

Disciplina:

SMART CONTRACTS

Professor: Pablo V. Rego



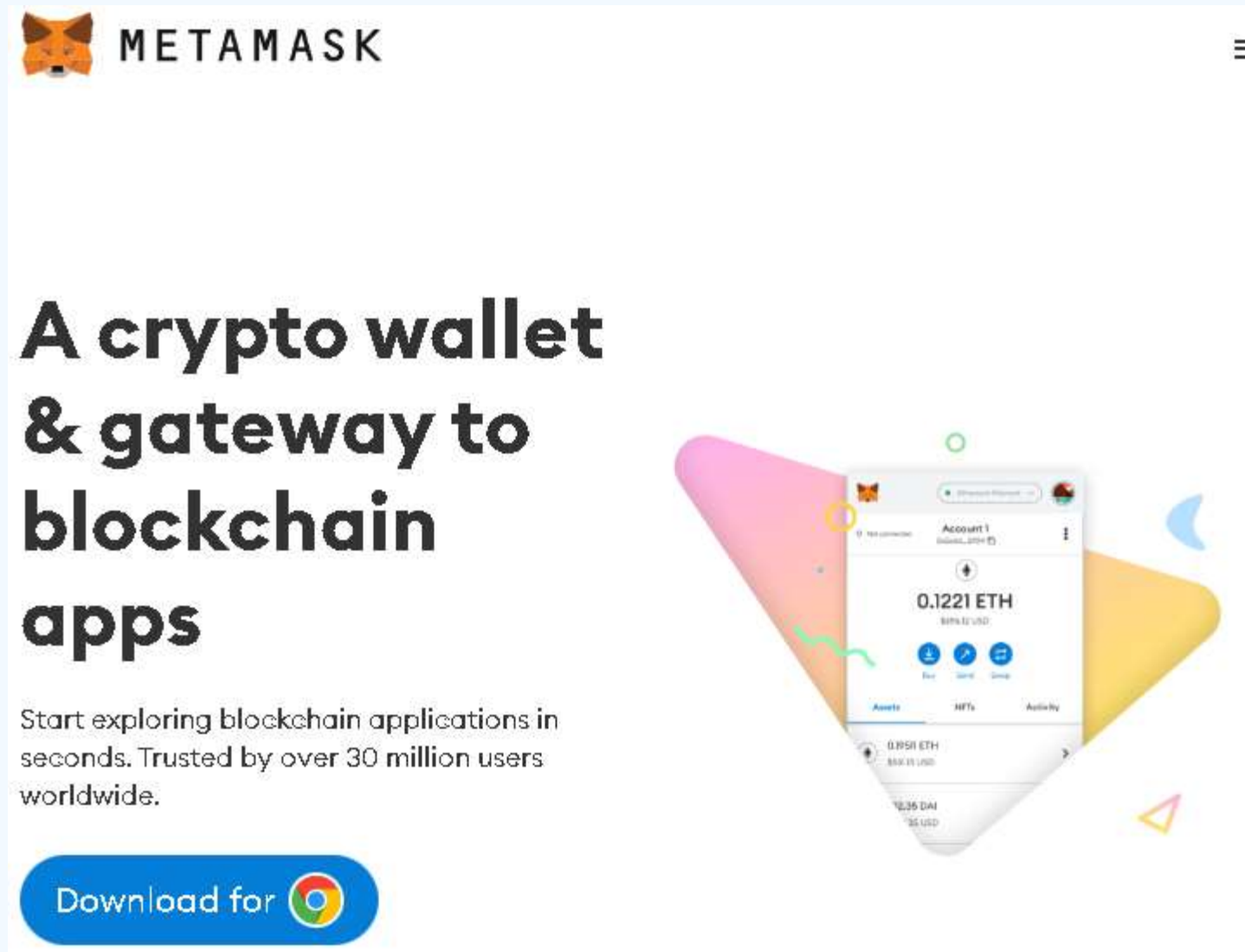
SMAC_2022Sem02–Mod.05

Agenda Módulo #5 : Prática 02

- **Inc/dec**
- **Primitivas**
- **Variáveis**
- **Constantes e Imutáveis**
- **Leitura e Escrita de Variáveis de Estado**
- **Ether e Wei**
- **Gas**
- **If/Else**
- **For/While**
- **Mapping**
- **Array**
- **Enum**
- **Structs**
- **Storage, Memory, Calldata**
- **Functions**
- **View Pure**
- **Erros**
- **Modificadores**
- **Eventos**
- **Construtores**
- **Herança**
- **Sombreamento**
