

Использование Биткоина

Урок 1

Как взаимодействовать с блокчейном Биткоина на уровне
пользователя и разработчика



Знакомство и содержание урока

Борис Тахохов

Редактор внутренних коммуникаций Яндекс,
автор статей и видео о Web 3.0

Пользуюсь криптовалютами с 2017 года.
В 2020 году стал исследовать метавселенные и NFT, а также
рассказывать о них в крупнейших блокчейн-медиа.

- 🌟 1 млн просмотров канала Maff Media на YouTube
- 🌟 Организовывал мероприятия в метавселенных для Dating.com и Fringe Finance
- 🌟 Работал с криптобиржами Binance, Bybit и Broex

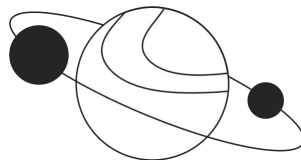




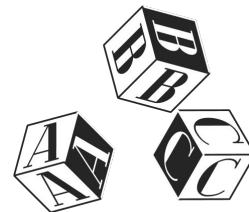
**Ответьте на несколько вопросов
сообщением в чат**



Как вас зовут?



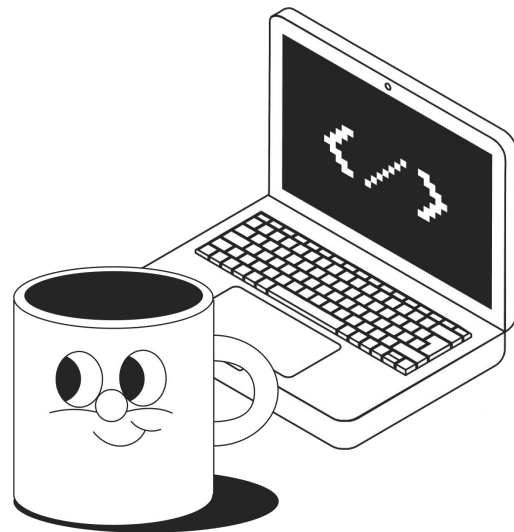
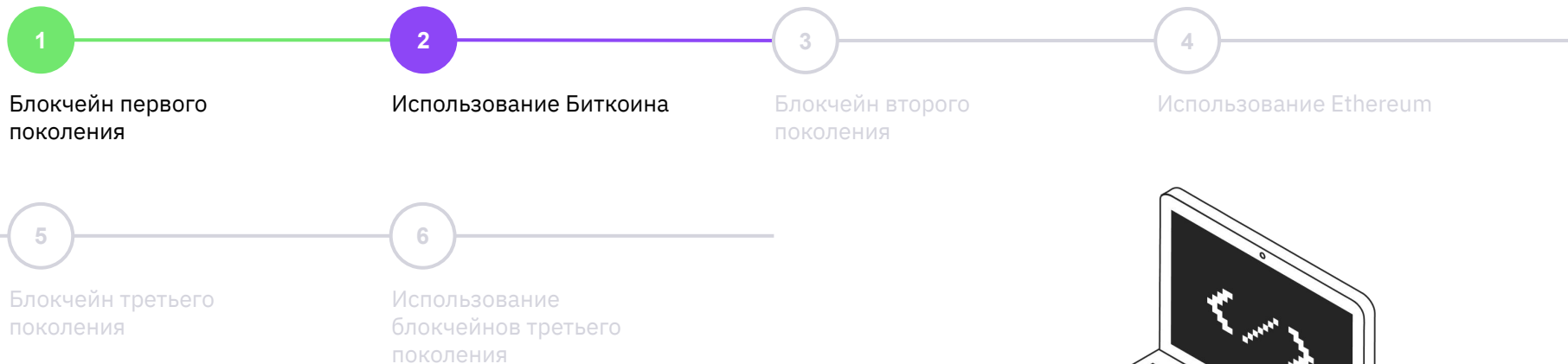
Откуда вы?



Ваш любимый блокчейн?



