

Лабораторная работа 1. Безопасное хранение ключей: МетаМаск и разделение секретов Шамира

Цель

Познакомиться с криптовалютным кошельком МетаМаск и методом хранения секретной фразы.

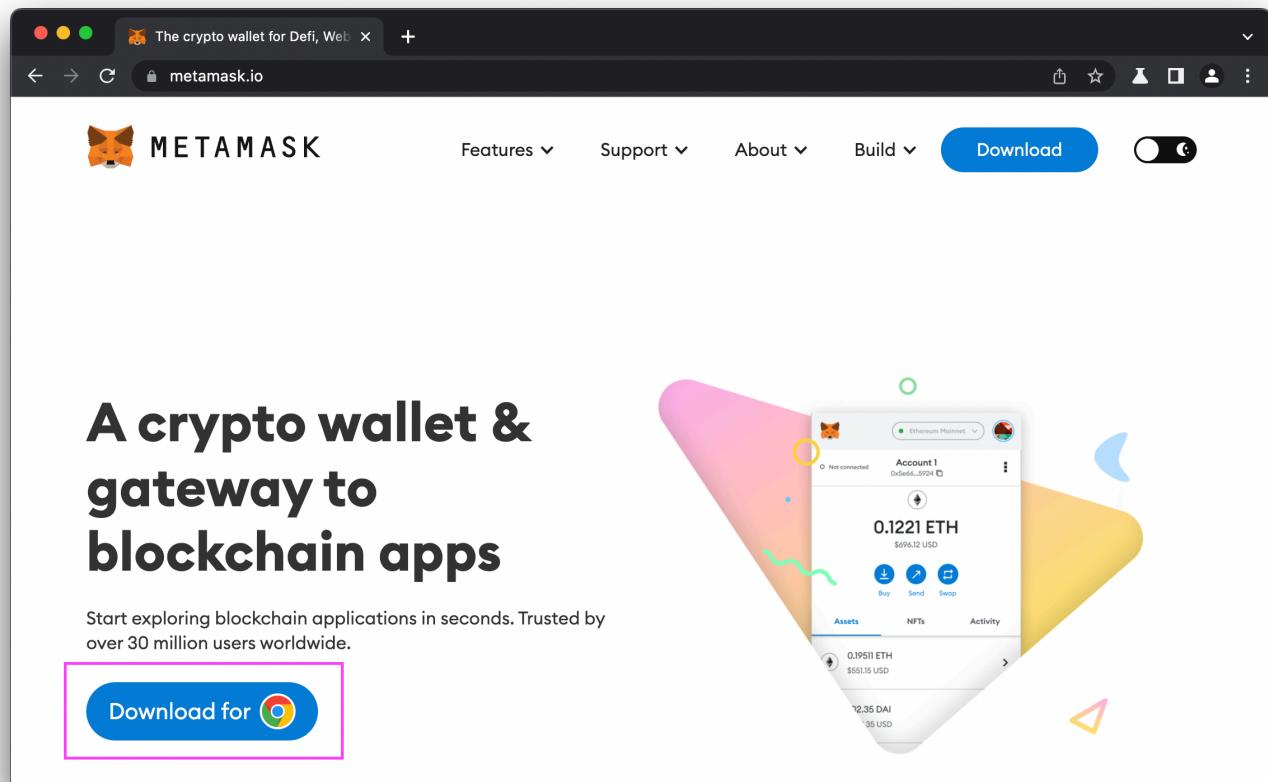
Шаги:

1. Установить МетаМаск.
2. Удостовериться, что вы можете посылать транзакции.
3. Сохранить секретную фразу безопасным способом.

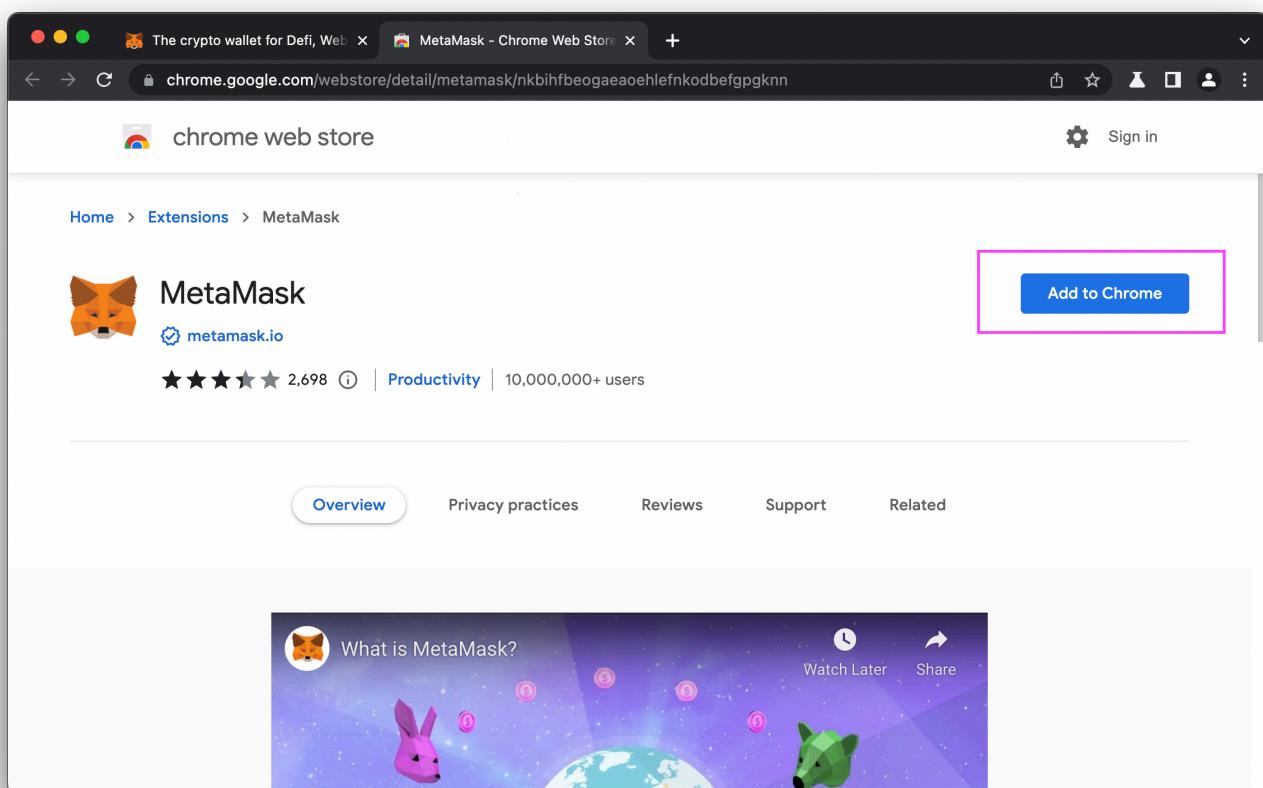
1. Установка МетаМаск

МетаМаск предлагается как расширение для браузера и как мобильное приложение. Мы будем ставить его как расширение для браузера. Для избежания путаницы, здесь рекомендуется использовать браузер [Google Chrome](#).

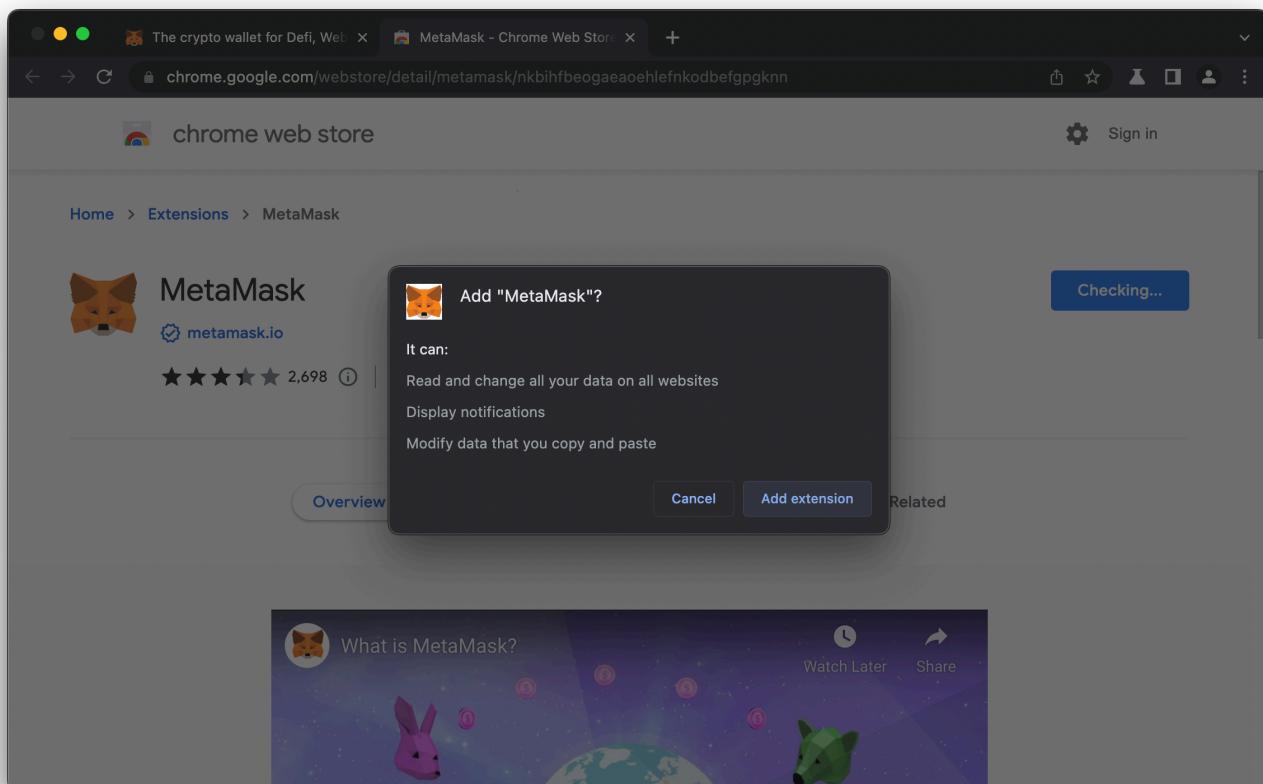
Зайдите на сайт кошелька <https://metamask.io>



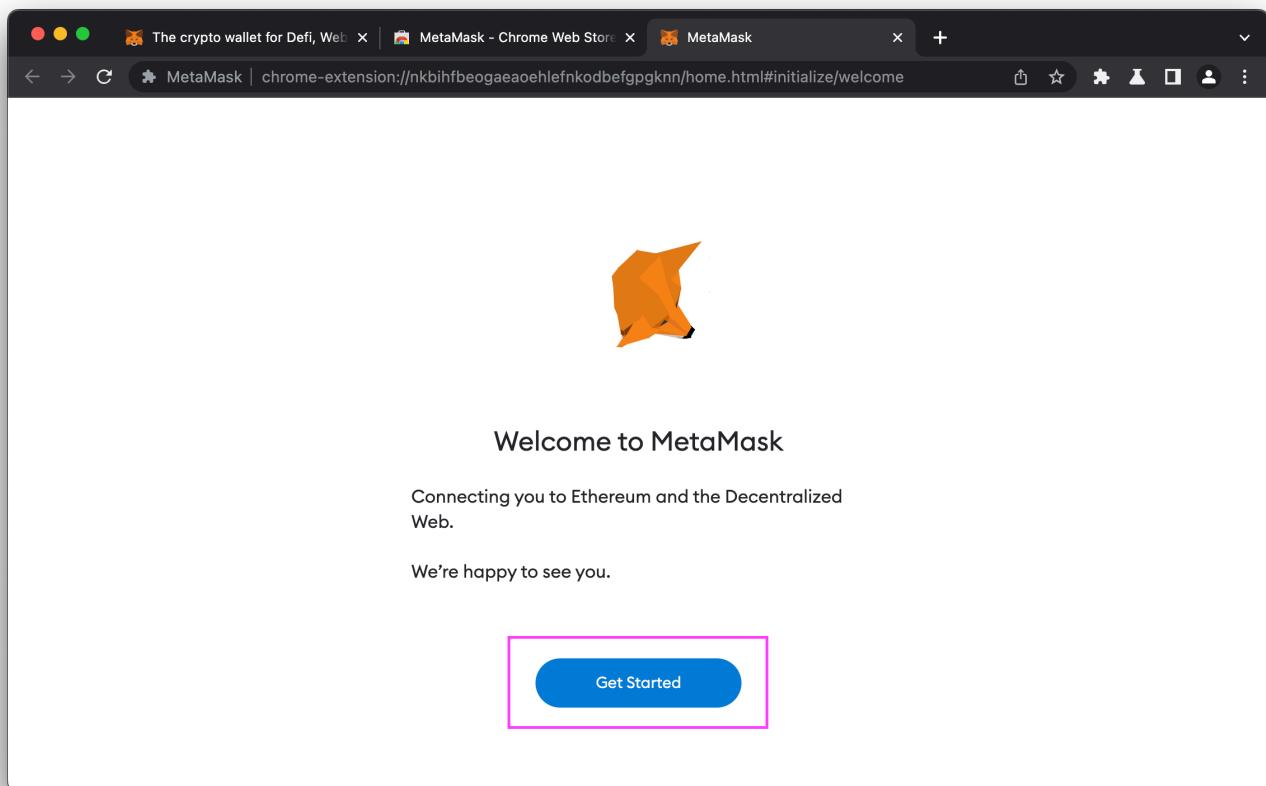
Нажмите кнопку "Download for..." Откроется новая вкладка на Chrome Web Store. Здесь нужно нажать кнопку "Add to Chrome".



