Транзакция Биткоина

Над проектом работали:
Кулага Маргарита, Марус Анна, Романовская Анастасия, Турчук Анастасия, Гуд Даниил, Пархимчик Андрей

СОДЕРЖАНИЕ

Bitcoin

Биткоин (англ. Bitcoin) — пиринговая платёжная система, использующая одноимённую единицу для учёта операций. Для обеспечения функционирования и защиты системы используются криптографические методы, но при этом вся информация о транзакциях между адресами системы доступна в открытом виде.

Минимальная передаваемая величина (наименьшая величина дробления) — 10^{-8} биткойна — получила название «сато́ши» — в честь создателя Сатоси Накамото, хотя сам он использовал в таких случаях слово «цент».

Для чего используется биткоин

1

Замена дебетовой карты

В некоторых точках мира уже функционируют биткоин-банкоматы, которые выполняют такие же функции, как традиционные АТМ-устройства.

3

Альтернативное средство оплаты

Биткоин – это точно такие же деньги, как любая другая валюта. Им можно рассчитываться в интернете, обменять на бумажные деньги и наоборот.

2

Замена фиатной валюты

Биткоин уже способен создать здоровую конкуренцию фиатной валюте или быть её полноценной альтернативой.

Для чего используется биткоин

Международные платежи

Биткоин стал международным платежным инструментом, который имеет силу в любой точке планеты.

Постоянный регистр транзакций

Биткоин может использоваться для обмена информацией и ценностями, не имеющими отношения к нему самому. Блокчейн фиксирует все транзакции этой криптовалюты.

Инвестиции

Большинство приобретает цифровые деньги с целью заработка, а не для практического использования.

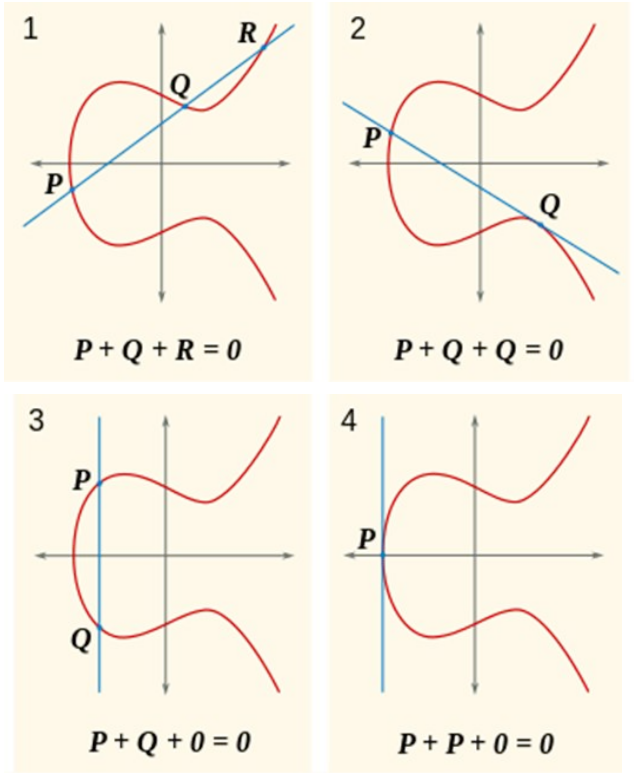
Создание публичного и приватных ключей, сложение на кривой secp256k1

ECDSA является важным алгоритмом, используемым в криптосистеме Bitcoin(хотя кривую можно использовать и в других алгоритмах, таких как Schnorr). Для генерации ключей необходимо знать base point кривой и её порядок n.

Алгоритм:

1. Выбрать случайное число в диапазоне k в диапазоне [1; 2^256]
2. Посчитать K = k*G
3. K представляет собой публичный ключ, а k - приватный

Публичный ключ может хранится в так называемом compressed и uncompressed виде. Compressed занимает 33 байта и содержит в себе префикс, указывающий, какое значение y(x) надо выбрать(если y(x) четное, то 0x02; если



Алгоритмы хэширования и кодирования

1. **sha256** – это один самых известных и часто используемых алгоритмов хэширования. Отличается безопасностью и скоростью.

