



Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Лабораторная работа № 1 «Введение в Bitcoin»

по курсу «Распределенные системы обработки информации и
блокчейн технологии»

Калуга, 2025

Цель и задачи работы, требования к результатам ее выполнения

Целью выполнения лабораторной работы является формирование теоретических знаний и практических навыков по работе с децентрализованной платформой Bitcoin.

Основными задачами выполнения лабораторной работы являются:

1. получить теоретический знания о устройстве децентрализованной платформе Bitcoin;
2. получить практические навыки работы (майнинга) с децентрализованной платформой Bitcoin;
3. научиться устанавливать необходимые компоненты для работы с Bitcoin;
4. овладеть навыками создания и использования электронного кошелька.
5. понять процесс майнинга и научиться использовать майнер на примере Bitcoin

Результатами работы являются:

- созданный аккаунт для электронного кошелька Bitcoin;
- созданный аккаунт на одном из пулов Bitcoin;
- установленный и настроенный майнер;
- запущенный процесс майнинга;
- подготовленный отчет.

Краткая характеристика объекта изучения, исследования

1. Необходимость криптовалюты

Интернет-коммерция в большинстве случаев опирается на финансовые учреждения, выступающие в роли доверенных посредников для проведения электронных платежей. Такая схема хорошо работает для большинства транзакций, но в ее основе лежит доверие, что влечет определенные проблемы.

Необходима платежная система, основанная на криптографии, а не на доверии, которая позволила бы любым двум участникам осуществить перевод средств напрямую, без участия посредника. Вычислительная дороговизна отмены транзакций оградила бы продавцов от мошенничества, а легкоосуществимые механизмы эскроу защитили бы покупателей.

Система находится в безопасности, пока под совокупным контролем ее честных участников находится больше вычислительной мощности, чем под контролем группы действующих совместно злоумышленников.

2. Транзакции

Определим электронную монету как последовательность цифровых подписей. Очередной владелец отправляет монету следующему, подписывая хэш предыдущей транзакции и публичный ключ будущего владельца и присоединяя эту информацию к монете. Получатель может проверить каждую подпись, чтобы подтвердить корректность всей цепочки владельцев (рисунок 1).

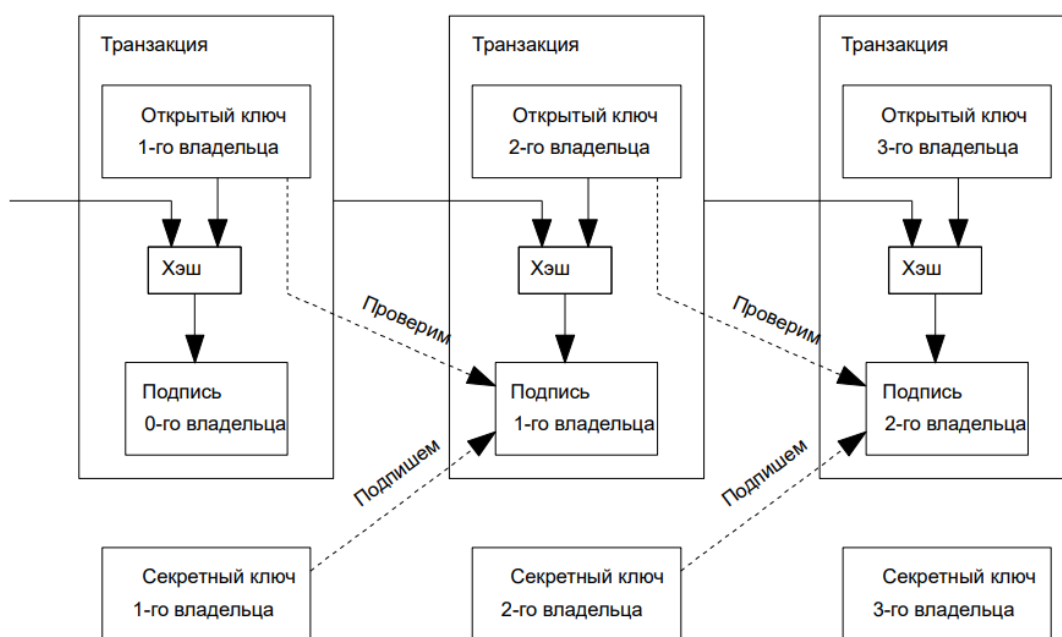


Рисунок 1 – Цепочка транзакций.