- **Parent Calldata**
- **Visibilidade**
- **Interfaces**
- **Payable**
- **Enviando Ether**
- **Fallback**
- **Call**
- **Delegatecall**
- **Function Selector**
- **Chamada de Outro Contrato**
- **Contract Factory**
- **Try Catch**
- **Import**
- **Library**
- **ABI Decide**
- **Hashing**
- **Verificação de Assinatura**
- **Gas Saving Techs**
- **Bitwise Ops**

MetaMask


- <https://metamask.io>



METAMASK

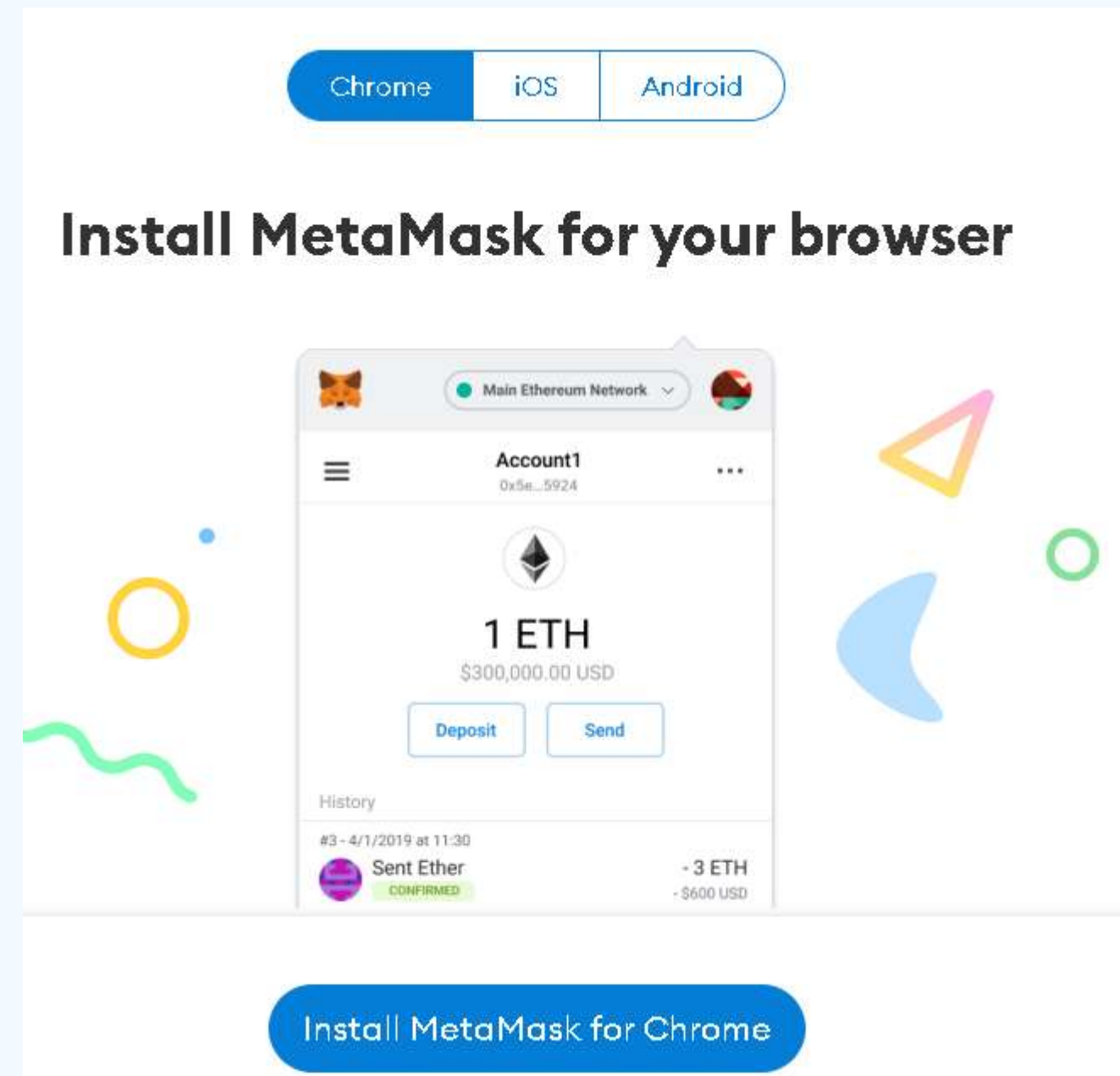
A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 30 million users worldwide.

Download for 

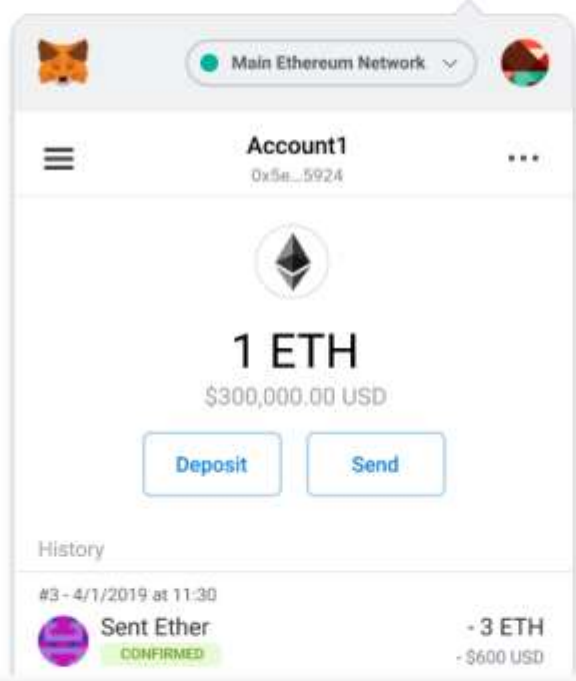
The banner features the MetaMask logo at the top left. Below it, the text 'A crypto wallet & gateway to blockchain apps' is prominently displayed. Underneath, a smaller line of text states 'Start exploring blockchain applications in seconds. Trusted by over 30 million users worldwide.' At the bottom left, there is a blue button with the text 'Download for' followed by the Chrome logo. On the right side of the banner, there is a stylized illustration of a smartphone displaying the MetaMask interface, showing a balance of 0.1221 ETH and various transaction history items. The background of the banner is white with colorful geometric shapes (triangles, circles, and lines) in shades of pink, yellow, and blue.