2. **RIPEMD160** – криптографическая хеш-функция. Для произвольного входного сообщения функция генерирует 160-разрядное хеш-значение, называемое сводкой сообщения.

3. **compressed key** – способ хранения открытого ключа в меньшем количестве байтов (33 вместо 65). Это точно такие же открытые ключи, просто хранящиеся по-другому.

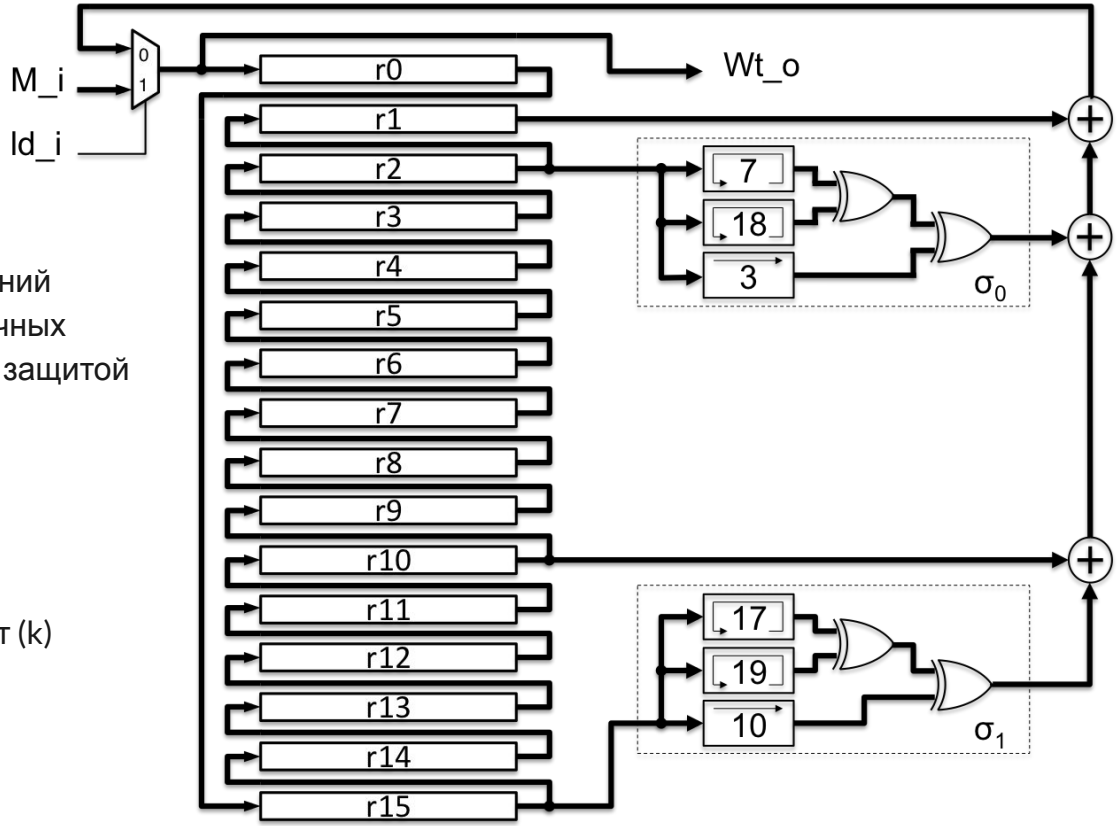
4. **b58encode** – вариант кодирования цифрового кода в виде буквенно-цифрового текста на основе латинского алфавита. Алфавит кодирования содержит 58 символов. Применяется для передачи данных в разнородных сетях

sha256

Хеш-функции предназначены для создания «отпечатков» или «дайджестов» для сообщений произвольной длины. Применяются в различных приложениях или компонентах, связанных с защитой информации.