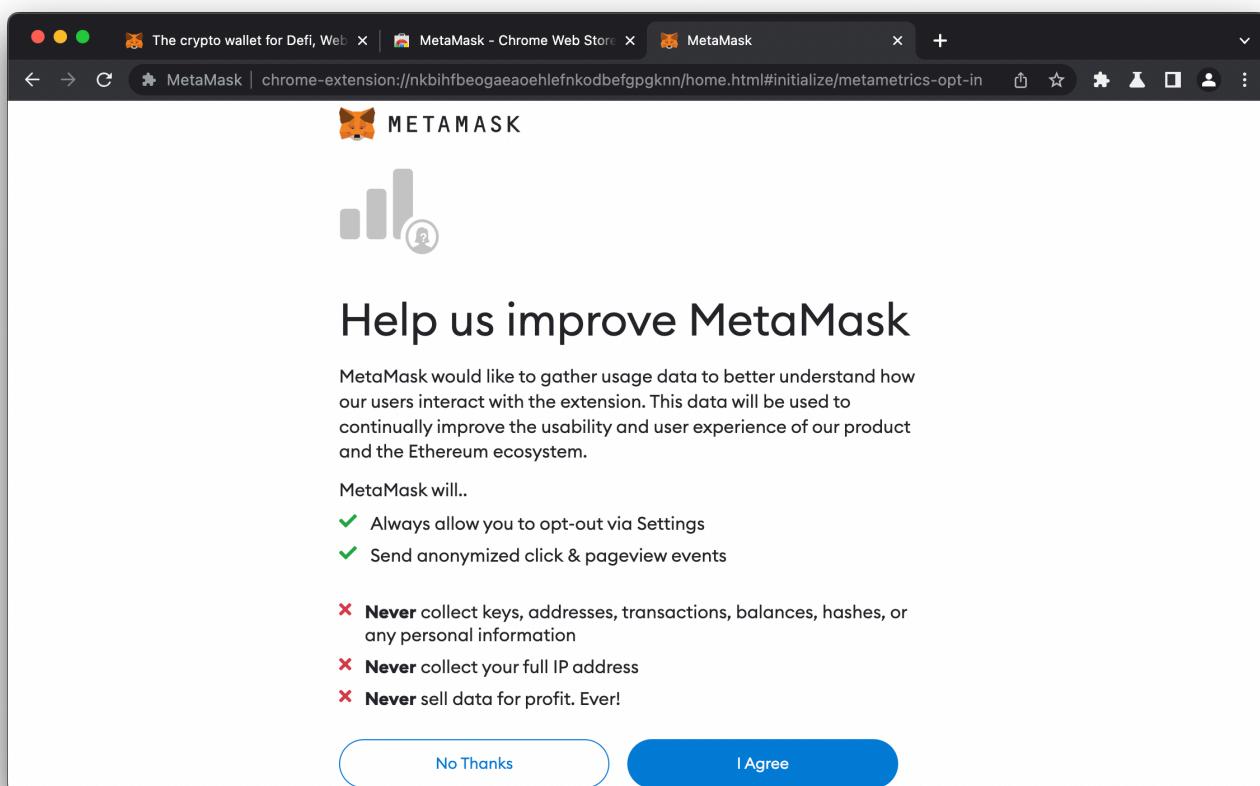
Браузер запросит разрешения на установку. Соглашайтесь.



Через некоторое время браузер установит расширение. Откроется новая вкладка. МетаМаск начнёт процедуру онбординга. Нажмите кнопку Get Started.

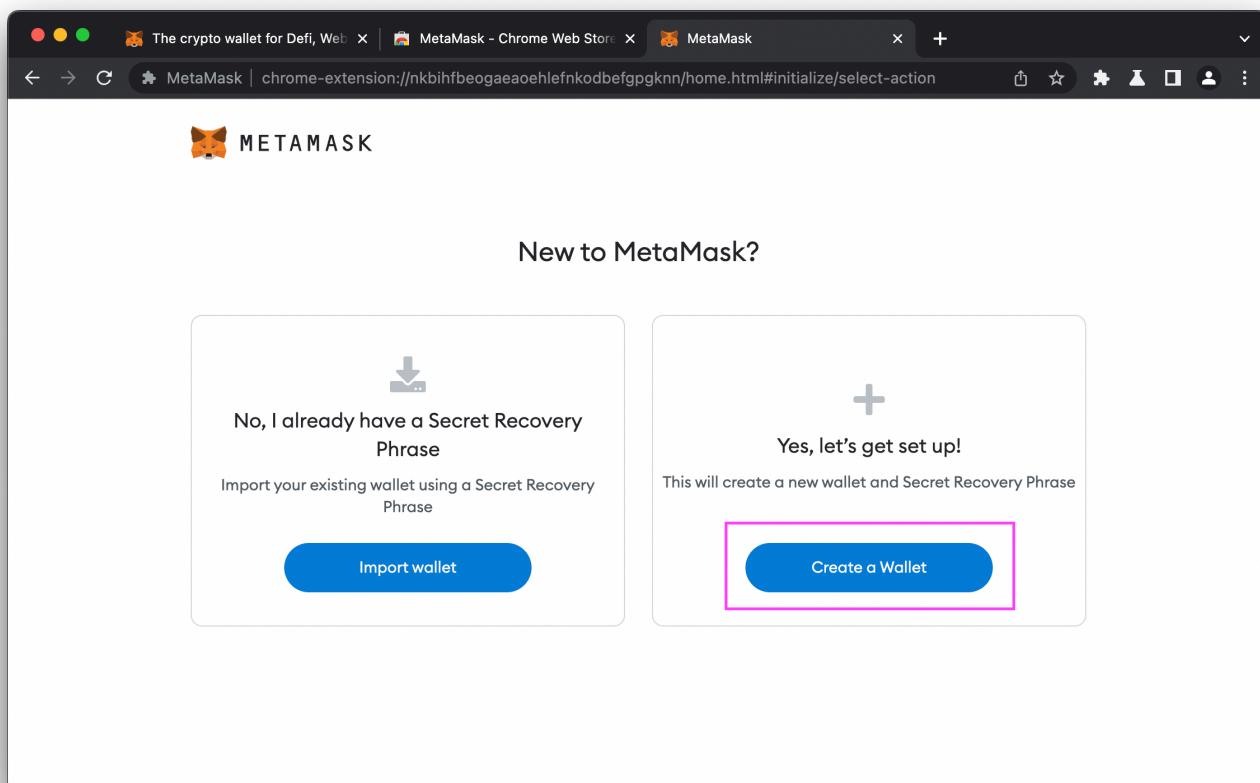


Вы можете согласиться на то, чтобы создатели МетаМаск получали анонимную статистику использования.



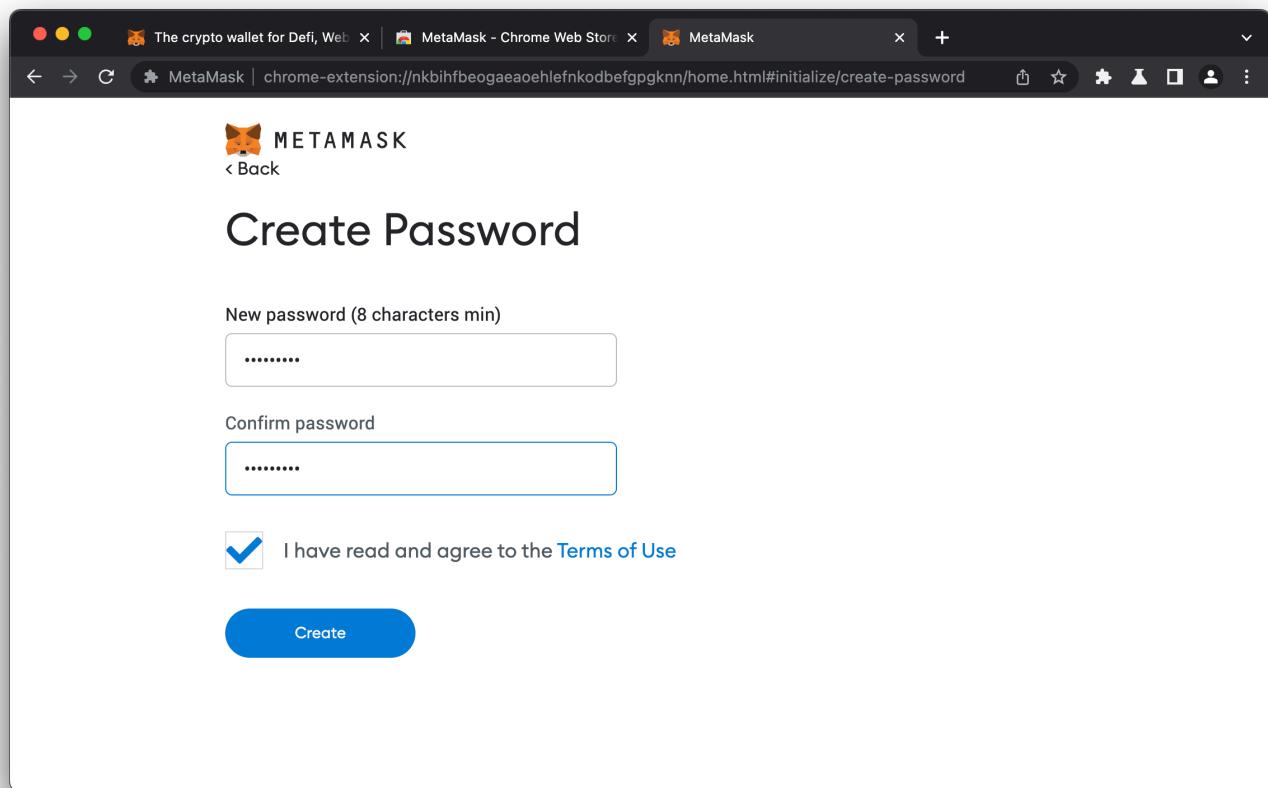
The screenshot shows the initial setup screen for the MetaMask extension. At the top, there's a navigation bar with tabs for "The crypto wallet for Defi, Web3..." and "MetaMask - Chrome Web Store". The main content area features the MetaMask logo (a fox head) and a bar chart icon. A large heading says "Help us improve MetaMask". Below it, a paragraph explains that MetaMask wants to gather usage data to improve the product and the Ethereum ecosystem. It lists what MetaMask will do (allow opt-out via Settings, send anonymized events) and what it will never do (never collect keys, addresses, balances, hashes, or personal info, never collect IP address, never sell data for profit). At the bottom are two buttons: "No Thanks" and "I Agree".

На следующем шаге МетаМаск запросит, хотите ли вы использовать существующую секретную фразу или создать новую. Мы начинаем с чистого листа, поэтому создаём новую.



