

Zero2Hero Bootcamp

Assignment 1

Вы можете работать в команде от 3-5 человек.
Дедлайн: 14 Марта 20:59 (Москва, UTC+3)

Напишите gmail всех участников команды (для оценок):

Ответ: Ksenia Ekshova

Задача 0 - Собрать команду

Заполните данный документ:

https://docs.google.com/spreadsheets/d/li-7WdLb09luguZC9L4_M_VOZVOSTnqtThArhIM5y4Z0/

номер команды и название:

N16 - No name

Задача 1 - Капсула времени

Каждый участник команды должен написать сообщение себе из будущего (сообщение себе после окончания программы).
Зашифруйте данное сообщение используя шифр AES (256 bit).

В качестве ключа используйте один ключ для всей команды.

Ключ: No name

Напишите результаты шифрования в base64:

Sfylo8s78+phoKP4vGxze7xuqgL7czJnUfGv4+N5Ak9IUQRQQ/L9+JOI7+IxLu
MimNQnDi/blPYnX43Ji05kP2t7RSj8jGxaQT2nOkYIBYj9qw17NNX/jHr7LwWl
rOHY2aF02bQGnt+krBje/L9Ng1DE/u+fcOl/j0vr0WPA+S3mIlg2Y/3B2vyK2Rzf
FETs3kSzcFToVlqGBUJ12yC1dyzm0K5TDJdUJKGQ3HX45nmi12LZruliUZEklE
u+wUy4aEi/7h1PuJE8zzi4iQKyihBKUYCzO8xw/8GsbpqkNu5gQsAyTnNCQ
gZ9Kn1hksDx+

Задача 2 - Майнинг

Найдите входное значения для алгоритма хэширования SHA256,
которое бы дало результат с 2 ведущими нулями.

Входное значение должно быть zero2hero+_____

входное значение:

zero2hero+201

полученный хэш:

00a1a07842acda45fdae72a46bb1e4c479e25c019ea2d15476abfedcab3e1201

Напишите чем отличается хеширование от шифрования (40-200 слов):

ответ:

Хеширование и шифрование - это две разные технологии, используемые в криптографии для защиты данных. Хеширование и шифрование выполняют разные функции и используются в разных ситуациях.

Хеширование предполагает использование математической функции для преобразования данных в строку символов фиксированной длины, известную как "хэш".

Хэш служит индикатором неизменности данных, поскольку любое, даже минимальное, изменение данных приведет к созданию абсолютно другого хэша. При повторном хешировании того же входного значения значение хэша остается неизменным. Хэш нельзя преобразовать назад в исходное значение, в отличие от зашифрованного значения.

Шифрование - это процесс преобразования открытого текста в зашифрованный с помощью шифра и секретного ключа. Оно используется для обеспечения конфиденциальности сообщения и защиты его от перехвата и прочтения неавторизованными лицами, чтобы только авторизованный клиент смог расшифровать сообщение.

EXTRA: найти входное значение, которое дает хэш с 5 ведущими нулями

входное значение:

zero2hero+1841486

полученный хэш:

000007f453946a7f1d68f52244d7acbfaf9f7031246508fd8dd6f2b181706b8f

Задача 3 – Работа с блокчейн

1. Создать metamask кошелек. Напишите ваши адреса metamask:
0x55b8A6b4e4f3304d05A3D82af90bac7baf1faC53
0x788c7e5E5e94E38649141A18Ca5EBCCC1DD43957
2. В metamask создать второй аккаунт и отправить туда 0.01 tBNB.
Оставьте ссылку на транзакцию где вы делаете перевод:
<https://testnet.bscscan.com/>
ссылка на транзакцию:
<https://testnet.bscscan.com/tx/0x2274df8d46daff0a95cdf0e3cccf4d74c1576fbcaf16164ef70c8af3f14e56e>
3. Работа с обозревателем блоков. Напишите в какой блок попала ваша транзакция, отправьте ссылку на данный блок в обозревателе блока. пример:
<https://testnet.bscscan.com/block/27801311> опишите данный блок (20-100 слов)
Ссылка на блок: <https://testnet.bscscan.com/block/28040607>
Описание блока:

Блок состоит из трех основных компонентов:

1. Заголовок блока: содержит метаданные о блоке, такие как номер версии, временная метка и ссылка на предыдущий блок в цепочке.
2. Транзакции: содержит список транзакций, которые были проверены и добавлены в блок. Каждая транзакция обычно содержит такую информацию, как адрес отправителя, адрес получателя, количество переводимой криптовалюты и цифровую подпись для подтверждения подлинности транзакции.
3. Хеш блока: уникальный идентификатор блока, который создается с помощью криптографической хэш-функции.