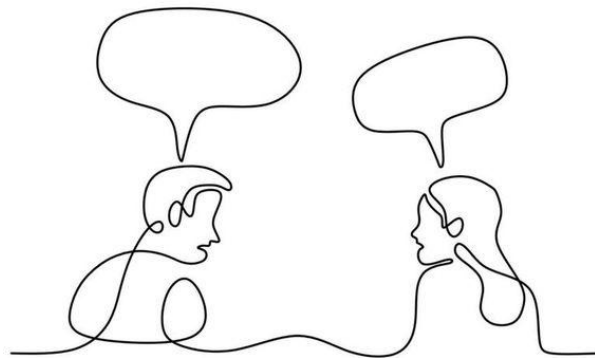
План курса “Блокчейн”





Что будет на уроке сегодня

- 📌 Научимся работать с биткоин-кошельками.
- 📌 Познакомимся с библиотекой BitcoinJS.





Вопросы?

Вопросы?



Вопросы?





Вспомним, что было на лекции





Задание 1. Создать Биткоин-кошелек

Electrum — удобный кошелёк со множеством настроек. Но можно использовать и аналоги.

- Перейдите на сайт <https://electrum.org/>.
- Установите подходящую версию кошелька.



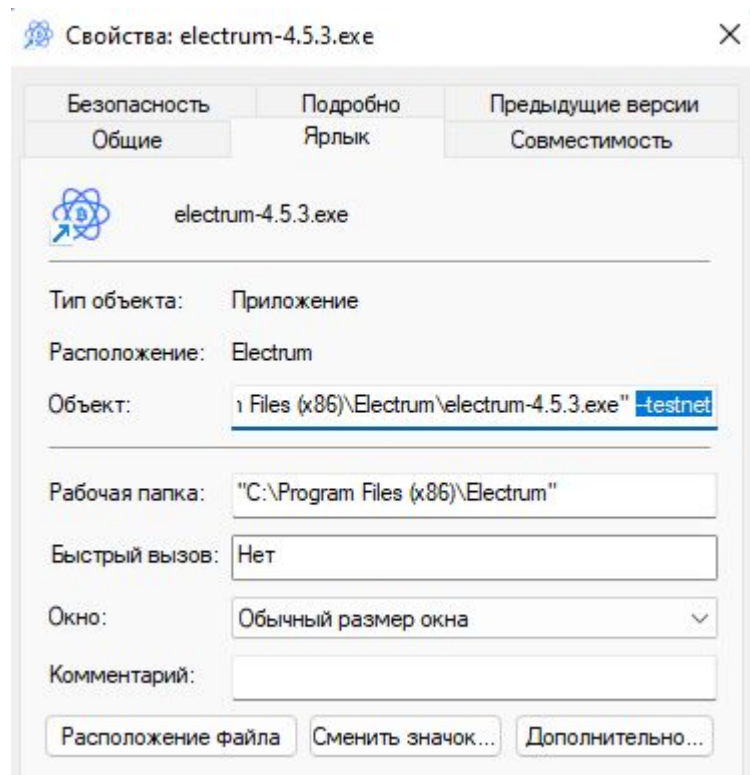
10 минут



Задание 2. Подключиться к тестовой сети

Для того, чтобы познакомиться с функционалом кошелька и не потратить денег понадобится тестовая сеть.

- Чтобы Electrum подключался к тестовой сети, в свойствах ярлыка на рабочем столе к расположению объекта нужно добавить параметр `--testnet`
- Для удобства лучше скопировать основной ярлык Electrum, чтобы на рабочем столе осталось две иконки — одна для основной сети, другая для тестовой.






Задание 3. Получить тестовые биткоины

Есть много сайтов, на которых размещена простая веб-форма, позволяющая получать тестовые биткоины.

- Перейдите на сайт <https://faucet.triangleplatform.com/bitcoin/testnet>, либо найдите аналог по запросу “Bitcoin testnet faucet”.
- Самостоятельно найти способ пополнить Electreum тестовыми биткоинами.