The screenshot shows the "New to MetaMask?" screen. The title "New to MetaMask?" is at the top. Two options are presented in boxes: "No, I already have a Secret Recovery Phrase" (with an import icon) and "Yes, let's get set up!" (with a create icon). The "Create a Wallet" button is highlighted with a pink border. The URL in the browser is "chrome-extension://nkbihfbeogaeaaoehlefknkodbefgpgknn/home.html#initialize/select-action".

Далее задайте пароль для входа в кошелёк. Пароль должен содержать 8 символов минимум. Пароль служит для контроля доступа к кошельку.



На следующем шаге МетаМаск предложит ознакомиться с тем, что такое секретная фраза. Можете пропускать.

The screenshot shows the MetaMask wallet setup interface. At the top, there's a navigation bar with tabs for "The crypto wallet for Defi, Web3, and Ethereum" and "MetaMask - Chrome Web Store". The main content area features the Metamask logo and the heading "Secure your wallet". Below this is a video player showing a video titled "Secure your wallet" with a duration of 0:00 / 1:35. To the right of the video is a sidebar with several sections:

- 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

Теперь настало время работы с секретной фразой. Нажмите на затемнённое поле, чтобы увидеть секретную фразу. Перепишите её в файл или на лист бумаги, нажмите кнопку продолжения.

This screenshot shows the "Secret Recovery Phrase" step of the MetaMask setup process. The top navigation bar and sidebar from the previous screen are visible. The main content area has the Metamask logo and the heading "Secret Recovery Phrase". Below this is a section with the text "Your Secret Recovery Phrase makes it easy to back up and restore your account." and a warning: "WARNING: Never disclose your Secret Recovery Phrase. Anyone with this phrase can take your Ether forever." To the right of the text are several "Tips:":

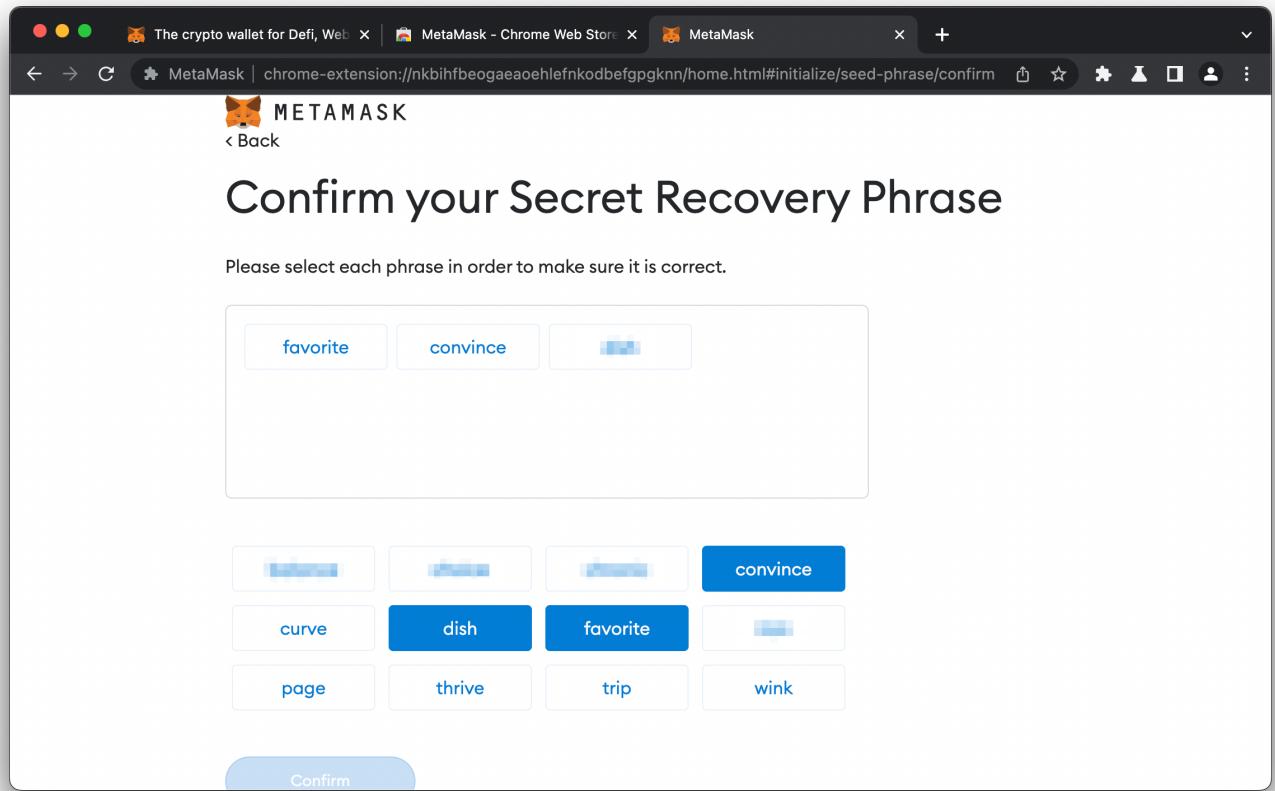
- Store this phrase in a password manager like 1Password.
- Write this phrase on a piece of paper and store in a secure location. If you want even more security, write it down on multiple pieces of paper and store each in 2 - 3 different locations.
- Memorize this phrase.
- Download this Secret Recovery Phrase and keep it stored safely on an external encrypted hard drive or storage medium.

At the bottom of the screen is a large button with a lock icon and the text "CLICK HERE TO REVEAL SECRET WORDS". Below this button are two buttons: "Remind me later" and "Next".

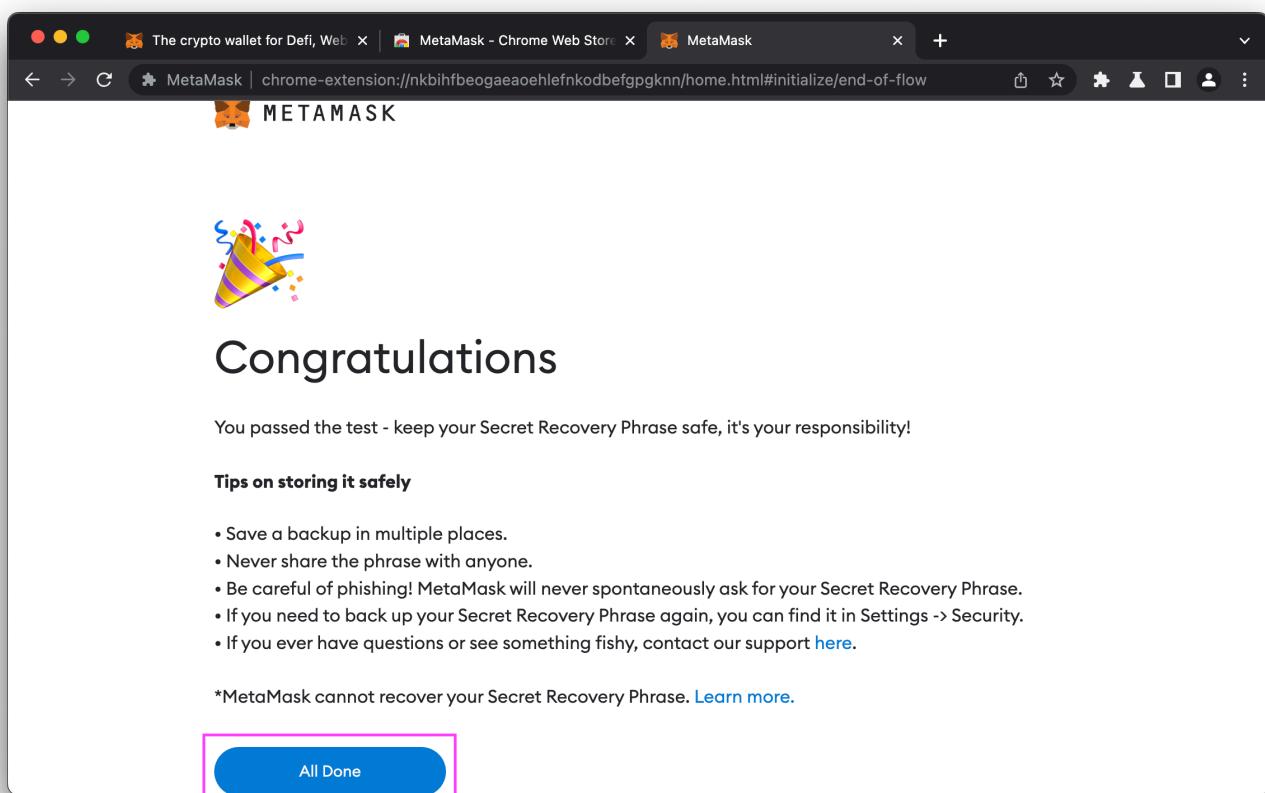
Довольно часто люди сразу забывают секретную фразу. Чтобы удостовериться, что секретную фразу вы сохранили, МетаМаск требует, чтобы вы её подтвердили. Выставите предложенные слова в порядок так, чтобы получилась имеющаяся у вас секретная фраза. Замечание: набор слов секретной фразы отличается от вашего.

Нажатие на блок слов внизу передвигает слово в верхний блок. Рекомендуется нажимать слова в нижнем блоке в порядке, указанном в вашей секретной фразе.

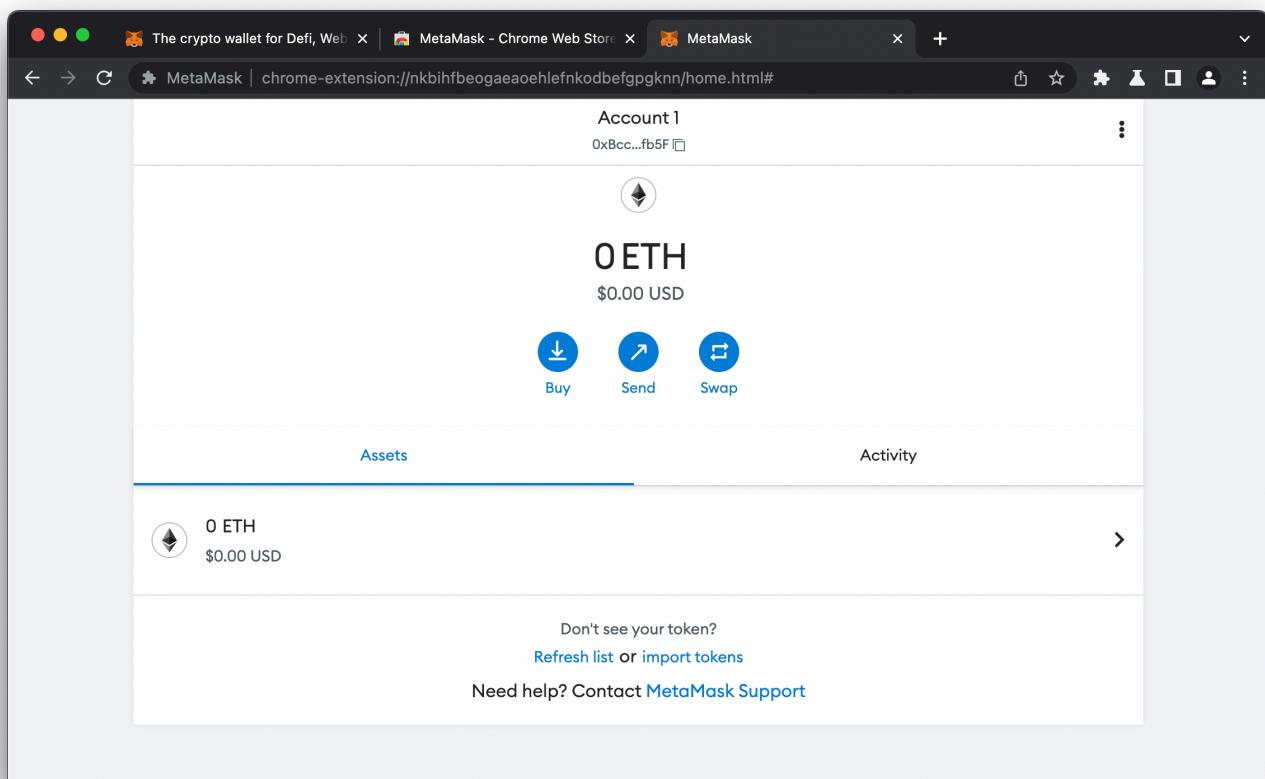
По окончании, нажмите кнопку подтверждения, чтобы перейти к следующему шагу. Если воссозданная секретная фраза не соответствует оригиналу, кнопку подтверждения будет неактивна.