Block Height:

28040607

<>

Timestamp:

⌚ 25 mins ago (Mar-14-2023 04:00:20 PM +UTC)

Transactions:

21 transactions and 33 contract internal transactions in this block

Validated by:

0x1284214b9b9c85549ab3d2b972df0deef66ac2c9 in 3 secs

Block Reward:

0.010373043 BNB

Difficulty:

2

Total Difficulty:

55,908,898

Size:

5,456 bytes

Gas Used:

945,922 (1.90%)

Gas Limit:

49,803,929

Fee Burnt:

🔥 0.0010373043 BNB 🔗

Extra Data:

Hex:
0xd98301011384676574688967f312e31372e3133856c696e7578000059afa6a3dd1dd1bccbe0f2ab91137af7252d46bf33338dec6114f3c840319e4259e25
0184c411a48fcf32fb8ea9101cce7b312c8750bc13a14738690ebfcfec99c4870ee00

ExtraVanity : .0000gethgo1.17.13linuxY♦♦♦
SignedData :
0xdd1dd1bccbe0f2ab91137af7252d46bf33338dec6114f3c840319e4259e250184c411a48fcf32fb8ea9101cce7b312c8750bc13a14738690ebfcfec99c487
0ee00

Hash:

0x4ea19feaa88a52cb785988634ae4625e431251ce105007168bb08f600b26a

Parent Hash:

0x9df5dceb44a59a83cc289ecf28a24057a736f591ef7ff6d5a852c962c8eb4d0c

Sha3Uncles:

0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347

Nonce:

0x0000000000000000

4. Совершите обмен tBNB на BUSD в <https://pancakeswap.finance/?chain=bscTestnet> (оставьте ссылку на транзакцию)
ссылка на транзакцию:
<https://testnet.bscscan.com/tx/0xf80711be615e68ec7ddf4eeb9dfe9984>
5. Добавьте ликвидность tBNB и BUSD через:
<https://pancakeswap.finance/liquidity?chain=bscTestnet> (оставьте ссылку на транзакцию)

ссылка на транзакцию:

<https://testnet.bscscan.com/tx/0xffffcd218ed21bb8d8c7ae87d98e682535a84e670716db1912a30207c5a59788c>

6. Опишите для чего нужна ликвидность (20-100 слов)

Ответ:

Ликвидность в контексте блокчейна обычно означает способность криптовалюты или токена легко покупаться или продаваться на бирже или другой платформе без существенного влияния на ее цену. Криптовалюта с высокой ликвидностью - это криптовалюта, которую можно легко конвертировать в наличные или другие активы, не испытывая при этом сильных колебаний цены.

Добавляя ликвидность (к паре токенов), можно зарабатывать 0,17% от всего объема сделок по этой паре пропорционально доле в торговой паре. Комиссионные добавляются к паре, начисляются в режиме реального времени и могут быть востребованы при снятии ликвидности.

Ликвидность важна для активов на основе блокчейна, поскольку она помогает обеспечить их легкую торговлю и использование в качестве средства обмена.

Если ликвидности нет – никто не может обменивать валюту.

EXTRA: Напишите эссе до 500 слов по yellow paper ethereum

"Yellow Paper Ethereum" это важнейший технический документ, описывающий технические характеристики и фундаментальные принципы блокчейна Ethereum. В "Yellow Paper Ethereum", автором которого является доктор Гэвин Вуд, соучредитель Ethereum, дается всестороннее и подробное объяснение виртуальной машины Ethereum (EVM), механизма консенсуса и структуры блокчейна.

EVM- это двигатель, на котором работает блокчейн Ethereum и исполняются смарт-контракты. Понимание того, как работает EVM, крайне важно для создания децентрализованных приложений (Dapps)

и взаимодействия блокчейном Ethereum. В "Yellow Paper Ethereum" содержится подробная спецификация EVM, включая его инструкции, расположение памяти, архитектуру стека и газовую модель.

В "Yellow Paper Ethereum" также объясняется механизм консенсуса, используемый в Ethereum, который называется "Proof-of-Work (PoW)". Механизм POW используется для подтверждения транзакций и блоков в блокчейне Ethereum, гарантируя, что блокчейн остается безопасным и защищенным от взлома. В документе содержится подробное описание работы механизма консенсуса POW, включая то, как майнеры подтверждают транзакции, как они соревнуются в решении криптографических задач и как они получают вознаграждение за свою работу.

В "Yellow Paper Ethereum" также подробно описана структура блокчейна Ethereum. В нем содержится полное описание различных компонентов блокчейна, включая блоки, транзакции и состояние, а также объясняется, как состояние блокчейна Ethereum обновляется по мере обработки транзакций и как можно урезать блокчейн для повышения эффективности.

В целом, "Yellow Paper Ethereum" является важнейшим техническим справочником для разработчиков, создающих децентрализованные приложения на блокчейне Ethereum, и для всех, кто хочет понять, как работает эта технология. Всестороннее и подробное объяснение различных компонентов блокчейна Ethereum делает его бесценным ресурсом для всех, кто интересуется технологией блокчейн.

Задача (EXTRA) – Провести менторство для новичков, расписать результат менторства. Кто были ваши mentee, что они узнали от вас

Ответ: