Колледж Автономной некоммерческой образовательной организации высшего образования «Научно-технологический университет «Сириус»

25

**Реферат на тему Блокчейн-технологии**

**в разработке: создание простого криптокошелька.**

Работу подготовил:

Студент группы К0709-24/2

Иванченко Н.А.

Преподаватель:

Яковлева С. В.

Оглавление

[**Введение** 2](#_Toc192705939)

[**Что такое блокчейн?** 3](#_Toc192705940)

[История и эволюция 3](#_Toc192705941)

[**Криптография в блокчейне** 4](#_Toc192705942)

[**Создание криптокошелька. Архитектура кошелька.** 5](#_Toc192705943)

[**Безопасность криптокошельков. Основные угрозы** 6](#_Toc192705944)

[**Текущие тренды. DeFi и NFT** 7](#_Toc192705945)

[**Реализация простого кошелька на Python** 8](#_Toc192705946)

[**Итоги-блокчейн-технологий и создания криптокошелька** 9](#_Toc192705947)

[**Литература** 10](#_Toc192705948)

# **Введение**

За последние десять лет блокчейн-технологии и криптовалюты переросли статус нишевых инноваций, превратившись в ключевые драйверы трансформации глобальной экономики. Их влияние уже вышло за рамки финансового сектора, охватывая сферы, где требуется повышенная безопасность, прозрачность и децентрализация. Например, в здравоохранении блокчейн используется для безопасного хранения и обмена медицинскими данными, в логистике — для отслеживания цепочек поставок в реальном времени, а в юриспруденции — для автоматизации смарт-контрактов.

Актуальность блокчейна подтверждается его экспоненциальным ростом. Согласно отчёту MarketsandMarkets, объём рынка блокчейн-решений может превысить $39 млрд к 2025 году, что связано с внедрением технологии в государственное управление, ритейл и даже энергетику. Криптовалюты, такие как Bitcoin, Ethereum и их аналоги, стали не только инструментом для спекуляций или платежей, но и способом сохранения сбережений в условиях экономической нестабильности, например, в странах с высокой инфляцией.

Для разработчиков знание блокчейна становится критически важным. Это связано не только с созданием децентрализованных приложений (dApps) или смарт-контрактов, но и с адаптацией традиционных систем к новым стандартам безопасности и прозрачности. Понимание принципов работы распределённых реестров, консенсус-алгоритмов и криптографии помогает участвовать в проектах будущего — от Web3 до метавселенных. Таким образом, блокчейн перестаёт быть «трендом» и становится основой для цифровой экономики, где разработчики играют ключевую роль.

## **Что такое блокчейн?**

Блокчейн — это децентрализованная база данных, состоящая из связанных криптографическими методами блоков, которые хранят информацию о транзакциях или других операциях.

# История и эволюция

Технология была предложена в 2008 году анонимным автором (или группой) под псевдонимом Сатоши Накамото как основа для Bitcoin — первой децентрализованной криптовалюты. Сегодня блокчейн вышел за рамки финансов: его используют в логистике, здравоохранении, энергетике, авторском праве и даже в голосовании.

Первоначально созданная для криптовалюты Bitcoin, технология сейчас применяется в различных сферах благодаря своим ключевым особенностям:

Децентрализация : управление сетью распределено между участниками, без единого центра.

Консенсус : новые данные добавляются только после согласия участников (например, через PoW или PoS).

Прозрачность : все записи публичны и доступны для проверки.

Неизменяемость : данные нельзя изменить после записи — любое вмешательство требует пересчёта всей цепочки.

Репликация : копии блокчейна хранятся на всех узлах сети, обеспечивая надёжность.

Эти свойства делают блокчейн инструментом для безопасного и прозрачного взаимодействия без посредников.

# **Криптография в блокчейне**

Криптография в блокчейне — это основа безопасности системы, обеспечивающая защиту данных и подтверждение подлинности транзакций без доверия к третьим лицам. Её ключевые элементы:

Асимметричная криптография

Каждый участник имеет публичный ключ (адрес для получения транзакций) и приватный ключ (секретный ключ для подписи).

Приватный ключ шифрует данные, публичный — проверяет их подлинность.

Хеш-функции преобразуют данные в уникальный фиксированный код (хеш).

Гарантируют неизменяемость : изменение данных в блоке меняет его хеш, нарушая цепочку.

Используются в механизмах консенсуса (например, Proof of Work в Bitcoin).

Цифровые подписи

Подтверждают авторство транзакции: отправитель подписывает её приватным ключом, сеть проверяет подпись через публичный ключ.

Пример работы :

Пользователь А отправляет Bitcoin пользователю Б:

Создаёт транзакцию с адресом Б (публичный ключ).

Подписывает её своим приватным ключом.

Сеть проверяет подпись и, если она верна, добавляет транзакцию в блок.

Криптография делает блокчейн безопасным, прозрачным и устойчивым к взломам, обеспечивая децентрализованное взаимодействие.