Шаги хэш-алгоритма:

1. Предварительная работа
2. Инициализация значений хэша (h)
3. Инициализация округленных констант (k)
4. Цикл фрагментов
5. Создание расписания сообщений (w)
6. Сжатие
7. Изменение окончательных значений
8. Финальный хэш

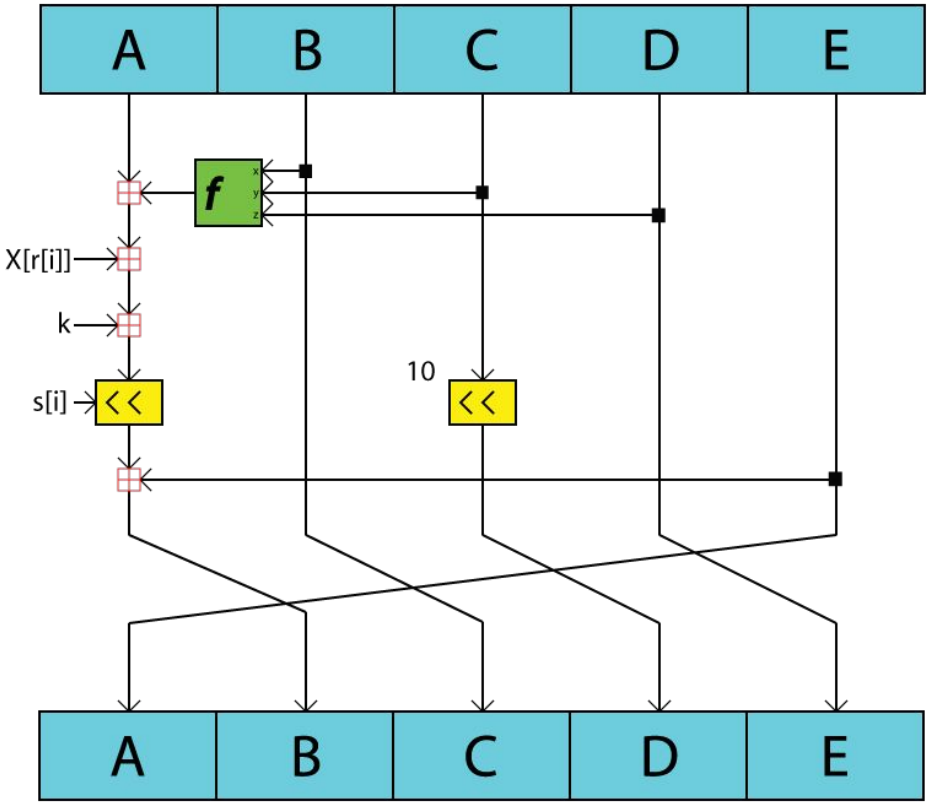


RIPEMD160

RIPEMD-160 была разработана в открытом академическом сообществе, в отличие от SHA-1 и SHA-2, которые были созданы NSA. С другой стороны, RIPEMD-160 на практике применяется несколько реже, чем SHA-1.
Использование RIPEMD-160 не ограничено какими-либо патентами.