- Extensão no browser



Chrome iOS Android

Install MetaMask for your browser



1 ETH
\$300,000.00 USD

Deposit Send

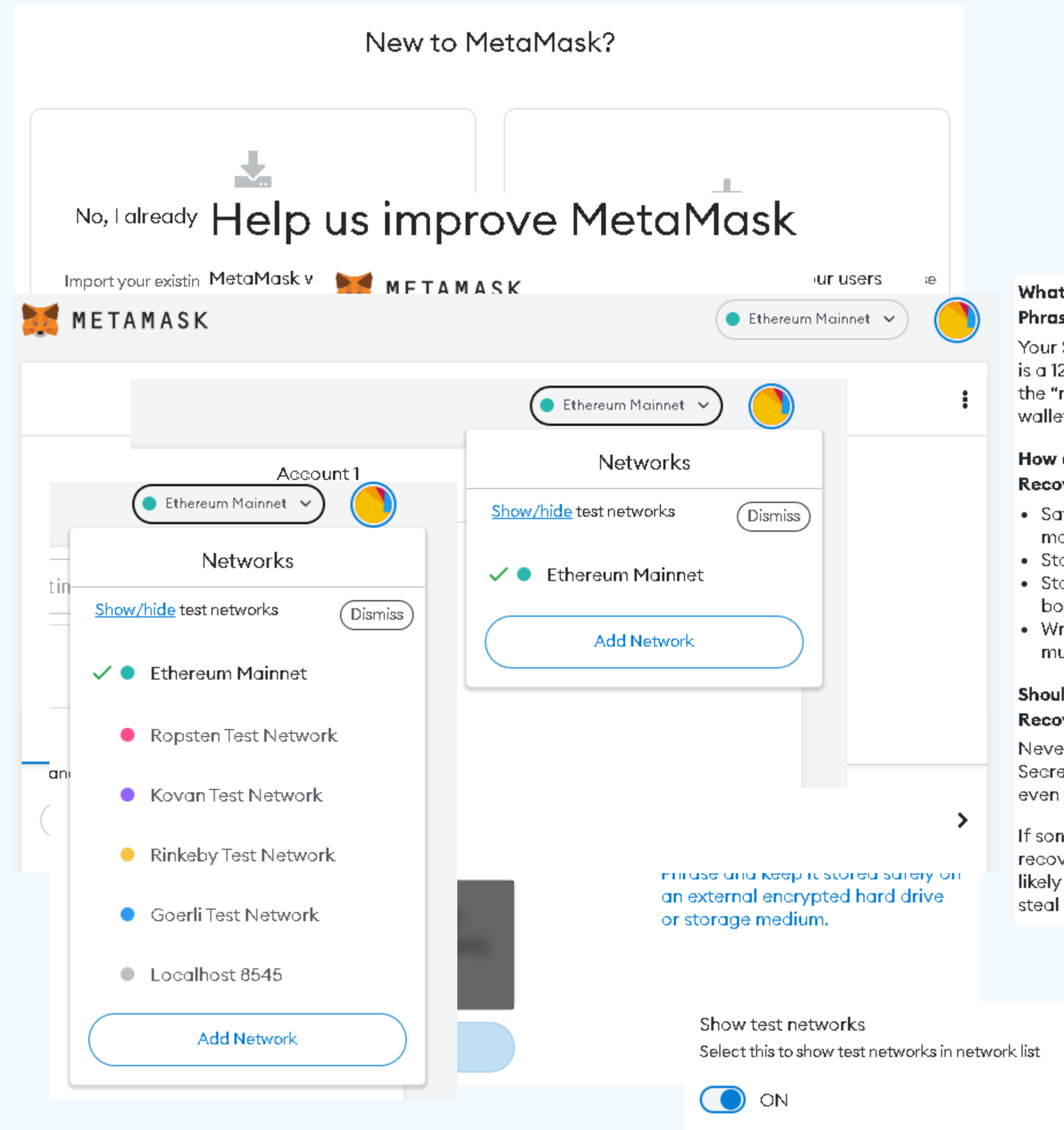
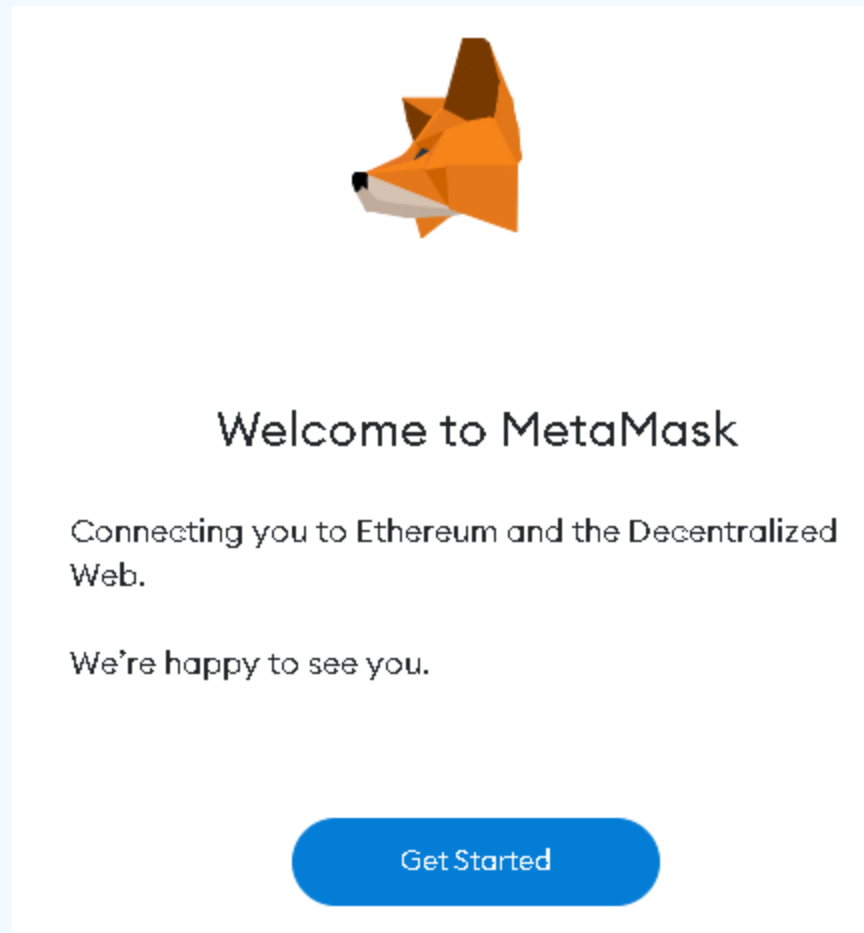
History

