10 contas abertas)

- Ganache é
 - Blockchain
 - Carteira
- É o “dois em um”
- Vamos prestar atenção ao *endpoint*
- RPC Server



The screenshot shows the Ganache application interface. At the top, there is a navigation bar with tabs for ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. Below this is a status bar with various metrics: CURRENT BLOCK (0), GAS PRICE (20000000000), GAS LIMIT (6721975), HARDFORK (MUIRGLACIER), NETWORK ID (5777), RPC SERVER (HTTP://127.0.0.1:7545), MINING STATUS (AUTOMINING), and WORKSPACE QUICKSTART. Below the status bar is a mnemonic phrase: "caught drum history camp village shed ... true ladder burger inch fault".

ADDRESS	BALANCE	TX COUNT	INDEX
0x92a996D85FF9F6007e054bB69FaCc669E2aC65	100.00 ETH	0	0
0x72Dad945c5C040AE289E6E17E9DbecA02B478143	100.00 ETH	0	1
0x45E5A93326bbFF5C765BCAd67ed0b54ab729AFdf	100.00 ETH	0	2
0x9f474f8D35B58A65087EF08a34170A1C08215651	100.00 ETH	0	3
0x56eD6995db202E44E5A753C65c255714F5E28441	100.00 ETH	0	4
0x0d338eFdfAA523c9B1B057Cb4c1F22503B3f759	100.00 ETH	0	5
0x4903a03EC70Aef15Faf327231b8Dd7DDc48285E9	100.00 ETH	0	6

De volta para o Remix

- Selecionar o ambiente “Web3 Provider”

Executar o comando

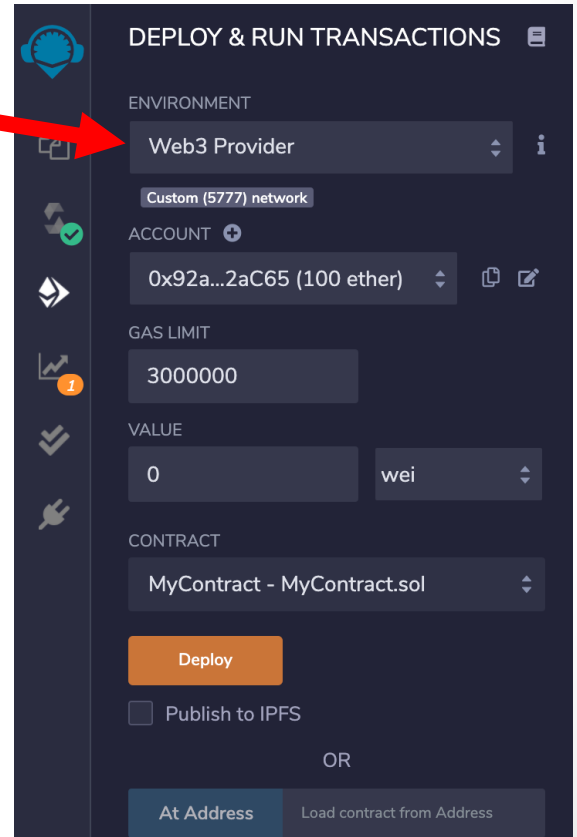
```
open -n -a /Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome --args --user-data-dir="/tmp/chrome_dev_test" --disable-web-security
```

Linux

```
google-chrome --disable-web-security
```

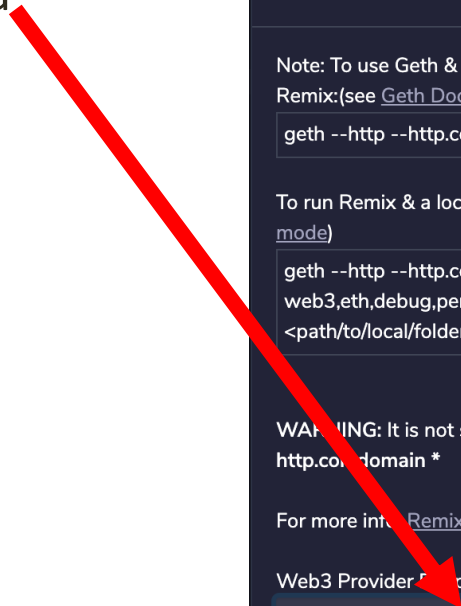
Windows

```
"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security --disable-gpu --user-data-dir=~\chromeTemp
```



De volta para o Remix

- Alterar o número da porta
- O endereço IP é o mesmo
 - É o do Localhost



External node request ✕

Note: To use Geth & <https://remix.ethereum.org>, configure it to allow requests from Remix: (see [Geth Docs on rpc server](#))

```
geth --http --http.corsdomain https://remix.ethereum.org
```

To run Remix & a local Geth test node, use this command: (see [Geth Docs on Dev mode](#))

```
geth --http --http.corsdomain="http://remix.ethereum.org" --http.api web3,eth,debug,personal,net --vmdebug --datadir <path/to/local/folder/for/test/chain> --dev console
```

WARNING: It is not safe to use the `--http.corsdomain` flag with a wildcard: `--http.corsdomain *`