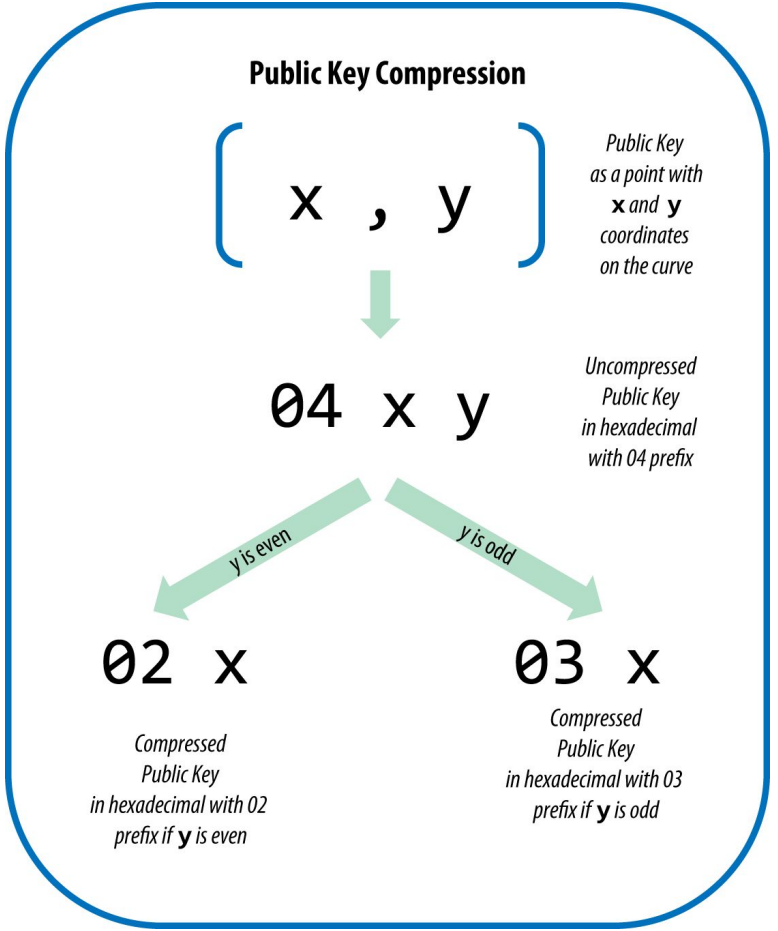
Реализация RIPEMD-160:

1. Добавление недостающих битов
2. Добавление длины сообщения
3. Определение действующих функций и констант
4. Выполнение алгоритма хеширования



compressed key

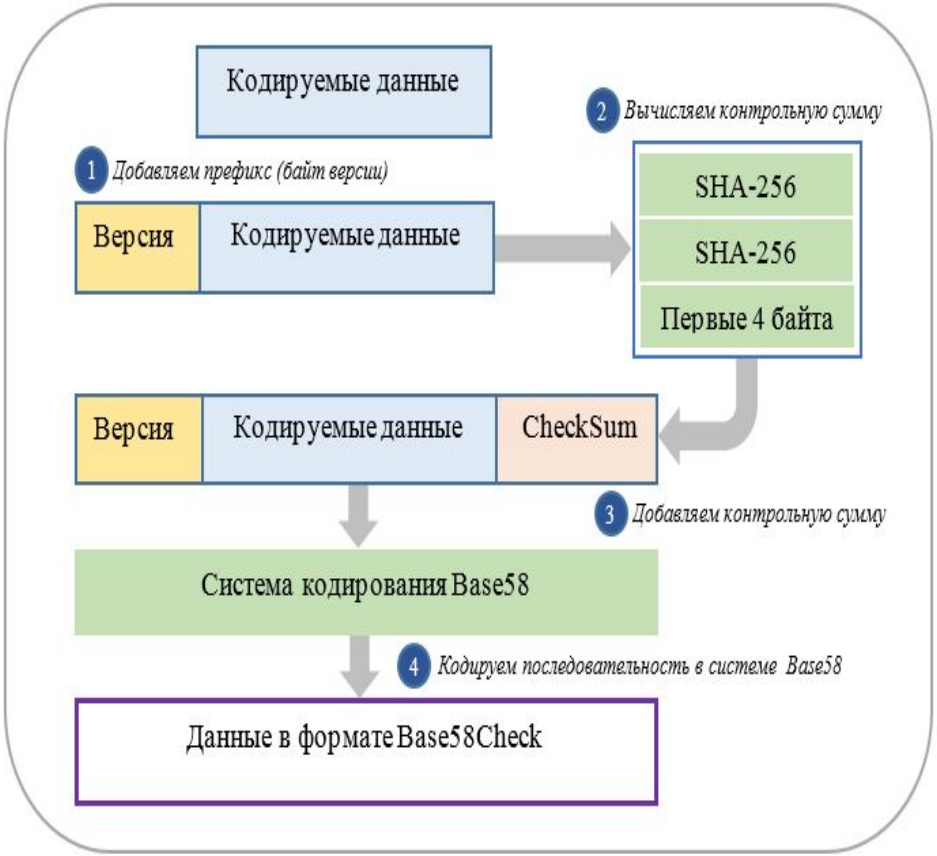
Сжатый ключ - это просто способ хранения открытого ключа в меньшем количестве байтов (33 вместо 65). Нет никаких проблем с совместимостью или безопасностью, потому что это точно такие же ключи, просто хранящиеся по-другому. Оригинальное программное обеспечение Bitcoin не использовало сжатые ключи только потому, что их использование было плохо задокументировано в OpenSSL. У них нет никаких недостатков, кроме того, что требуется немного дополнительных вычислений, прежде чем их можно будет использовать для проверки подписи.