# **Создание криптокошелька. Архитектура кошелька.**

1. Структура криптокошелька

Криптокошелёк — это инструмент, позволяющий пользователям безопасно хранить, отправлять и получать криптовалюту. Его работа основана на следующих ключевых элементах:

- Приватный ключ:

Секретная информация, необходимая для подтверждения владения средствами и подписания транзакций.

- Публичный ключ:

Вычисляется на основе приватного ключа и служит для получения платежей. Он является аналогом банковского счёта в блокчейне.

- Адрес кошелька:

Уникальный идентификатор, созданный путём хеширования публичного ключа. Используется для приёма средств.

- История транзакций:

Хранит все операции пользователя, связанные с отправкой и получением криптовалюты. Может быть локальной или синхронизированной с глобальным блокчейном.

- Интерфейс взаимодействия:

Предоставляет пользователю простой способ управления кошельком через графический интерфейс или командную строку.

Основные функции

- Генерация пары ключей: Создание приватного и публичного ключей для обеспечения безопасности.

- Отслеживание баланса: Постоянное обновление информации о количестве доступных средств.

- Подписание транзакций: Подтверждение операций с использованием приватного ключа.

- Синхронизация с сетью: Обмен данными с блокчейном для проверки состояния счета и подтверждения транзакций.

# **Безопасность криптокошельков. Основные угрозы**

Основные угрозы безопасности криптокошельков

Угрозы для криптокошельков:

Несмотря на высокую безопасность блокчейна, сами кошельки могут быть уязвимы. Вот основные риски:

Утрата приватного ключа:

Если пользователь теряет доступ к приватному ключу, он больше не сможет получить доступ к своим средствам.

Фишинг:

Махинации, направленные на обман пользователя для получения его приватного ключа или пароля.

Малварь (вредоносное ПО):

Вирусы или трояны могут украсть приватные ключи с устройства пользователя.

Хакерские атаки:

Атаки на горячие кошельки, подключённые к интернету, особенно опасны для крупных сумм.

Человеческий фактор:

Ошибки при управлении кошельком (например, использование слабых паролей) также могут привести к потерям.

Лучшие практики безопасности:

Использование hardware-кошельков для долгосрочного хранения.

Регулярное резервное копирование приватных ключей.

Хранение средств на разных кошельках для минимизации рисков.

Включение двухфакторной аутентификации (2FA).

Безопасность криптокошельков зависит от правильного выбора инструментов и соблюдения рекомендаций. Защита приватных ключей — это ключевой аспект успешного использования криптовалют.

# **Текущие тренды. DeFi и NFT**

DeFi (Decentralized Finance): DeFi представляет собой экосистему децентрализованных финансовых приложений, работающих на блокчейне без участия традиционных финансовых учреждений. Основные особенности:

Кредиты без залога: Пользователи могут брать займы, используя свои цифровые активы в качестве залога.

Стейкинг (Staking): Возможность зарабатывать, предоставляя свои криптоактивы в пулыliquidity.

Обмен активами: Децентрализованные биржи (DEX), такие как Uniswap или SushiSwap, позволяют обменивать криптовалюты напрямую между пользователями.

Пример использования:

Пользователь может предоставить свои токены в пул ликвидности и получать проценты за их использование другими участниками сети.

NFT (Non-Fungible Tokens):

NFT — это уникальные цифровые активы, представляющие произведения искусства, музыку, видео, игры и другие объекты. Каждый NFT имеет собственную ценность и не может быть заменён другим токеном.

Искусство: Художники продают свои работы в виде NFT через платформы, такие как OpenSea или Rarible.

Гейминг: Игры используют NFT для представления уникальных предметов или персонажей.

Домены: Проекты, такие как ENS (Ethereum Name Service), позволяют регистрировать уникальные доменные имена в блокчейне.

Пример использования:

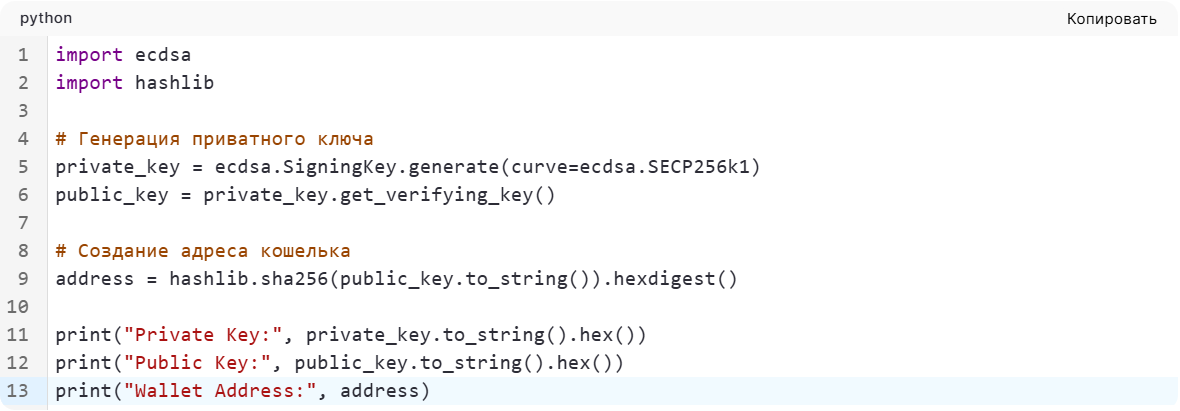
Художник создаёт цифровое произведение и выпускает его в виде NFT. Покупатель приобретает этот токен, получая право владения оригиналом.