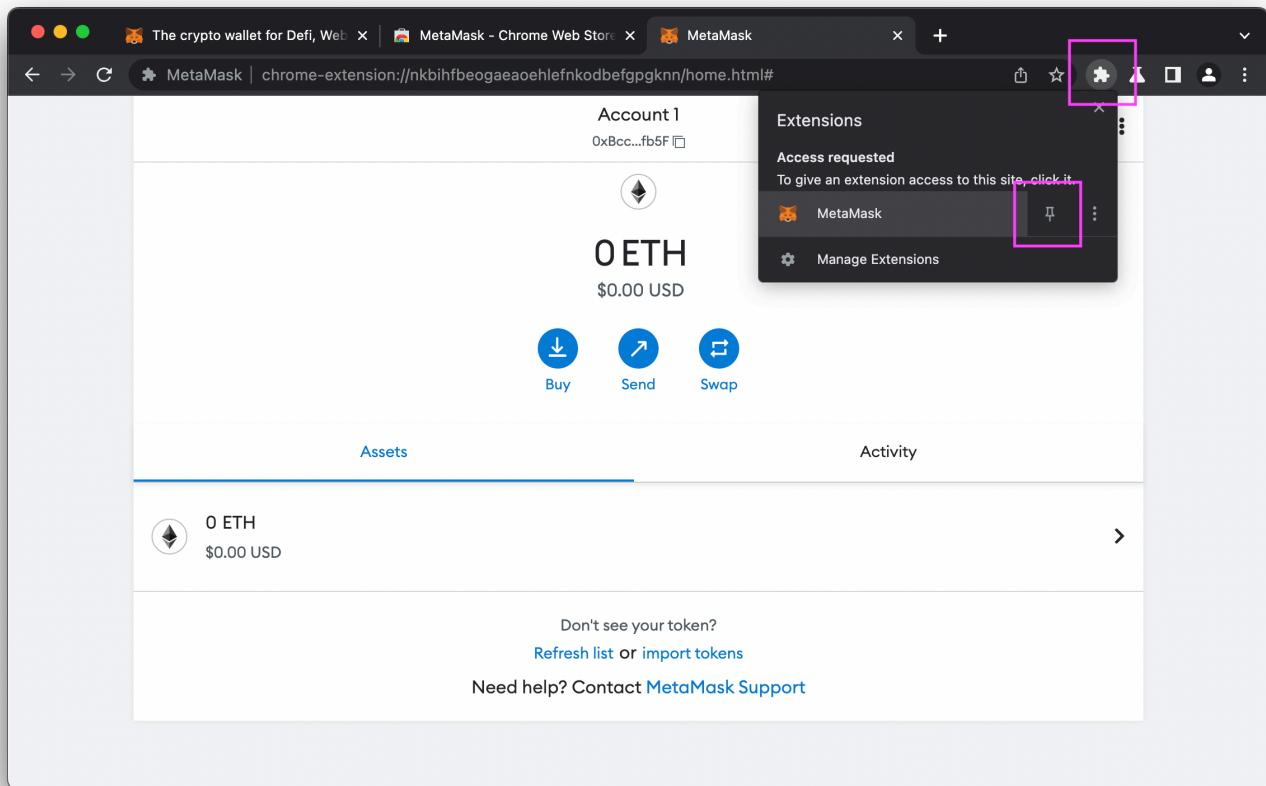
Если всё прошло хорошо, на экране появится приветствие как последния этап онбординга. Нажмите кнопку продолжения.



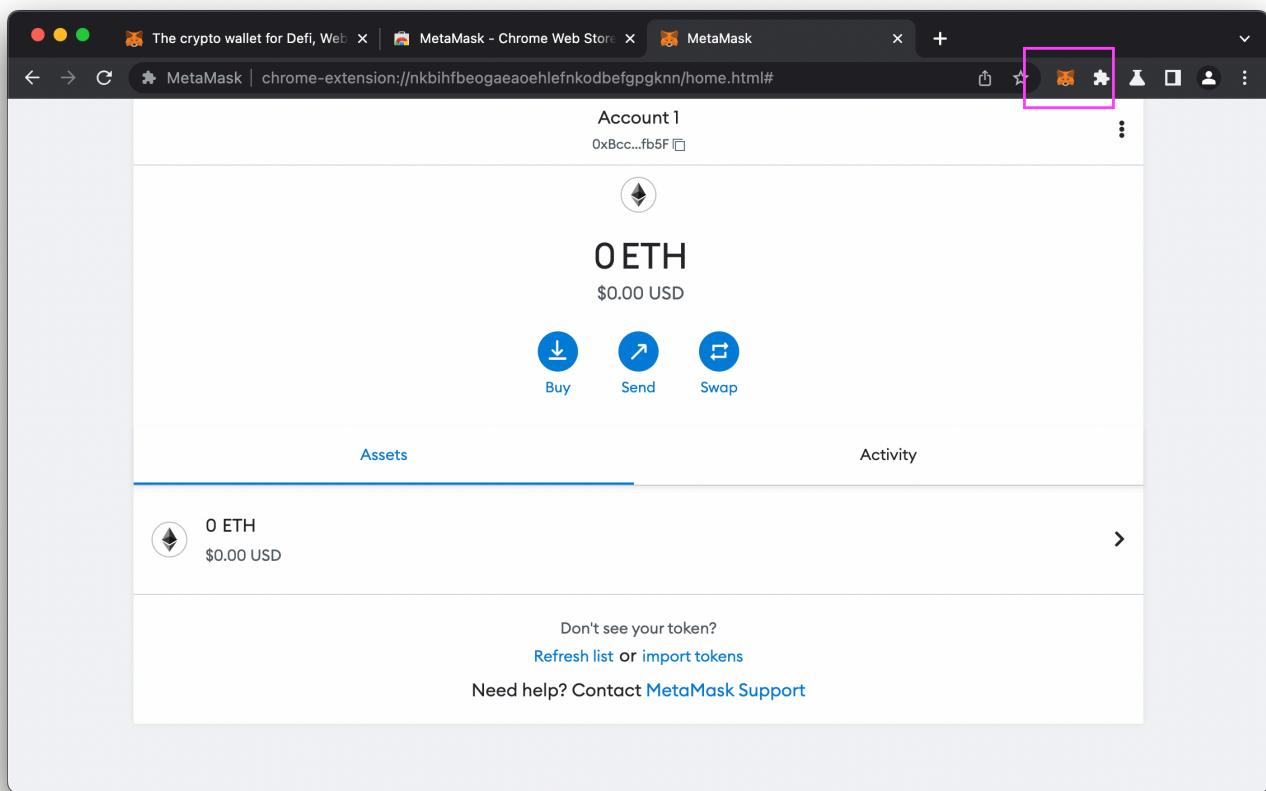
По завершении онбординга откроется страница кошелька, выглядящая как на снимке ниже. Как видно, кошелёк пуст.



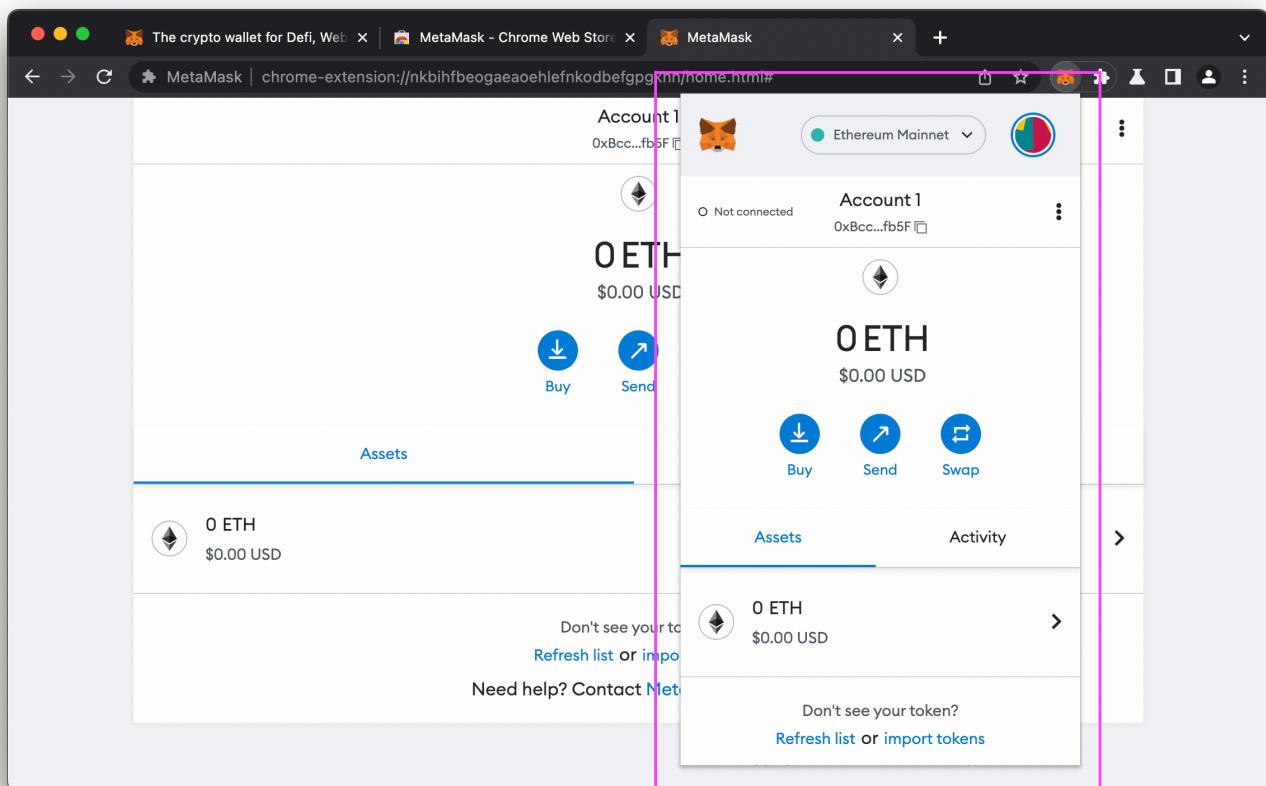
Преимущественно вместо этого вида, кошельёк используется из панели инструментов браузера. По умолчанию, он скрыт, но вы можете вывести его на панель, закрепив его, нажав на кнопку с булавкой.



Иконка МетаМаска должна появиться в интерфейсе браузера.

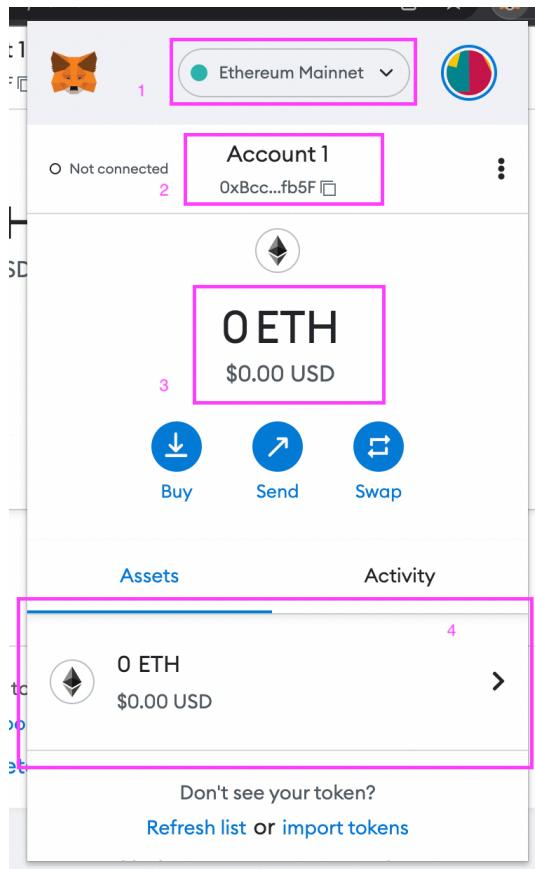


Если щёлкнуть по ней, откроется более приемлемый для ежедневной эксплуатации вид попапа.



