DOI 10.36622/VSTU.2022.25.3.009
УДК 004.056.55/003.26

БЛОКЧЕЙН, КРИПТОВАЛЮТЫ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.Ю. Филяк, С.С. Ярков

Рассматривается подход к обеспечению информационной безопасности на базе применения современного инструментария такого, как технология BlockChain. Важным фактором обеспечения безопасности является устройство как самого Blockchain, так и различных сетей криптовалют. В тексте описываются различные виды блокчейнов, а также принципы их работы. В работе упоминаются такие принципы как PoW, RPoW, DPoS, PoH. Принципы на которых базируется блокчейн показывают степень защищенности самой сети. Немаловажным фактором являются и вспомогательные программы категории смарт-контрактов, которые включаются в блокчейны и обеспечивают надежность и безопасность транзакций. В статье представлены варианты реализации технологии блокчейн с помощью скриптов, разработанных авторами самостоятельно, которые применяются в непосредственной связке с платформами для блокчейн, на которых они базируются, без чего технология блокчейн не может быть реализована.

Ключевые слова: BlockChain, PoW, RPoW, DPoS, PoH, криптовалюта, смарт-контракт, токен, NFT, транзакция, сеть, хеш, Solana, Bitcoin, Ethereum.

Блокчейн

Изучение темы криптовалют необходимо начинать с понятия блокчейн. Есть много различных вариантов его описания, строения и определения. Будем считать, что блокчейн – это некий реестр децентрализованных данных, в котором обмен безопасен [1].

Технология блокчейн позволяет группе пользователей обмениваться данными независимо от обьема. Также с помощью блокчейна можно собирать и передавать данные разных транзакций сразу из нескольких источников (рис. 1). Данные в свою очередь разбиваются на определенные блоки, которые связаны друг с другом с помощью специальных, неповторимых идентификаторов, а именно криптографических хэшей. Блокчейн способен обеспечить целостность данных при помощи единого источника достоверной информации, устраняя дублирование данных и повышая безопасность.

Взлом и последующая подмена данных предотвращаются за счет того, что данные в случае подмены считаются недействительными, а все субъекты, участвовавшие в создании блокчейна, будут уведомлены о изменении даже одной ячейки блокчейна. Реестр данных блокчейна всегда используется совместно, но изменять или вносить различные поправки не предоставляется возможным.

История

Идея, на которой основана технология блокчейн была опубликована в 1991 году учеными Стюарт Хабер и Скотт Штоннетт. Изначально имея лишь онлайн документы со штампом времени, они внедрили в них вычислительно-практическое решение, благодаря чему не возможно было подделать документы или оформить их более ранним числом.

Система выглядела достаточно не замысловато. Она представляла из себя цепочку блоков длиной n, в которой документы хранились с отметкой времени. В 1992 году в систему были добавлены полные двоичные деревья – деревья Меркла (которые используются и по сей день в Bitcoin и Ethereum). Благодаря этому нововведению появилась возможность собирать несколько документов в один блок (рис. 2).