Адресат должен знать, что никто из предыдущих владельцев не подписал транзакцию, предшествующую по времени той, что находится в цепочке отправленной ему монеты. Для наших целей лишь первая транзакция из нескольких является истинной, поэтому мы не должны беспокоиться о поздних попытках двойной траты.

Чтобы избавить схему от посредника, участникам необходимо открыто публиковать транзакции, а также уметь приходить к согласию относительно единого порядка их следования. Получателю нужно доказательство того, что для каждой транзакции из цепочки большинство пользователей согласны считать ее первой.

3. BTC и майнинг

Общий объем эмиссии биткоинов ограничен и не превысит 21 млн. К середине 2016 года больше половины криптовалюты было уже сгенерировано.

Биткоины можно купить на бирже или "добывать", проводя вычисления. Во втором случае компьютер (или центр обработки данных) владельца решает сложные математические задачи, получая в качестве награды виртуальные деньги.

Все проходящие транзакции проходят через майнеров: их компьютеры должны проверить достоверность перевода с помощью секретного ключа и информации о всех новых транзакциях. Если подтверждение операции произошло, за формирование блока майнер раньше получал награду в 25 биткоинов. Каждые четыре года система сокращает размер вознаграждения, и уже в 2017 году оно было меньше ровно вдвое.

4. Узлы

Узел (node) — это просто компьютер, на котором запущена биткоин-клиент. Что еще более важно, узел подключен к другим компьютерам (под управлением той же программы) для создания сети Bitcoin. Другими словами, сеть Bitcoin состоит из узлов (node).

Каждый узел (биткоин-клиент) запрограммирован на выполнение набора правил. Следуя этим правилам, узел может проверять транзакции, которые он получает, и ретранслировать их, если с ними всё в порядке. При возникновении каких-либо проблем транзакция не передается далее в сеть Bitcoin.

Основная работа узла заключается в обмене информацией с другими узлами, и квинтэссенцией информации, которую узел передает, являются **транзакции**.

Как уже упоминалось, каждый узел также хранит блоки подтвержденных транзакций. Они хранятся вместе в файле (базе данных) под названием блокчейн (blockchain).

5. Присоединение к сети биткойн

Все, что нужно сделать, чтобы присоединиться к сети биткойна, это загрузить (и запустить) биткоин-клиент. При запуске клиент подключится к другим узлам сети и начнет загрузку полной копии блокчейна (файла,

содержащего все проверенные транзакции). После этого клиент начнет получать транзакции с других узлов и ретранслировать их по сети.

Для работы с биткойном необязательно быть частью сети и хранить весь блокчейн на своем ПК. Можно отправлять и получать биткойны, не будучи узлом, нужно просто отправить транзакцию в Биткойн-сеть.

Майнинг Биткойна (BTC)

Для майнинга биткойна **без** создания собственного узла блокчейна (node) и его последующей синхронизации понадобятся:

- Биткойн кошелек.
- Зарегистрированный аккаунт на одном из пулов.
- Майнер.

1. Биткойн кошелек

Чтобы хранить биткойны и тратить их - потребуется биткойн-кошелек. Строго говоря, сами биткойны нигде не хранятся, а задача кошелька – хранение цифровых ключей, которые обеспечивают доступ к биткойн-адресу и возможность подписывать транзакции. Помните, что операции с криптовалютами нельзя отменить, поэтому, если вы планируете иметь дело с электронными монетами, вам нужно завести безопасный биткойн-кошелек.

Имеется огромный выбор из криптовалютных кошельков. Они бывают для ПК, Браузера или для мобильных устройств.

Подойдет любой кошелек. Для примера можно использовать простой веб-кошелек **Coinbase** (<https://www.coinbase.com/ru>). Регистрация не вызовет трудностей – она, как и везде, происходит с помощью e-mail.