Здесь вы можете увидеть:

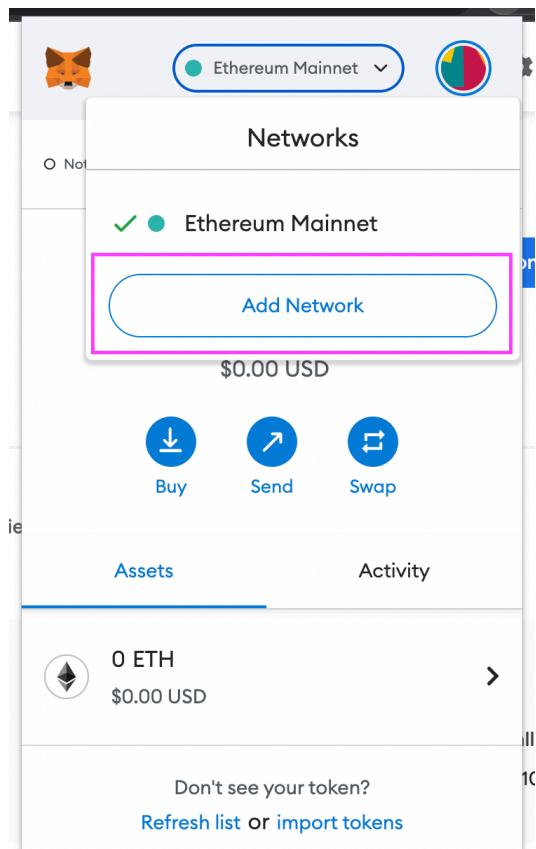
1. блокчейн, к которому подключён кошелёк,
2. ваш блокчейновый адрес,
3. баланс в токенах сети,
4. набор доступных токенов.



2. Посылка транзакции

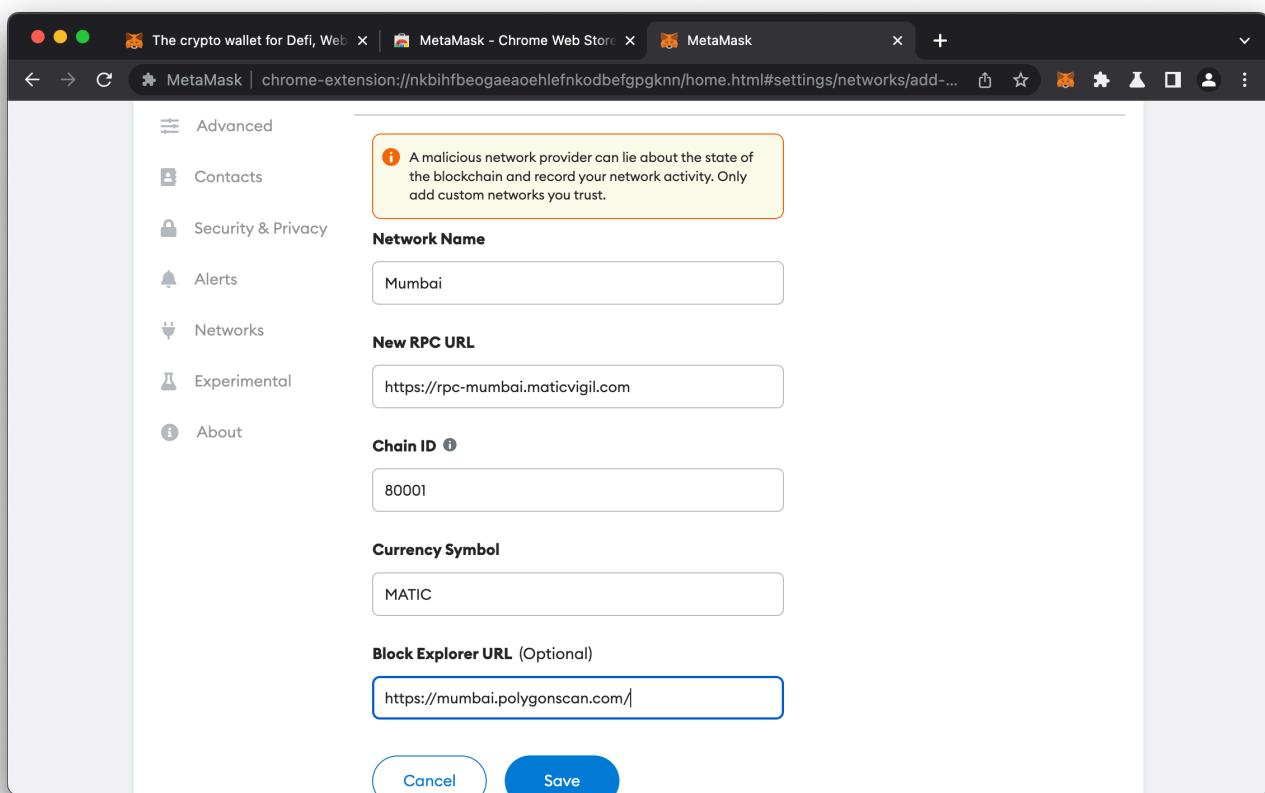
На этом шаге мы подключимся к сети Polygon Mumbai и пошлём транзакцию самому себе. Это тестовая сеть, совместимая с основной сетью Эфириума (Ethereum Mainnet).

Для подключения к тестовой сети Polygon Mumbai, нажмите на блок "Блокчейн, к которому подключён кошелёк". В появившемся выпадающем меню нажмите на кнопку добавить.

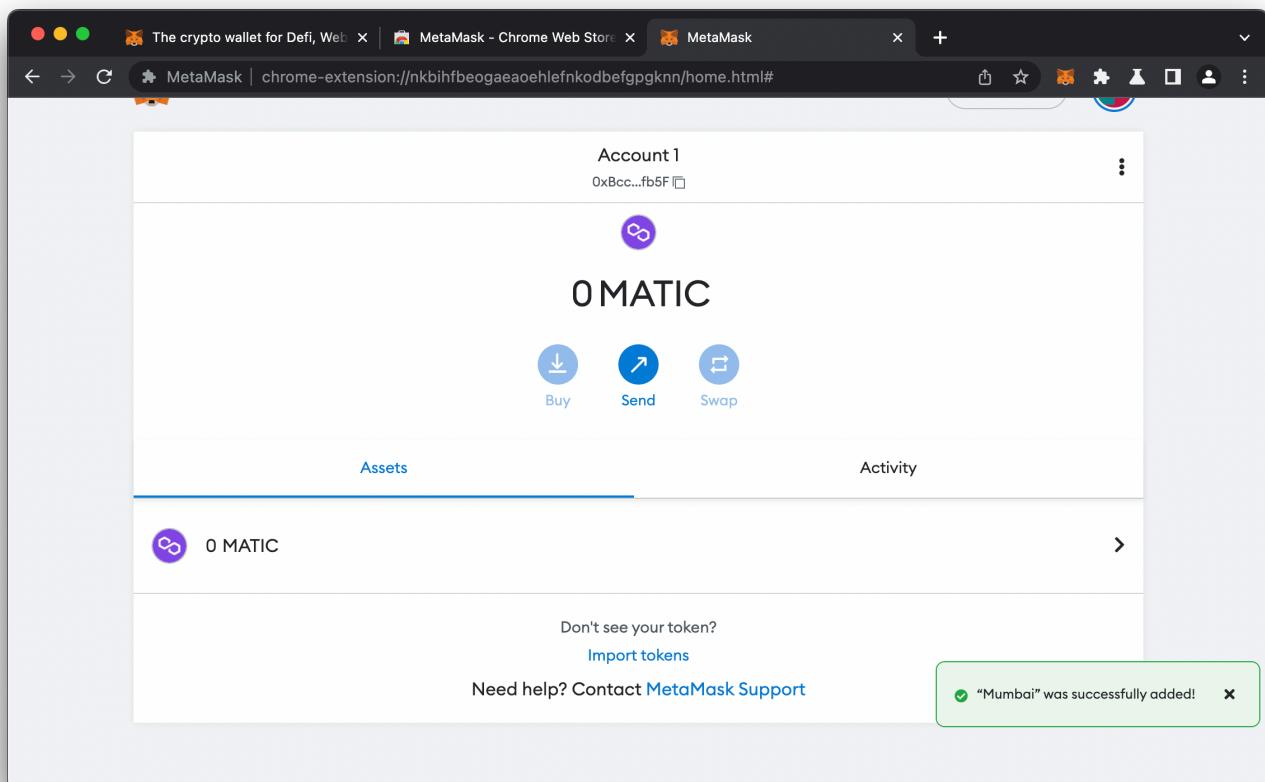


В открывшемся окне нужно заполнить данные для подсоединения. Источником истины здесь являются документация сети [Polygon](#) и список сетей [ChainList](#).

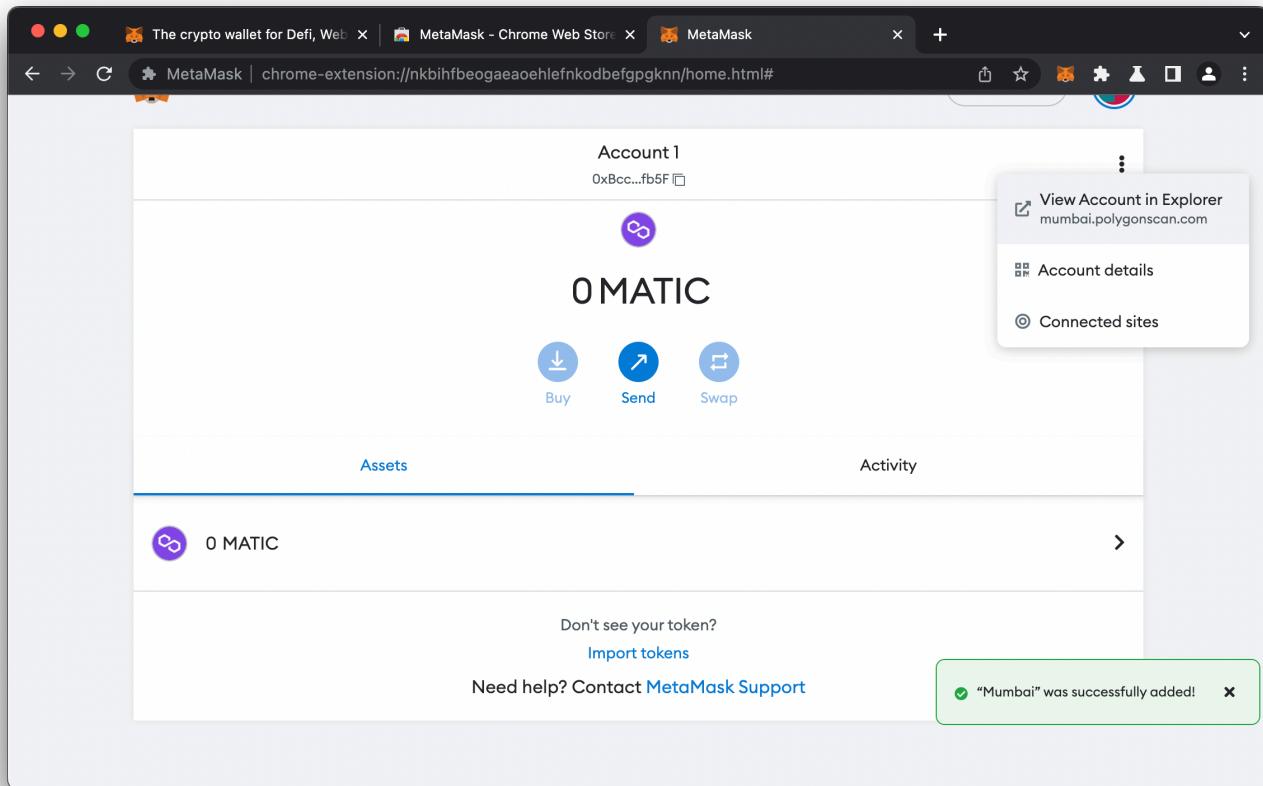
- Network Name: `Mumbai`
- RPC URL: `https://rpc-mumbai.maticvigil.com`
- Chain ID: `80001`
- Currency Symbol: `MATIC`
- Block Explorer URL: `https://mumbai.polygonscan.com/`



Если всё прошло хорошо, МетаМаск переключится на сеть Mumbai.