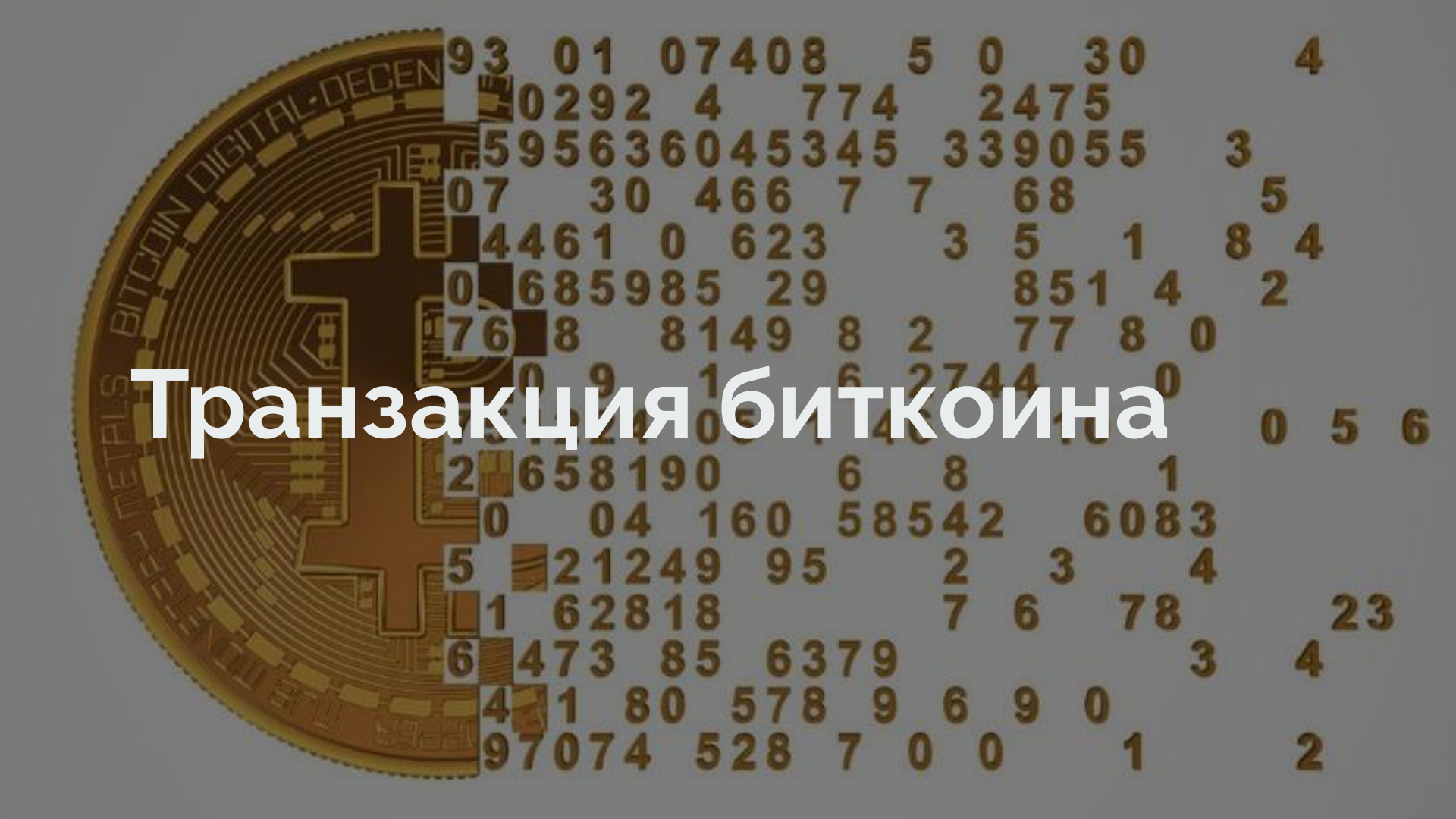


b58encode

Применяется для передачи данных в разнородных сетях (транспортное кодирование). Стандарт похож на Base64, но отличается тем, что в результатах нет не только служебных кодов, но и алфавитно-цифровых символов, которые могут человеком восприниматься неоднозначно.

Стандарт был разработан для уменьшения визуальной путаницы у пользователей, которые вручную вводят данные на основе распечатанного текста или фотографии, то есть без возможности машинного копирования и вставки.




Транзакция биткоина

Транзакция Биткоина — это подписанный раздел данных, который транслируется в сеть и записываются в блоки. Она ссылается на предыдущие транзакции и переводит определённое количество BTC (биткоин-монет) на указанный открытый ключ (Bitcoin-адрес).

Вход — это ссылка на выход другой транзакции. Часто в одной транзакции может быть записано несколько входов, в таком случае значения всех упомянутых выходов предыдущих сделок суммируются и общая сумма записывается на выход текущей транзакции. Скрипт состоит из двух компонентов, подписи и открытого ключа. Открытый ключ принадлежит инициатору транзакции и подтверждает что он обладает суммой необходимой для выполнения транзакции. Второй компонент — это подпись, полученная из хэша транзакции по алгоритму ECDSA . Вместе они подтверждают что транзакция была создана реальным владельцем Bitcoin-адреса. Различные флаги определяют как упростить транзакцию, и могут быть использованы для создания различных типов оплаты.