После регистрации в правом верхнем углу нажмите кнопку “Получение и отправка”, далее должно появиться окно, на котором перейдите на вкладку

“Получить”, где и будет биткойн адрес (рисунок 2). Этот адрес нам понадобится дальше.

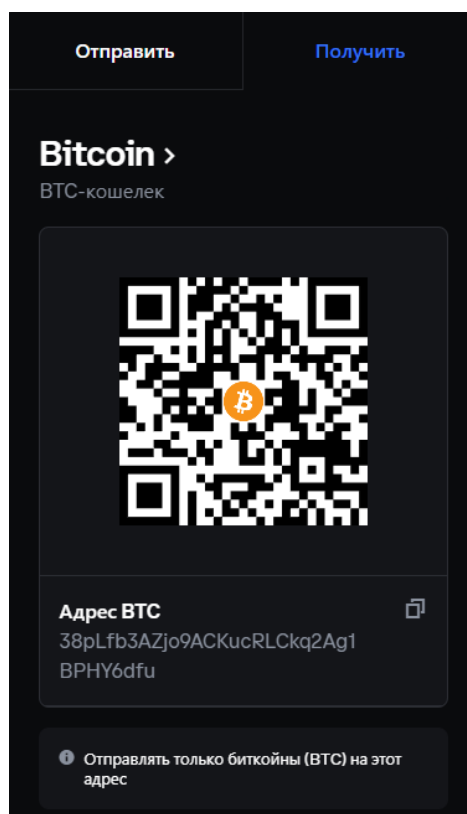


Рисунок 2 – Адрес BTC.

2. Пул

Пул – Это решение, позволяющее майнерам совместно добывать биткойн или другую криптовалюту. В рамках пула специальное программное обеспечение дает возможность майнерам совместно обрабатывать транзакции криптовалюты и генерировать записи для очередного блока.

Существует множество пулов. Для примера остановимся на f2pool (<https://www.f2pool.com/>). Регистрация не вызывает трудностей, кроме одной особенности – почти все пулы требуют двухфакторную аутентификацию, например, через Google Authenticator.

После регистрации нажмите справа сверху на имя своего аккаунта – далее на “Account settings”. Вы попадете на страницу с майнинг аккаунтами. Нажмите на имя своего аккаунта и на кнопку Add BTC Address. На этом шаге

и потребуется привязать двухфакторную аутентификацию. После привязки должно появиться окно (рисунок 3), в которое нужно вставить номер BTC кошелька, созданного нами ранее и ввести код из аутентификатора для подтверждения действия.

Before adding or changing your address, please confirm whether the address you are using has the required minimum deposit amount to avoid unnecessary losses.

BTC Address [Add Partner Wallet](#) [Recommend](#)

[Test if it's a partner wallet](#)

Address Source Description (Optional)

Sync BTC Payout Address with Mining Accounts (Optional)

Two-Factor Authentication Code

[Lost your device?](#)

OK

Рисунок 3 – Окно добавления BTC кошелька

Справа, около своего имени, выберите нужную криптовалюту (BTC). Вы попадете на страницу, где можно отслеживать майнинг. Ниже есть раздел, называющийся Pool URL. Нам понадобится любой из перечисленных адресов для майнинга.

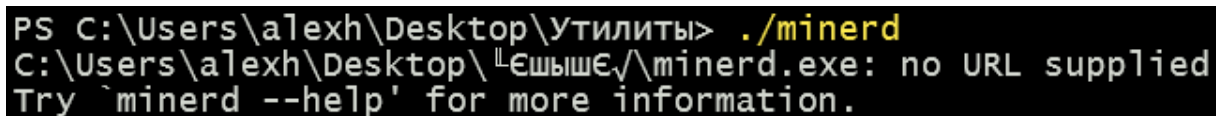
3. Майнер

Выбор майнера зависит от используемого оборудования. Существуют майнеры для видеокарт, процессоров и специального оборудования для майнинга. Есть специальные программы даже для разных производителей видеокарт. Для примера можно выбрать CPU Miner (скачать можно по ссылке:

<https://sourceforge.net/projects/cpuminer/files/>, либо через [git: https://github.com/pooler/cpuminer](https://github.com/pooler/cpuminer)), при выполнении лабораторной работы вы можете выбрать любой майнер. Данный майнер работает на процессоре (что не очень эффективно, но для обучения пойдет.)