#3 - 4/1/2019 at 11:30
Sent Ether CONFIRMED - 3 ETH - \$600 USD

Install MetaMask for Chrome

The image shows the MetaMask website's installation page for browser extensions. At the top, there are three buttons for 'Chrome', 'iOS', and 'Android'. Below these, the heading 'Install MetaMask for your browser' is centered. The main visual is a screenshot of the MetaMask browser extension interface. The interface shows the 'Main Ethereum Network' selected, the account name 'Account1' with address '0x5e...5924', and a balance of '1 ETH' valued at '\$300,000.00 USD'. There are 'Deposit' and 'Send' buttons. Below this, a 'History' section shows a transaction: '#3 - 4/1/2019 at 11:30', 'Sent Ether', 'CONFIRMED', '- 3 ETH', and '- \$600 USD'. At the bottom, there is a blue button that says 'Install MetaMask for Chrome'. The background of the page is white with colorful geometric shapes (circles, triangles, and lines) in shades of yellow, blue, and green.

Metamask : Setup



What is a Secret Recovery Phrase?

Your Secret Recovery Phrase is a 12-word phrase that is the "master key" to your wallet and your funds

How do I save my Secret Recovery Phrase?

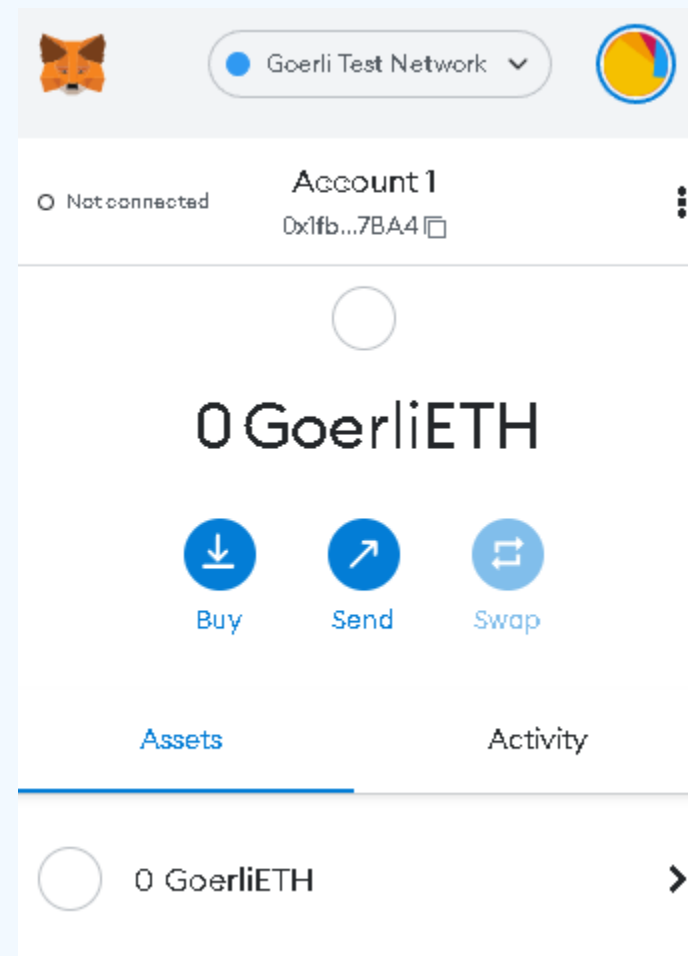
- Save in a password manager
- Store in a bank vault
- Store in a safe deposit box
- Write down and store in multiple secret places

Should I share my Secret Recovery Phrase?