Вы можете посмотреть на содержимое вашего кошелька с точки зрения блок-эксплорера. Щёлкните на гамбургер в правой стороне блока с адресом. В выпадающем меню выберите пункт просмотра на эксплорере.



В соседней вкладке откроется окошко с эксплорером (<https://mumbai.polygonscan.com/>). Как сможете убедиться, ваш свежесозданный аккаунт пуст.

The screenshot shows the PolygonScan interface for the address 0xbcc...fb5f. The top navigation bar includes links for Home, Blockchain, Tokens, Misc, and Testnet. The main content area has two sections: 'Overview' and 'More Info'. The 'Overview' section shows a balance of 0 MATIC. The 'More Info' section shows 'My Name Tag: Not Available'. Below these are tabs for 'Transactions' and 'ERC-20 Token Txns', with the 'Transactions' tab selected. A search bar at the top right allows searching by Address / Txn Hash / Block / Token. The bottom of the page features a footer with links for Add Mumbai Network and Preferences.

Теперь наша задача - завести нативный токен на кошёлёк. Это тестовая сеть, так что мы воспользуемся краном (как на раковине, faucet). Для начала, скопируйте ваш адрес в буфер обмена: нажмите на блок с адресом.

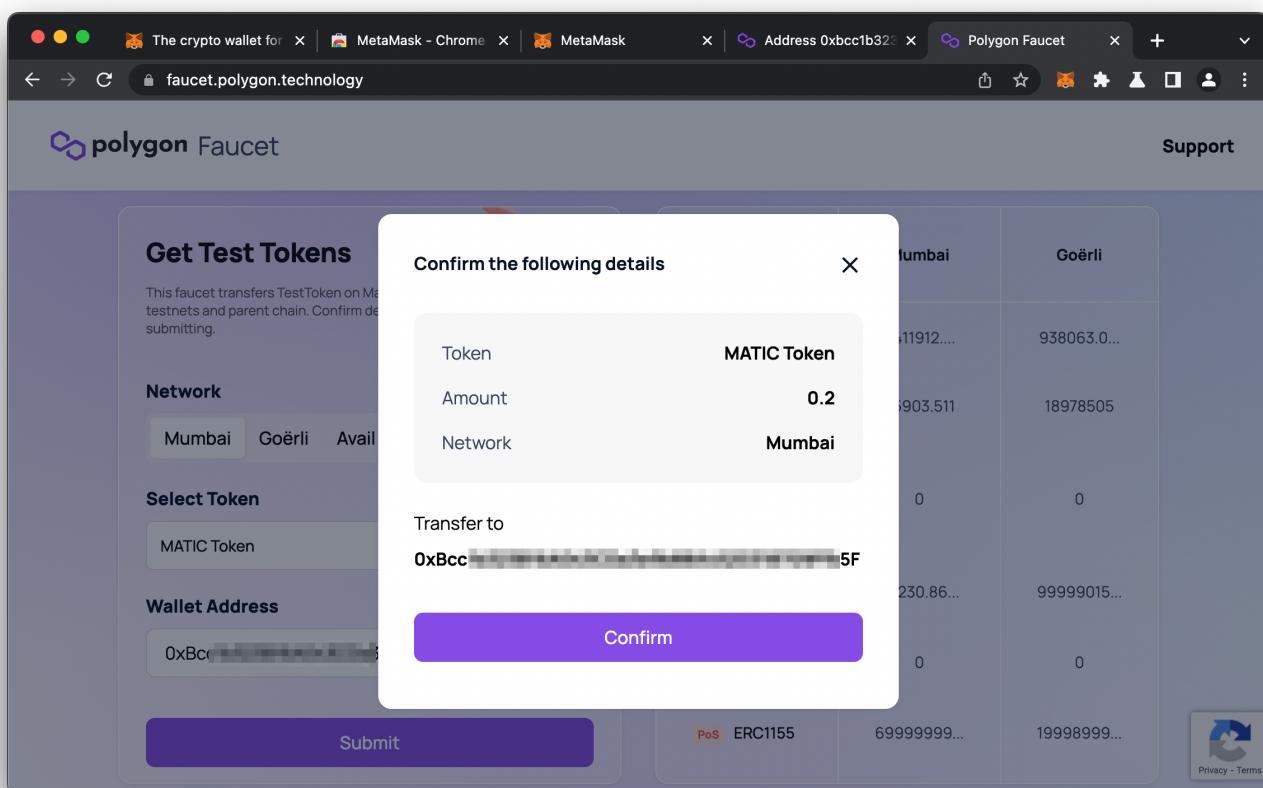
The screenshot shows the MetaMask extension interface. The address 0xbcc...fb5f is highlighted with a pink box. Below it, the balance is listed as 0 MATIC with three buttons: Buy, Send, and Swap. At the bottom, there are links for Assets, Activity, and Import tokens. A message at the bottom says 'Don't see your token? Import tokens' and 'Need help? Contact MetaMask Support'. A green notification box on the right says '“Mumbai” was successfully added!'. The browser tabs include 'The crypto wallet for Defi, Web3, and Ethereum' and 'MetaMask - Chrome Web Store'.

Зайдите на сайта крана <https://faucet.polygon.technology/> В поле адреса кошелька вставьте ваш эфириумный адрес.

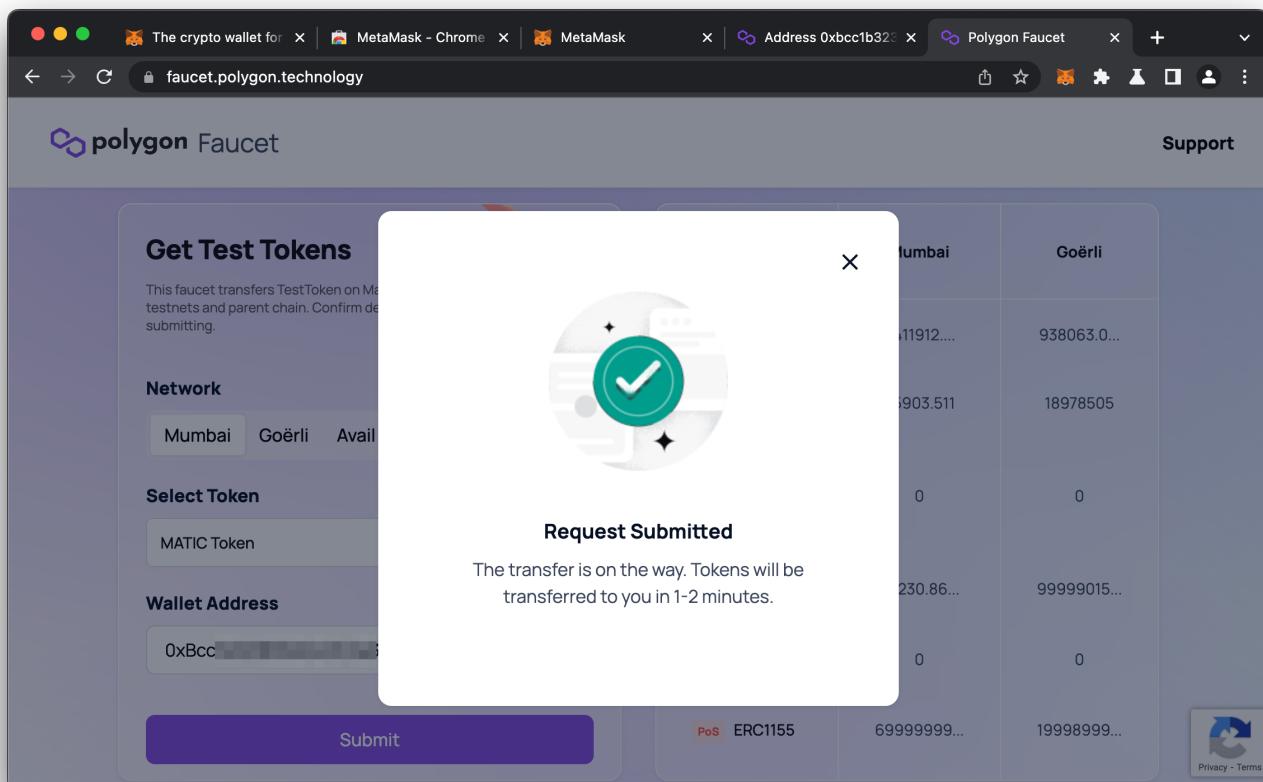
The screenshot shows the Polygon Faucet interface. On the left, there's a form titled 'Get Test Tokens' with fields for selecting a network (Mumbai, Goerli, Avail Devnet, Avail Testnet) and a token type (MATIC Token). A 'Wallet Address' field contains the placeholder '0xbcc...' and a 'Submit' button. The entire 'Wallet Address' input field is highlighted with a pink border. On the right, there's a table titled 'Test Balances' comparing Mumbai and Goerli networks across various token types: MATIC Token, PLASMA ERC20, PLASMA ERC721, PoS ERC20, PoS ERC721, and PoS ERC1155. The table shows the current balance for each category on both networks.

	Mumbai	Goerli
MATIC Token	9411912...	938063.0...
PLASMA ERC20	55903.511	18978505
PLASMA ERC721	0	0
PoS ERC20	39230.86...	99999015...
PoS ERC721	0	0
PoS ERC1155	69999999...	19998999...

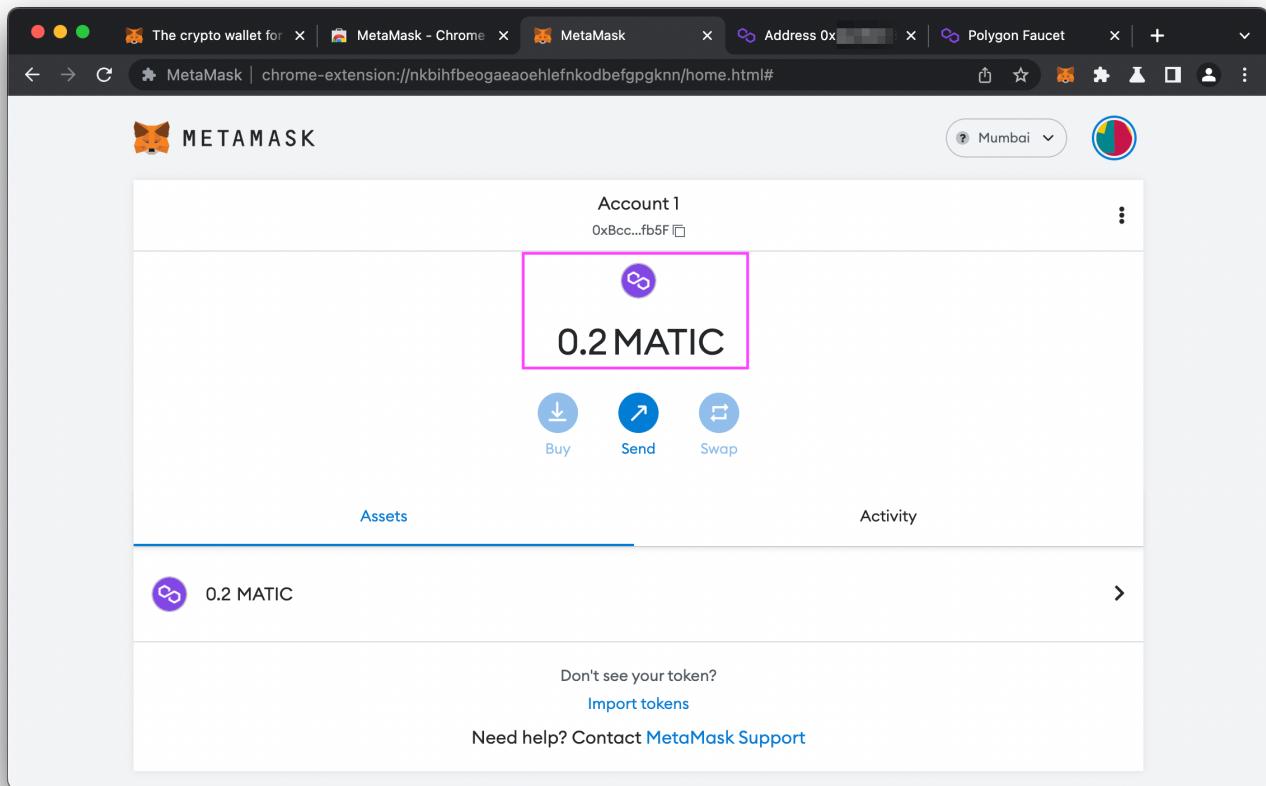
В качестве сети по умолчанию выбрана нужная нам сеть Mumbai. После заполнения поля адреса нажмите кнопку отправки формы и подтвердите намерение.