ВНИМАНИЕ! Скачивайте майнеры только с проверенных источников (например: через официальные GIT репозитории).

В архиве будет находится файл с майнером (minerd.exe). Извлеките данный файл в удобное место. После чего в терминале (powershell, cmd и т.д.) нужно переместится в каталог, где находится файл. Для проверки работы CPU miner введите “./minerс”. Появится сообщение об ошибке, т.к. мы не указали параметры майнинга (рисунок 4)



```
PS C:\Users\alexh\Desktop\Утилиты> ./minerd
C:\Users\alexh\Desktop\Утилиты> ./minerd.exe: no URL supplied
Try 'minerd --help' for more information.
```

Рисунок 4 – Проверка майнера

Вы можете ввести данную команду (./minerd --help) чтобы получить подробную информацию о опциях майнера. Для корректной работы необходимо предоставить правильные опции майнеру.

Для майнинга на любом майнере необходимы: Адрес пула (Pool URL), Имя работника (Worker), и его пароль. Адрес пула мы получили выше (например: stratum+tcp://btc.f2pool.com:1314), имя работника – это имя аккаунта + номер работника (разделяется точкой) – например: “myname.001”, пароль может быть произвольным. Подробная инструкция для f2pool майнинга: <https://f2pool.io/mining/guides/how-to-mine-bitcoin/>.

В случае с CPU miner исходная строка запуска должна выглядеть следующим образом:

```
./minerd.exe --url=<URL> --userpass=<USER>.<WORKER_ID>:<PASSWORD>
```

При запуске должно происходить следующее (рисунок 5):

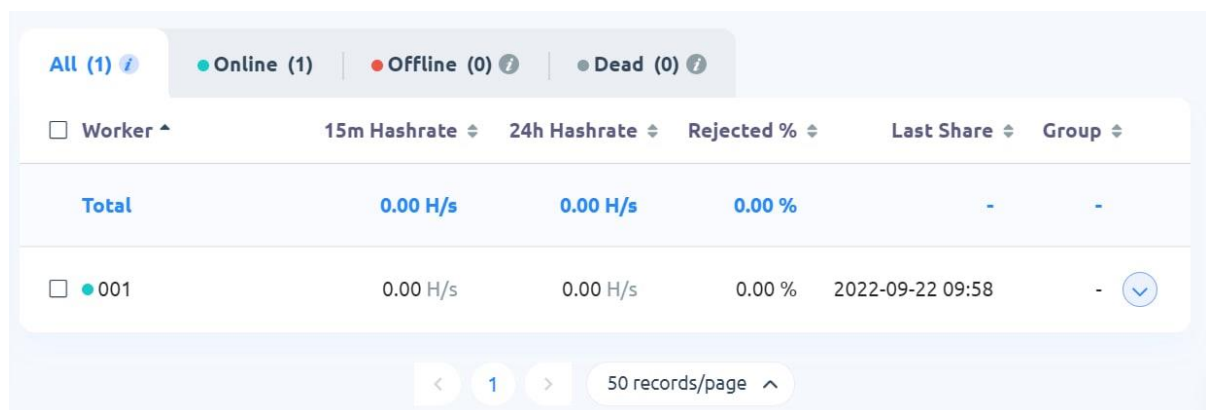
```

$ ./minerd.exe --url=stratum+tcp://btc.f2pool.com:1314 --userpass=alexhromov.001:123
[2022-09-22 20:54:04] Starting Stratum on stratum+tcp://btc.f2pool.com:1314
[2022-09-22 20:54:04] Binding thread 0 to cpu 0
[2022-09-22 20:54:04] Binding thread 2 to cpu 2
[2022-09-22 20:54:04] 4 miner threads started, using 'scrypt' algorithm.
[2022-09-22 20:54:04] Binding thread 3 to cpu 3
[2022-09-22 20:54:04] Binding thread 1 to cpu 1
[2022-09-22 20:54:04] Stratum requested work restart
[2022-09-22 20:54:06] thread 2: 4104 hashes, 10.72 khash/s
[2022-09-22 20:54:06] thread 3: 4104 hashes, 10.69 khash/s
[2022-09-22 20:54:06] thread 1: 4104 hashes, 10.61 khash/s
[2022-09-22 20:54:06] thread 0: 4104 hashes, 10.62 khash/s
[2022-09-22 20:55:08] thread 1: 636852 hashes, 10.22 khash/s
[2022-09-22 20:55:08] thread 0: 636912 hashes, 10.20 khash/s
[2022-09-22 20:55:08] thread 3: 641676 hashes, 10.21 khash/s
[2022-09-22 20:55:09] thread 2: 643356 hashes, 10.21 khash/s
[2022-09-22 20:56:05] thread 1: 613032 hashes, 10.71 khash/s
[2022-09-22 20:56:05] thread 0: 612048 hashes, 10.67 khash/s
[2022-09-22 20:56:06] thread 3: 612336 hashes, 10.67 khash/s
[2022-09-22 20:56:06] thread 2: 612792 hashes, 10.68 khash/s