 10 минут




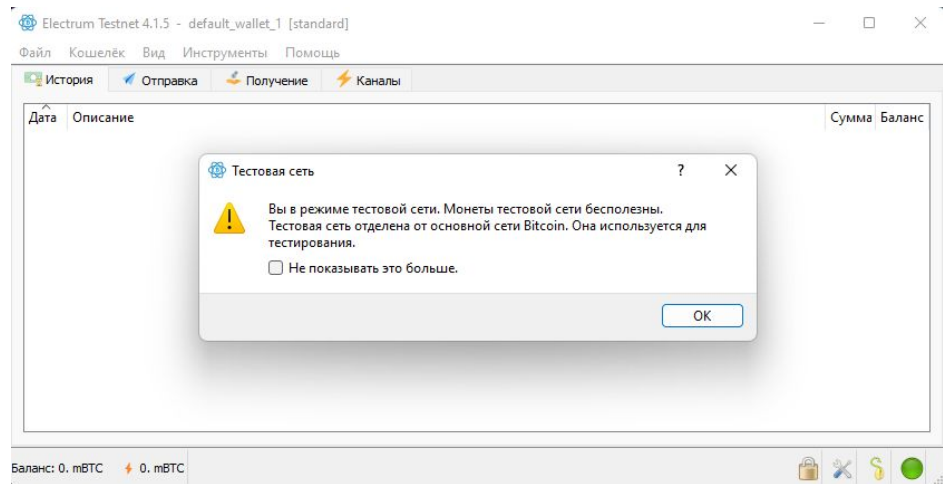


Задание 4. Отправить BTC

Обратите внимание, что в Electrum есть возможность генерировать новые адреса для каждой новой операции.

- Отправьте свой адрес в чат.
- Разделитесь на пары и обменивайтесь биткоинами.
- Измените блокчейн-обозреватель в настройках.
- Поделитесь ссылкой на транзакцию в блокчейн-обозревателе.

 10 минут





Задание 5. Другие функции Electrum

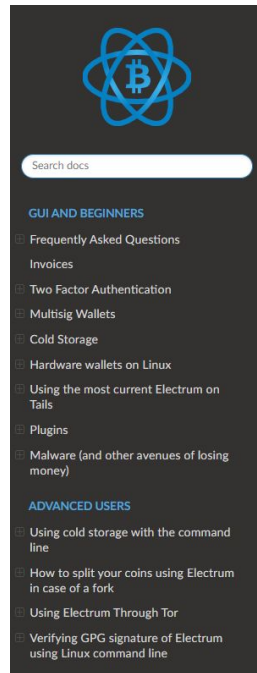
У Electrum много функций для продвинутых пользователей. Попробуйте разобраться, как они работают:

- Подписать/подтвердить сообщение.
- Зашифровать/расшифровать сообщение.
- Консоль.

Все консольные команды и прочие функции Electrum можно найти в официальной документации — <https://electrum.readthedocs.io/en/latest/index.html>



10 минут



🏠 / Welcome to the Electrum Documentation!

[Edit on GitHub](#)

Welcome to the Electrum Documentation!