Never, ever share your Secret Recovery Phrase, not even with MetaMask!

If someone asks for your recovery phrase they are likely trying to scam you and steal your wallet funds.

MetaMask : Free Ether (Testnets)



Faucets (nem sempre funcionam)

- <https://faucet.metamask.io/>
- Paradigm :
 - <https://faucet.paradigm.xyz>
- *Ropsten*:
 - <https://faucet.metamask.io>
- *Rinkeby*:
 - <https://faucet.rinkeby.io>
 - <https://www.rinkebyfaucet.com>
 - <https://app.mycrypto.com/faucet>
 - <https://faucets.chain.link/rinkeby>
- *Kovan*:
 - <https://gitter.im/kovan-testnet/faucet>
- *Goerli*:
 - <https://goerli-faucet.slock.it/index.html>
 - <https://faucet.goerli.mudit.blog>

Inc/Dec

- Aqui está um contrato simples que você pode obter, aumentar e diminuir o armazenamento de contagem neste contrato.
- `counter.sol`

Primitivas

- Alguns tipos de dados primitivos disponíveis no Solidity.
- `boolean`
- `uint`
- `int`
- `address`
- `primitives.sol`

Variáveis

- Existem 3 tipos de variáveis no Solidity
 - local
 - declarado dentro de uma função
 - não armazenado no blockchain
 - state
 - declarado fora de uma função
 - armazenado na blockchain
 - global (fornece informações sobre a blockchain)
- `variables.sol`

Constantes e Imutáveis

- Constantes são variáveis que não podem ser modificadas.
- Seu valor é codificado e o uso de constantes pode economizar custos de gás.
- `constants.sol`
- Variáveis imutáveis são como constantes. Valores de variáveis imutáveis podem ser definidos dentro do construtor, mas não podem ser modificados posteriormente.

Leitura e Escrita de Variáveis de Estado

- Para escrever ou atualizar uma variável de estado, você precisa enviar uma transação.
- Simplestorage.sol
- Por outro lado, você pode ler variáveis de estado, gratuitamente, sem nenhuma taxa de transação

Ether e Wei

- As transações são pagas com éter.
- Semelhante a como um dólar é igual a 100 centavos, um éter é igual a $1e18$ wei.
- [Etherwei.sol](https://etherwei.sol)

Gas

Quanto éter você precisa pagar por uma transação?

- Você paga o gás gasto * valor do preço do gás de éter, onde
 - gás é uma unidade de computação
 - gás gasto é a quantidade total de gás usada em uma transação
 - preço do gás é quanto de éter você está disposto a pagar por gás
- As transações com preço de gás mais alto têm maior prioridade para serem incluídas em um bloco.
- O gás não gasto será reembolsado.

Limite de gás

- Existem 2 limites superiores para a quantidade de gás que você pode gastar
 - limite de gás (quantidade máxima de gás que você está disposto a usar para sua transação, definido por você)
 - limite de gás do bloco (quantidade máxima de gás permitida em um bloco, definida pela rede)

- Gas.sol

If/Else

- Ifelse.sol

For/While

- Solidity suporta loops for, while e do while.
- Não escreva loops ilimitados, pois isso pode atingir o limite de gás, fazendo com que sua transação falhe.
- Pelo motivo acima, os loops while raramente são usados.
- `forwhile.sol`

Mapping

- Os mapas são criados com o mapeamento de sintaxe (keyType => valueType).
 - O keyType pode ser qualquer tipo de valor interno, bytes, string ou qualquer contrato.
 - valueType pode ser qualquer tipo, incluindo outro mapeamento ou uma matriz.
 - Os mapeamentos não são iteráveis.
- Mappings.sol

Array

- O array pode ter um tamanho fixo em tempo de compilação ou um tamanho dinâmico.
- Arrays.sol