```

Рисунок 5 – Процесс майнинга на процессоре

Спустя минут 10-20 результат так же должен появиться в f2pool (вкладка Workers) (рисунок 6):



The screenshot shows the 'Workers' tab in the f2pool dashboard. At the top, there are filters for 'All (1)', 'Online (1)', 'Offline (0)', and 'Dead (0)'. Below this is a table with columns: Worker, 15m Hashrate, 24h Hashrate, Rejected %, Last Share, and Group. The table has two rows: a 'Total' row and a row for worker '001'. Both rows show 0.00 H/s for the 15m and 24h hashrates, 0.00 % for rejected shares, and a last share time of 2022-09-22 09:58. The worker '001' is marked as 'Online' with a green dot. At the bottom, there are navigation arrows, a page number '1', and a dropdown for '50 records/page'.

Worker	15m Hashrate	24h Hashrate	Rejected %	Last Share	Group
Total	0.00 H/s	0.00 H/s	0.00 %	-	-
001	0.00 H/s	0.00 H/s	0.00 %	2022-09-22 09:58	-

Рисунок 6 – Отслеживание процесса майнинга в f2pool.

Так как майнинг на процессоре слишком неконкурентоспособный, то и хешрейт майнинга на скриншоте около 0.

Задание на лабораторную работу

- 1) Изучить теоретическую часть лабораторной работы.
- 2) Зарегистрироваться на электронном кошельке Bitcoin (на выбор)
- 3) Зарегистрироваться на пуле (на выбор). Внимание! Желательно, чтобы к пулу можно было привязать созданный ранее биткойн-кошелек
- 4) Скачать майнер (на выбор)
- 5) Запустить процесс майнинга.
- 6) Показать результаты майнинга (в терминале / интерфейсе пула)

Контрольные вопросы

- 1) Что такое транзакция? Что содержится в транзакции? Чем подписана транзакция?
- 2) Какой механизм используется для защиты Bitcoin блокчейн от фальсификации? Опишите этот механизм.
- 3) Что такой майнинг? Что обозначает термин "майнер"?
- 4) За что майнеры получают вознаграждение? Как оно рассчитывается?
- 5) Как подключиться к сети Bitcoin?
- 6) Что такое синхронизация блокчейна? Для чего она нужна?
- 7) Что такое "узлы" блокчейна?
- 8) Как создать электронный Bitcoin-кошелек, какие бывают кошельки?
- 9) Что такое пулы, для чего они нужны?
- 10) Как зарегистрироваться на пуле?
- 11) Как использовать конфигурацию пула?
- 12) На основе каких принципов выбирается майнер?
- 13) Какой алгоритм запуска майнера?

Форма отчета по лабораторной работе

На выполнение лабораторной работы отводится 3 занятия (6 академических часов: 5 часов на выполнение и сдачу лабораторной работы и 1 час на подготовку отчета).

Структура отчета (на отдельном листе(-ах)): титульный лист, формулировка задания, этапы выполнения работы (со скриншотами), результаты выполнения работы (скриншоты), выводы.