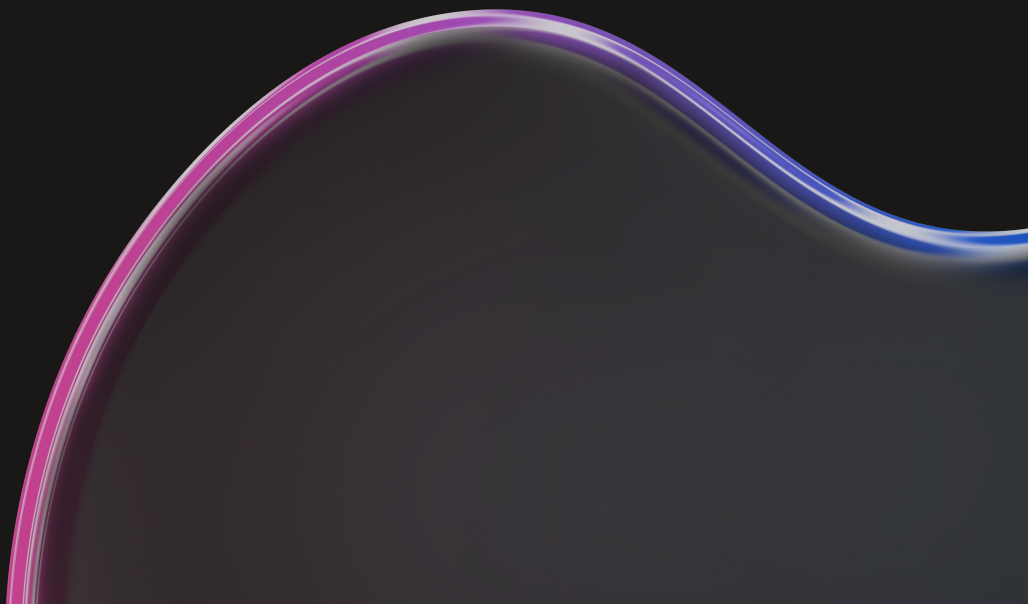
Electrum is a lightweight Bitcoin wallet.

GUI and beginners

- Frequently Asked Questions
 - How does Electrum work?
 - Does Electrum trust servers?
 - What is the seed?
 - How secure is the seed?
 - I have forgotten my password. What can I do?
 - How does Electrum get the Bitcoin price it uses?
 - My transaction has been unconfirmed for a long time. What can I do?
 - What does it mean to "freeze" an address in Electrum?
 - How is the wallet encrypted?
 - Does Electrum support cold wallets?
 - Can I import private keys from other Bitcoin clients?
 - Can I sweep private keys from other Bitcoin clients?
 - Where is the Electrum datadir located?
 - Where is my wallet file located?
 - How to enable debug logging?
 - Can I do bulk payments with Electrum? (batching)
 - Can Electrum create and sign raw transactions?
 - Electrum freezes when I try to send bitcoins.
 - What is the gap limit?
 - How can I pre-generate new addresses?
 - How do I upgrade Electrum?



Перерыв

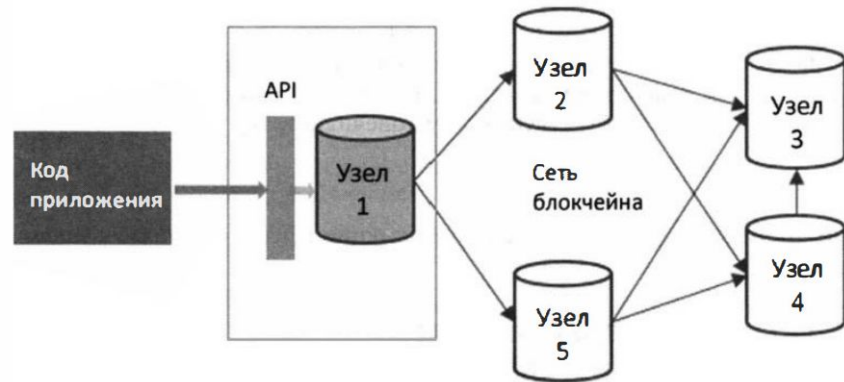




Задание 6. Библиотека BitcoinJS

Подобное Electrum приложение, мы можем создать самостоятельно и взаимодействовать с узлами Биткоина с помощью API. Для этого установим библиотеку BitcoinJS:

- Инициализируйте среду выполнения node.js с помощью команды `npm init`.
- Создайте точку входа для нашего приложения — файл `index.js` и пользовательский модуль для вызова функций библиотеки BitcoinJS — файл `btc.js`.
- Импортируйте `btc.js` в `index.js`.