Выход содержит инструкции на перевод BTC. Транзакция может содержать больше одного выхода, для того чтобы обработать всю сумму BTC указанную на входе, к примеру: если вход ссылается на транзакцию в 50 BTC, а вы хотите отправить получателю только 25 BTC, то будет создано 2 выхода: первый к Bitcoin-адресу получателя, а второй обратно к вашему адресу. В тех случаях когда на выходах транзакции обрабатывается не вся сумма BTC указанная на входе, любой необработанный остаток BTC признаётся комиссией за транзакцию: майнер, сгенерировавший блок в который включена запись о данной транзакции — получит эти BTC.

Расчет вознаграждения за транзакцию

Чтобы получить представление о текущей “рыночной ставке” комиссий за транзакции, доступно несколько веб-сайтов, или мы можем просто прокрутить некоторые транзакции в последнем блоке, чтобы получить представление. Несколько из транзакций были упакованы в блок со скоростью <1sat/B. Попробуем использовать очень щедрую плату, например, в размере 10 sat/B, или общую комиссию за транзакцию в размере 0,0000001. В этом случае мы вводим 0,001 BTC = 100 000 sat, комиссия составит 2500 sat (потому что наша транзакция составит около 250B), мы собираемся отправить 50 000 sat на наш целевой кошелек, а остальные (100,000 - 2,500 - 50,000 = 47 500) обратно к нам.3