For more info: [Remix Docs on Web3 Provider](#)

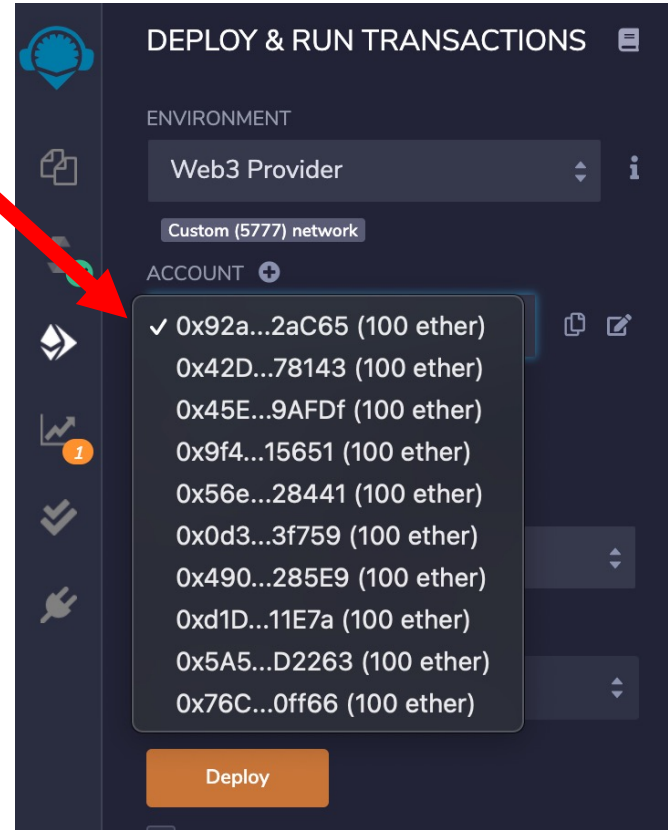
Web3 Provider endpoint

```
http://127.0.0.1:7545
```

OK Cancel

De volta para o Remix

- Seleciona-se uma conta para descontar o Gas
- Representado pela identidade da conta



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Web3 Provider

Custom (5777) network

ACCOUNT +

- ✓ 0x92a...2aC65 (100 ether)
- 0x42D...78143 (100 ether)
- 0x45E...9AFDf (100 ether)
- 0x9f4...15651 (100 ether)
- 0x56e...28441 (100 ether)
- 0x0d3...3f759 (100 ether)
- 0x490...285E9 (100 ether)
- 0xd1D...11E7a (100 ether)
- 0x5A5...D2263 (100 ether)
- 0x76C...0ff66 (100 ether)

Deploy

Deploy do MyContract

Deploy

Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 1

All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.

Deployed Contracts

- MYCONTRACT AT 0XC7B...1D234 (BLOC)

listen on network

Search with transaction hash or address

```
[block:1 txIndex:0] from: 0x92a...2aC65 to: MyContract.(constructor) value: 0 wei  
data: 0x608...10033 logs: 0 hash: 0x5b6...97e8c
```

Executa-se o MyContract

- Verificar que o número de conta é o do Ganache

The screenshot displays the Ganache interface for a contract named 'MYCONTRACT AT 0XC78...1D234 (BLOI'. The left sidebar shows a 'MyString' button and a 'Transact' button. The main area displays the contract's state, including the text 'string: Alo Alo ICMC'. The bottom panel shows a transaction log with the following entry:

```
CALL [Call] 0x92a996D85FF9Ef9c6d7e054bB69FaCc669E2aC65 to: MyContract.MyString()  
data: 0x183...73189
```

Red arrows highlight the 'MyString' button, the 'string: Alo Alo ICMC' text, and the transaction log entry.

O melhor para o desenvolvimento

- Viu como ele é rápido?
- Vantagem: o uso do blockchain é rápido por ser local
- Para o desenvolvimento?
- Melhor o JavaScript VM ou o Ganache
- Teremos outro laboratório com o Ganache

Sumário

- Potenciais mercados
- O que são transações?
- Ethereum e o Ether
- Prática I
- Prática II
- Prática III
- Prática IV
- Prática V (Usando Ganache Provider)
- Prática VI

Um outro exemplo

Executar o código disponível no link abaixo

<https://github.com/joueyama/blockchain/blob/main/jocoin.sol>

Lembrando: Um contrato no sentido de Solidity

- é uma coleção de código (suas funções) e dados (seu estado);
- que reside em um endereço específico na blockchain Ethereum

Alterar

- seu_nome_coin
- taxa de conversão para seu NUSP
- Implementar o modificador antes da venda do seu_nome_coin

Executar o contrato inteligente

- Baixar o código do https://remix-ide.readthedocs.io/en/latest/create_deploy.html
- Executar no Remix VM London
- Descrever o que é uma função “payable”
- O que acontece se transferirmos Ether em uma função “non-payable” (veja a resposta em <https://docs.alchemy.com/docs/solidity-payable-functions>)

Agora é a sua vez 😊

- Repita as quatro práticas para assimilar o seu conhecimento

Perguntas ??