Появится подтверждение сервиса о переводе.

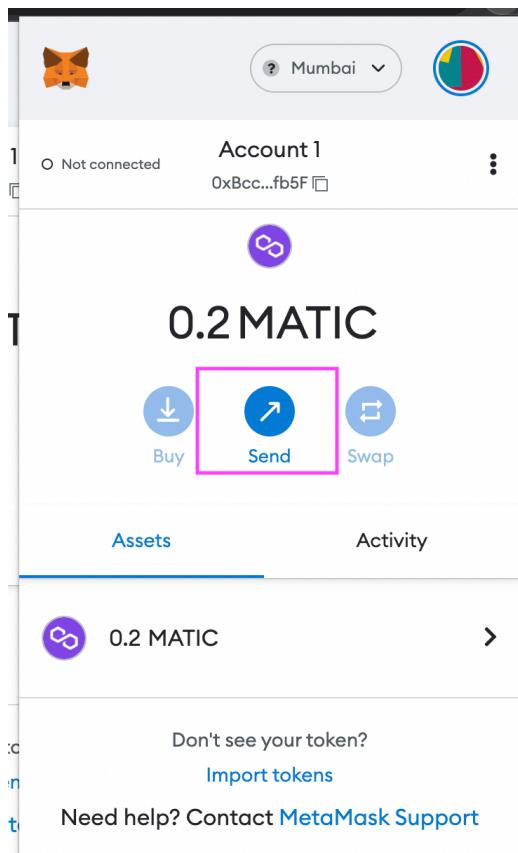


Через несколько минут вы можете открыть сайт эксплорера или ваш МетаМаск, убедившись, что до вас дошли отправленные с крана токены.



Теперь есть, чем посыпать транзакции.

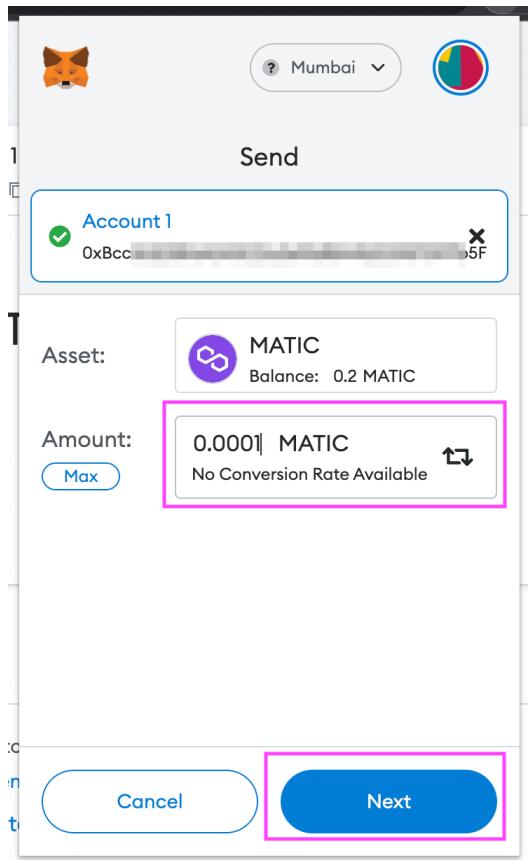
Попробуем послать себе транзакцию. Откройте кошельёк, нажав на иконку на панели инструментов браузера. Скопируйте ваш адрес в буфер обмена. Нажмите кнопку отправки транзакции.



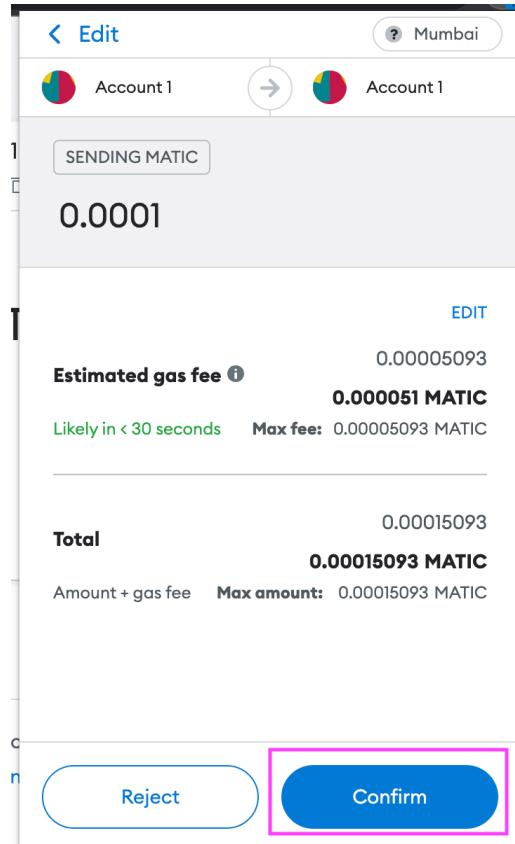
В появившемся интерфейсе введите ваш адрес в строку с адресом назначения.



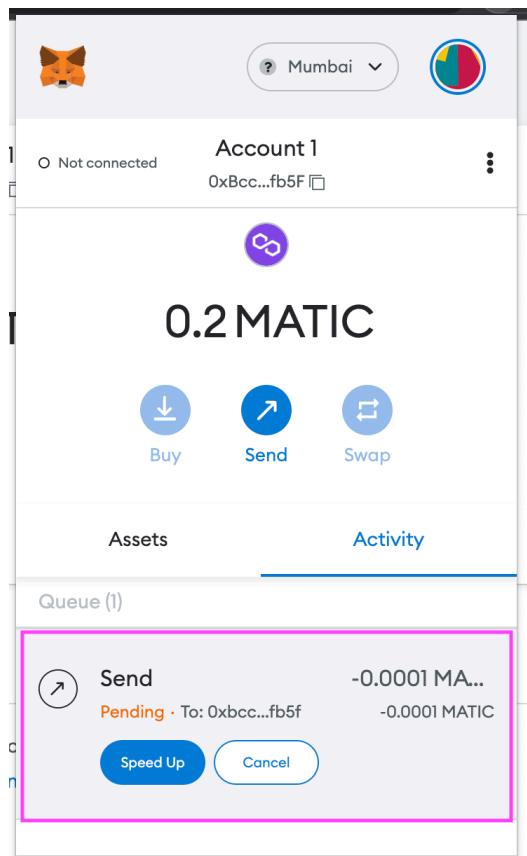
Через некоторое время интерфейс сменится. Теперь нужно ввести объём отправляемых токенов. Введите небольшую сумму, например `0.0001`.



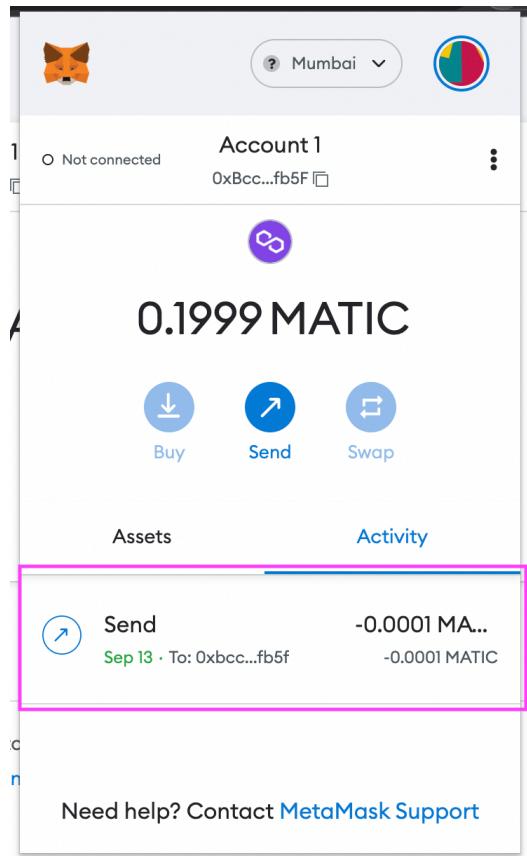
Нажмите кнопку продолжения. МетаМаск попросит вас проверить данные транзакции, включая количество газа, выделенного на транзакцию.



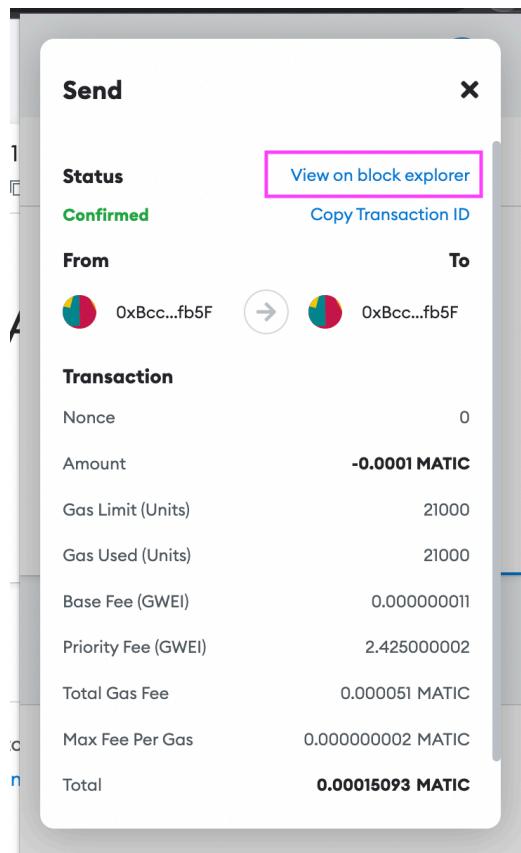
Теперь отправленная транзакция появится в списке транзакций со статусом Pending.



Через некоторое время, когда транзакцию замайнят, статус поменяется на Confirmed.



Вы можете просмотреть подробности транзакции, щёлкнув по ней в интерфейсе.



Вы также можете увидеть её в блок-эксплорере, щёлкнув на соответствующий элемент меню.

The screenshot shows a web browser window with multiple tabs open, including "The crypto wallet", "MetaMask - Chai", "MetaMask", "Address 0xbccc", "Polygon Faucet", and "Polygon Transaction". The main content is from "mumbai.polygonscan.com/tx/0x233...".

Transaction Details

Overview Logs (2)

[This is a Polygon PoS Testnet transaction only]

⑦ Transaction Hash: 0x233...324a ⓘ

⑦ Status: Success

⑦ Block: 280 ⓘ 61 Block Confirmations

⑦ Timestamp: 5 mins ago ⓘ

⑦ From: 0xbc...5f ⓘ

⑦ To: 0xbc...5f ⓘ

⑦ Value: 0.0001 MATIC (\$0.00)

⑦ Transaction Fee: 0.000050925000273 MATIC (\$0.00) 0.000050925000273 MATIC (\$0.00)

⑦ Txn Type: 2 (EIP-1559)

Click to see More ↴

⑦ Private Note: To access the Private Note feature, you must be [Logged In](#)

Если же в блок-эксплорере вы откроете свой адрес, не транзакцию, то вы можете увидеть вашу первую и пока единственную транзакцию. Заметьте, что баланс изменился на сумму комиссии за транзакцию.

The screenshot shows the PolygonScan interface for the address 0xbcc...5F. The balance is listed as 0.199949074999727 MATIC. A single transaction is shown, which is a transfer from SELF to the address 0xbcc...5F with a value of 0.0001 MATIC. The transaction was made 5 mins ago.

Txn Hash	Method	Block	Age	From	To	Value
0x233...	Transfer	28084403	5 mins ago	0xbcc...	SELF	0xbcc...5F 0.0001 MATIC

3. Сохранение секретной фразы безопасным способом

Полученную на первом этапе секретную фразу можно сохранить как есть. Очень желательно делать это на неэлектронном носителе. Для уверенности, секретную фразу можно разделить по схеме Шамира. Так, при схеме "2 из 3" вы получите 3 набора других секретных фраз. Оригинальную секретную фразу можно получить, сложив вместе любые два набора из трёх.

Для разделения секрета мы воспользуемся инструментом, созданным Яном Колманом: <https://iancoleman.io/shamir39/>

The screenshot shows the 'Split' section of the iancoleman.io/shamir39/ website. At the top, there's a navigation bar with links for English, 日本語, Español, 中文(简体), 中文(繁體), Français, and Italiano. Below the navigation, there's a text input field for generating a mnemonic, with a 'Generate' button and a dropdown menu set to 15 words. A 'Mnemonic Language' dropdown is also present. The main area has two sections: 'BIP39 Mnemonic' containing the phrase 'curve convince wink favorite trip', and 'Shamir39 Shares' containing three fragments of the mnemonic: 'shamir39-p1 ... cradle dwarf flat betray reject endorse age add cake', 'shamir39-p1 amused abandon hobby frame verb cute ...', and 'shamir39-p1 analyst abandon surface hazard ... fringe pulp rapid'. The 'Shamir39 Shares' section is highlighted with a pink border.

Split

Generate a random mnemonic, or enter your own below:

BIP39 Mnemonic: curve convince wink favorite trip

Shamir39 Shares:

shamir39-p1 ... cradle dwarf flat betray reject endorse age add cake

shamir39-p1 amused abandon hobby frame verb cute ...

shamir39-p1 analyst abandon surface hazard ... fringe pulp rapid

Combine

Shamir39 Shares:

В поле BIP39 Mnemonic введите вашу секретную фразу. Далее выберите параметры разделения. Для данной работы следует выбрать схему 2 из 3. В поле ниже появятся три строки, каждая из которых представляет фрагмент оригинальной секретной фразы. Каждый из них следует сохранить отдельно.

Для восстановления секретной фразы из фрагментов ниже на той же странице есть секция Combine. В поле Shares нужно внести любые 2 из 3 фрагментов. В поле BIP39 Mnemonic ниже появится ваша секретная фраза.

Shamir39 - Mnemonic Code S... X +

iancoleman.io/shamir39/

Combine

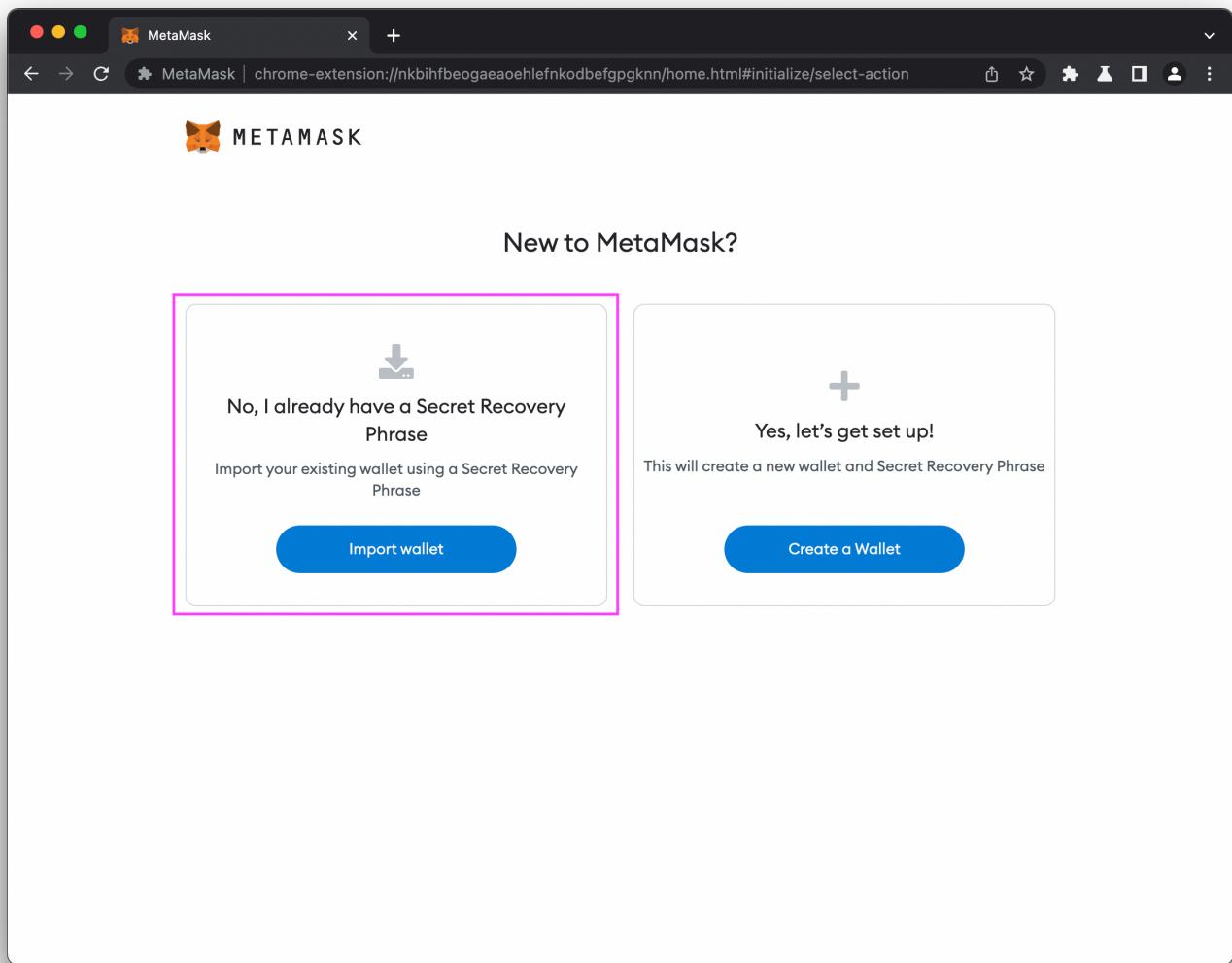
Shamir39 Shares	shamir39-p1 cradle dwarf flat betray reject endorse age add cake shamir39-p1 amused abandon hobby frame verb cute
BIP39 Mnemonic	curve convince wink favorite trip

More Info

Shamir39 Draft Specification
Read more about how Shamir Mnemonics are encoded and decoded in the [Draft Shamir39 Specification](#).
The specification is open to feedback. Feedback can be provided by raising a new issue in the [github repository iancoleman/shamir39](#).

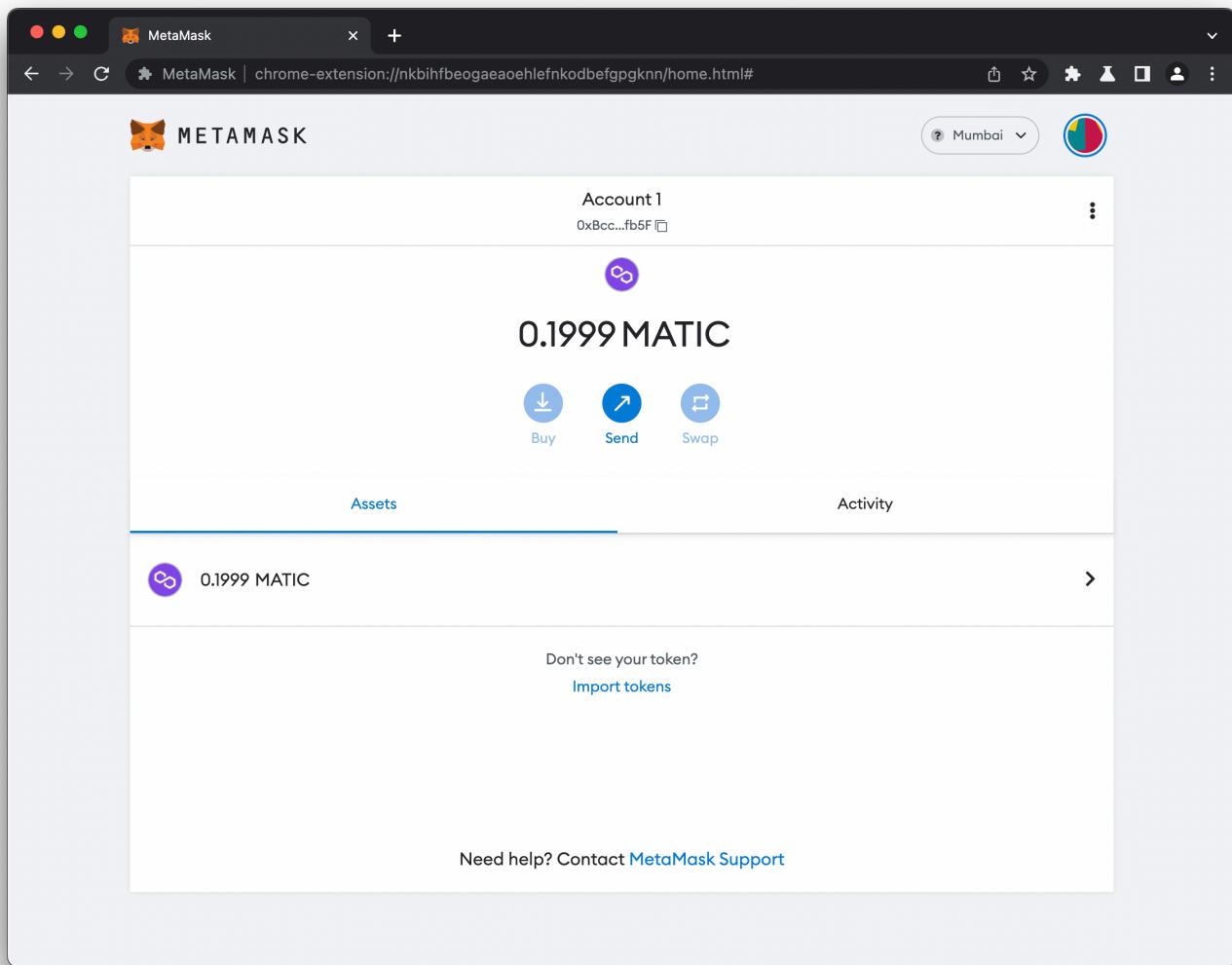
BIP39 Mnemonic code for generating deterministic keys
Read more at the [official BIP39 spec](#)

Теперь допустим, что вы лишились компьютера, браузера или Метамаска. Для симуляции подобного сценария, после сохранения фрагментов и восстановления секретной фразы через схему Шамира, удалите расширение Метамаск из браузера и установите его вновь. Метамаск предложит тот же сценарий онбординга, как мы проходили выше. На этот раз выберите импорт существующего кошелька.



Вставьте в появившиеся поля слова вашей секретной фразы, придумайте пароль. Пароль может отличаться от того пароля, который вы придумали выше.

Далее откроется МетаМаск с вашим адресом на сети Ethereum Mainnet. Перейдите на сеть Polygon Mumbai, и вы увидите ваш баланс, будто вы МетаМаск не удаляли. Подсказка: вместо заполнения полей для новой сети вы можете воспользоваться сервисом <https://chainlist.org/>.



Вопросы для самостоятельной проверки

- Где хранится баланс вашего кошелька?
- Что есть секретная фраза, с которой вы проводили операции в работе?
- Как создать несколько кошельков на одной секретной фразе в МетаМаске?
- В чём разница между различными блокчейн-сетями, в частности Ethereum Mainnet, Polygon Mumbai?
- Можно ли использовать один адрес на разных блокчейн-сетях?
- Куда ушла разница между первоначальным и последним балансом на кошельке?
- Как МетаМаск посылает транзакцию в распределённую блокчейн-сеть? Куда он шлёт данные, по какому протоколу?

Формат предоставления отчёта

Документ в PDF должен содержать:

- ваш созданный адрес в МетаМаске,
- ссылку на транзакцию отправки/получения токенов,
- скриншот страницы с блокчейн-эксплорера,
- краткий текст, объясняющий ваши действия.

Подготовьтесь к отчёту, ответив на вопросы выше. Чем глубже понимание ответов на вопросы, тем выше ваш балл.