Пример транзакции

```
from bit import PrivateKeyTestnet

my_key = PrivateKeyTestnet("cV6iiXiQLW9oqjGt85r9CVj1vgdB5eJ8jye7P7DT7sGyCYcDxxJq")

print(my_key.version)

print(my_key.to_wif())

print(my_key.address)
#cV6iiXiQLW9oqjGt85r9CVj1vgdB5eJ8jye7P7DT7sGyCYcDxxJq
#muGYcQ3ntZqdoDPKxTtsPzfV586sNA1oYM
```

```
test
cV6iiXiQLW9oqjGt85r9CVj1vgdB5eJ8jye7P7DT7sGyCYcDxxJq
muGYcQ3ntZqdoDPKxTtsPzfV586sNA1oYM
```

```
print(my_key.balance_as('usd'))
```

```
0
```

```
tx_hash = my_key.send([('mgh4VjZx5MpkHRis9mDsF2ZcKLdXoP3oQ4', 1, 'usd')])

print(tx_hash)
```

```
599dc4bddecff1d5463f012063df0e1104eaa9350bd872a0bbd4eec283239c8b
```

Транзакции

Комиссия	0.00000226 BTC (1.000 sat/B - 0.250 sat/WU - 226 bytes)			+0.00003406 BTC
Хэш	599dc4bddecff1d5463f012063df0e1104eaa9350bd872a0bbd4eec283239c...			2022-05-23 22:25
	muGYcQ3ntZqdoDPKxTtsPzfV586sNA1oYM	0.00096371 BTC	mgh4VjZx5MpkHRis9mDsF2ZcKLdXoP3oQ4	0.00003406 BTC
			muGYcQ3ntZqdoDPKxTtsPzfV586sNA1oYM	0.00092739 BTC

Команда

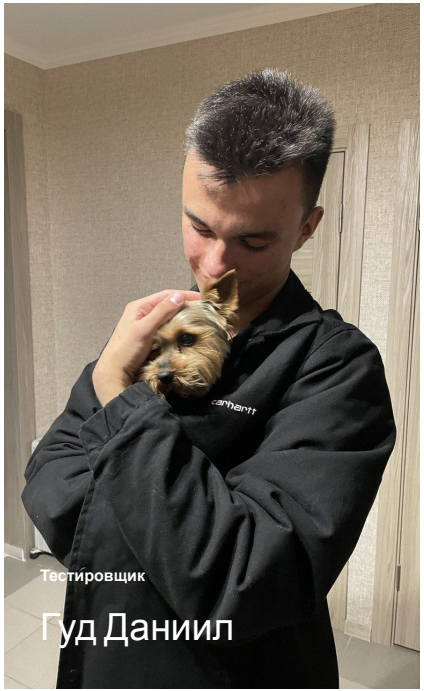
Наша команда – это группа из 6 специалистов разного профиля, которые активно вовлечены в работу над общим проектом.

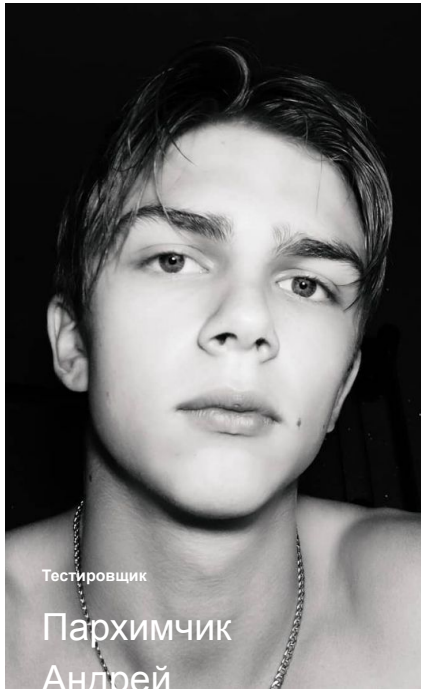
В работе над проектом активно участвовали директор, системный аналитик, математик, программист и два тестировщика.

Команда

Каждый участник нашей команды может выполнить следующие условия:

- Понимать объем и характер работы, которую предстоит проделать.
- Планировать выполнение порученных задач.
- Сотрудничать с другими членами коллектива.





Спасибо за внимание!