Почему эти тренды важны?

---DeFi меняет правила игры в финансовом секторе, предоставляя доступ к услугам без необходимости доверять банкам или брокерам.

---NFT расширяют понятие владения цифровыми активами, создавая новые рынки для творческих работ, коллекционирования и гейминга.

# **Реализация простого кошелька на Python**

****

Шаг 1: Импорт необходимых библиотек

ecdsa : Эта библиотека позволяет генерировать приватные и публичные ключи.

hashlib : Библиотека Python для создания адреса кошелька через хеширование публичного ключа.

Шаг 2: Генерация приватного ключа

ecdsa.SigningKey.generate() : Этот метод генерирует случайный приватный ключ.

curve=ecdsa.SECP256k1 : Указывает, что я использую кривую SECP256k1, которая является стандартом для многих блокчейнов, таких как Bitcoin. Эта кривая обеспечивает высокий уровень безопасности.

Шаг 3: Получение публичного ключа

get\_verifying\_key() : вычисляет публичный ключ на основе приватного ключа.

\*Публичный ключ используется для получения платежей. Он не является секретным и может быть открыт для всех участников сети.\*

Шаг 4: Создание адреса кошелька

public\_key.to\_string() : Преобразует публичный ключ в строку байтов для дальнейшей обработки.

hashlib.sha256() : Хеширует публичный ключ с использованием алгоритма SHA-256—гарант на уникальность адреса кошелька.

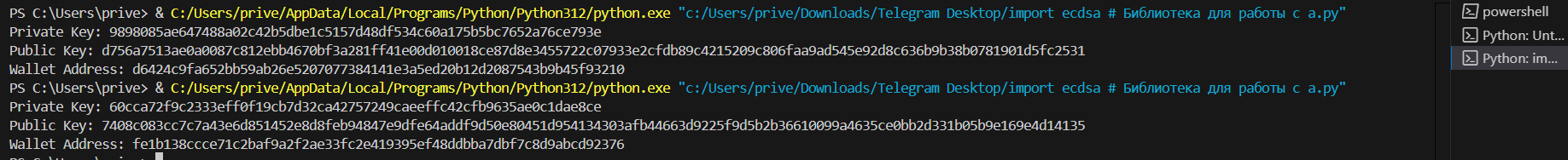
.hexdigest() : Преобразует полученный хеш в строку шестнадцатеричного формата для удобства чтения.

Шаг 5: Вывод результатов

private\_key.to\_string().hex() : Преобразует приватный ключ в шестнадцатеричный формат для вывода.

public\_key.to\_string().hex() : Преобразует публичный ключ в шестнадцатеричный формат для вывода.

address : Выводит сгенерированный адрес кошелька.

****

# **Итоги-блокчейн-технологий и создания криптокошелька**

Блокчейн-технологии становятся неотъемлемой частью современного мира. Изучение их основ и практических применений, таких как создание криптокошелька, открывает новые возможности для разработчиков и предпринимателей.

Новые возможности для карьерного роста : Рынок труда активно формирует спрос на специалистов, владеющих блокчейн-технологиями. Компании во всём мире ищут разработчиков, способных создавать decentralised applications (dApps), смарт-контракты и другие решения на основе блокчейна.

# **Литература**

Книга

Андерсон, Р. "Безопасность в компьютерных сетях".

Официальная документация:

Документация библиотеки ecdsa: https://ecdsa.readthedocs.io

Python Standard Library: https://docs.python.org/3/library/hashlib.html

Статьи и исследования:

"Introduction to Blockchain Technology" — CoinDesk: [https://www.coindesk.com/learn/what-is-blockchain-technology](https://www.coindesk.com/learn/what-is-blockchain-technology?spm=a2ty_o01.29997173.0.0.7b987db6FTEqUS)

"Decentralized Finance (DeFi): An Overview" — Investopedia: <https://www.investopedia.com/terms/d/decentralized-finance-defi.asp>

"Non-Fungible Tokens (NFTs): A Guide for Developers" — Medium: [https://medium.com/@david\_kim/nfts-a-guide-for-developers-9c8f5e7b4a3b](https://medium.com/@david_kim/nfts-a-guide-for-developers-9c8f5e7b4a3b?spm=a2ty_o01.29997173.0.0.7b987db6FTEqUS)

Ресурсы о блокчейне и криптовалютах:

Bitcoin.org — Официальный сайт Bitcoin- [https://bitcoin.org](https://bitcoin.org/?spm=a2ty_o01.29997173.0.0.7b987db6FTEqUS)

Ethereum.org — Официальный сайт Ethereum- [https://ethereum.org](https://ethereum.org/?spm=a2ty_o01.29997173.0.0.7b987db6FTEqUS)

BlockGeeks — материалы о блокчейне- [https://blockgeeks.com](https://blockgeeks.com/)