Задание 7. Создание ключей

Первое, что понадобится для работы с любым блокчейном — это пара ключей.

Выполните приведенный фрагмент кода. В нём используется класс `ECPair` библиотеки `BitcoinJS` и вызывается метод `makeRandom` для создания случайных пар ключей для тестовой сети.

```
var getKeys = function () {  
  
    var aliceKeys = btc.ECPair.makeRandom({  
        network: network  
    });  
  
    var bobKeys = btc.ECPair.makeRandom( {  
        network: network  
    });  
  
    var alicePublic = aliceKeys.getAddress();  
    var alicePrivate = aliceKeys.toWIF();  
    var bobPublic = bobKeys.getAddress();  
    var bobPrivate = bobKeys.toWIF () ;  
  
    console.log(alicePublic, alicePrivate,  
bobPublic, bobPrivate);  
};
```



20 минут



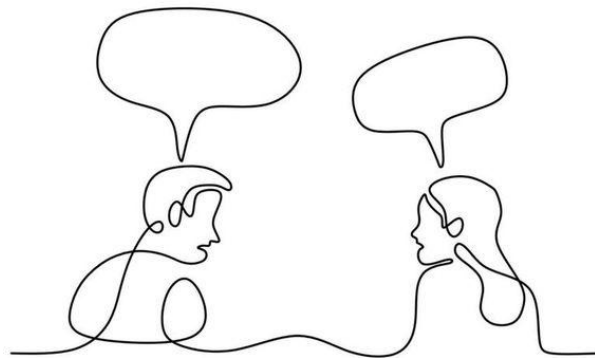
Подведение итогов



Если вам понадобится создавать более сложные приложения для работы с Биткоином, теперь вы знаете к какой библиотеке обращаться!



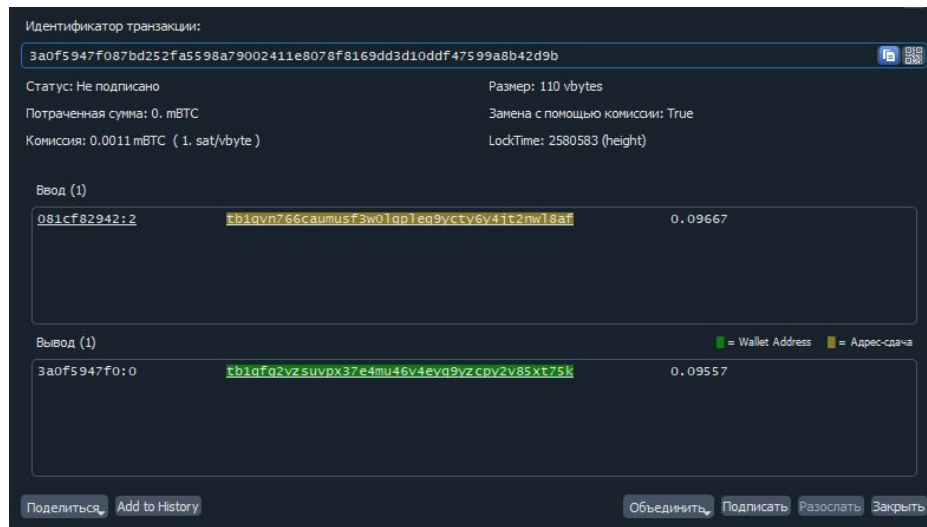
Вы умеете использовать биткоин-кошельки и понимаете, как в них устроены адреса.





Домашнее задание

1. Пополните адрес alicePublic тестовыми биткойнами.
2. Переведите тестовые биткойны с адреса alicePublic на любой из своих адресов в Electrum-кошельке. Для этого воспользуйтесь функцией “Кошелёк->Приватные ключи->Импорт” и введите туда значение alicePrivate.
3. Отправьте ссылку на транзакцию или скрин транзакции и объясните, что произошло.



20 минут



Вопросы?

Вопросы?



Вопросы?





Спасибо за внимание