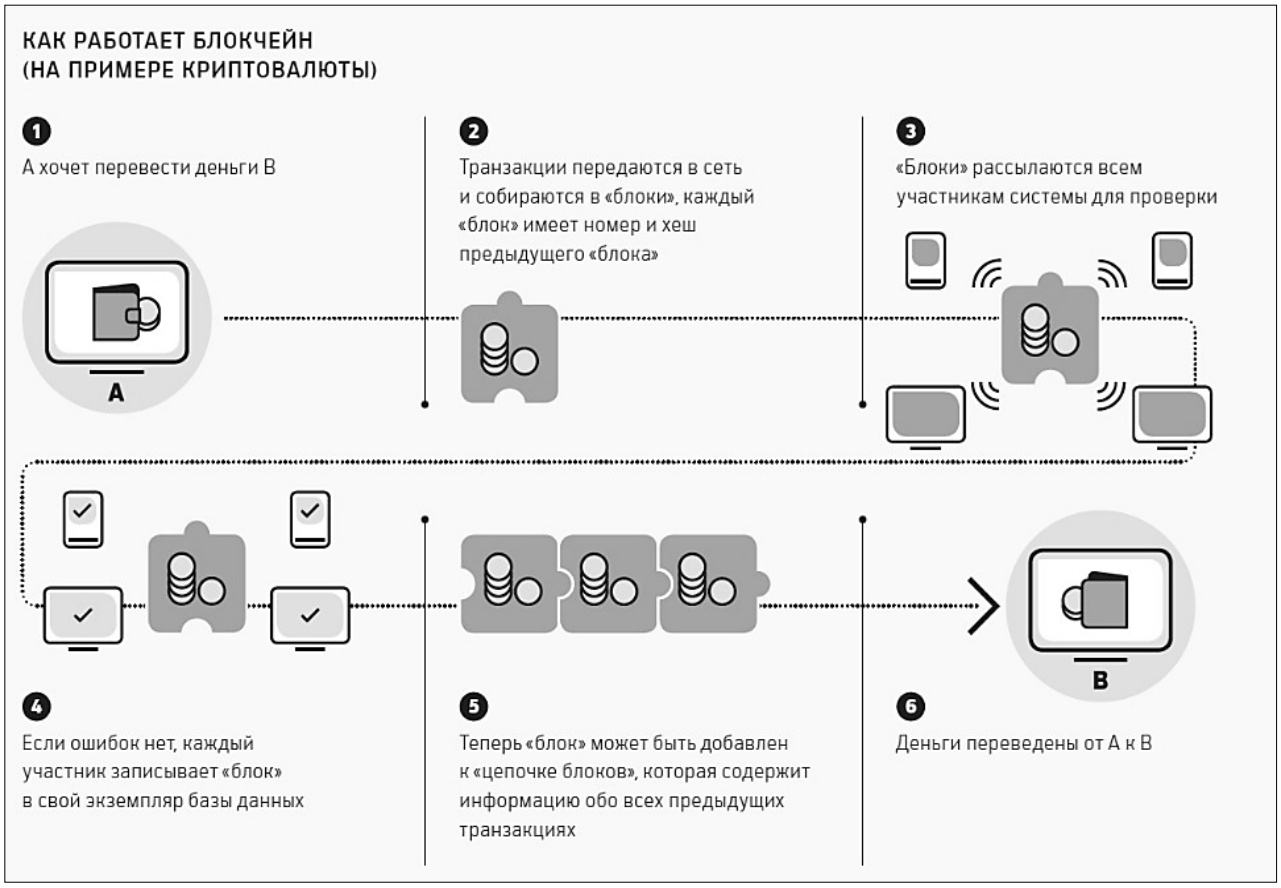

Рис. 1. Принцип работы Blockchain

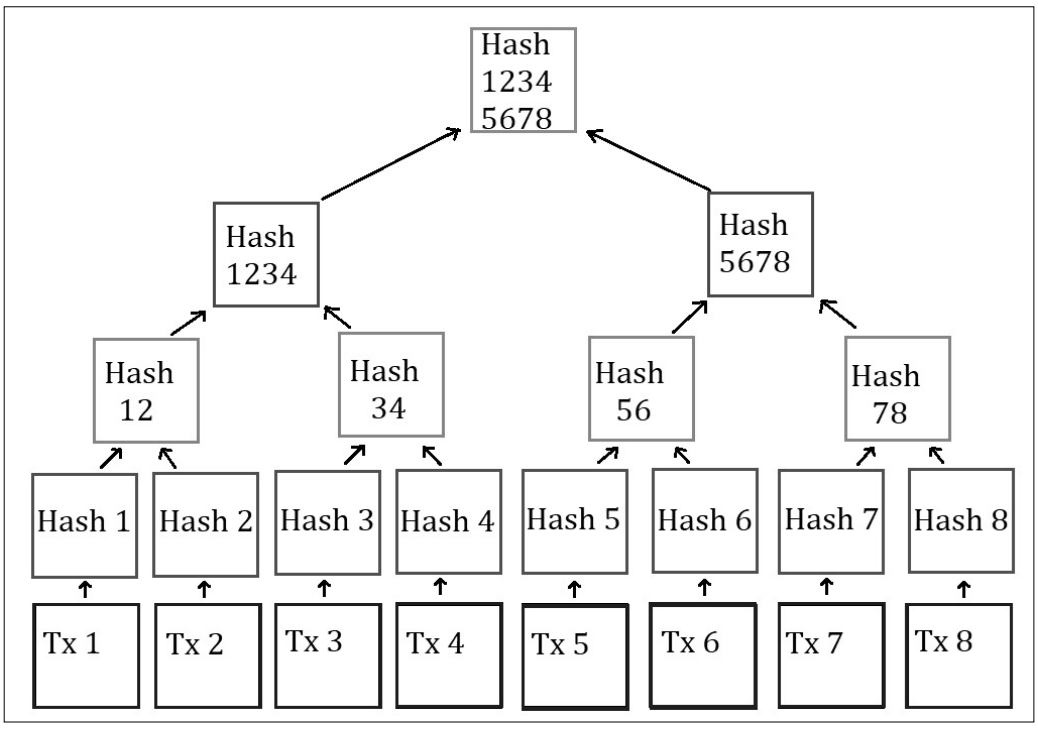

Рис. 2. Хеш Дерево

Reusable Proof of Work

В 2004 году случился прорыв в развитии технологии блокчейн. Программист Хэл Финни создал систему «Доказательство выполнения работы» или RPoW (рис. 3).

Система работала на принципе защиты сетевых систем от внешних воздействий. К таким угрозам можно отнести Dos-attacks или спам. Принцип работы был довольно прост, клиент совершал некую достаточно простую, но длительную задачу, а результат проверялся сервером.

Особенностью является – «асимметрии затрат времени» – время для нахождения решения во много раз больше, чем для проверки.

Эта система решила проблему повторной покупки ценных бумаг и смогла уберечь миллиарды долларов инвесторов. Таким образом, каждый владелец мог проверить целостность своих активов.

Поэтому RPoW — это первый этап развития криптовалют.

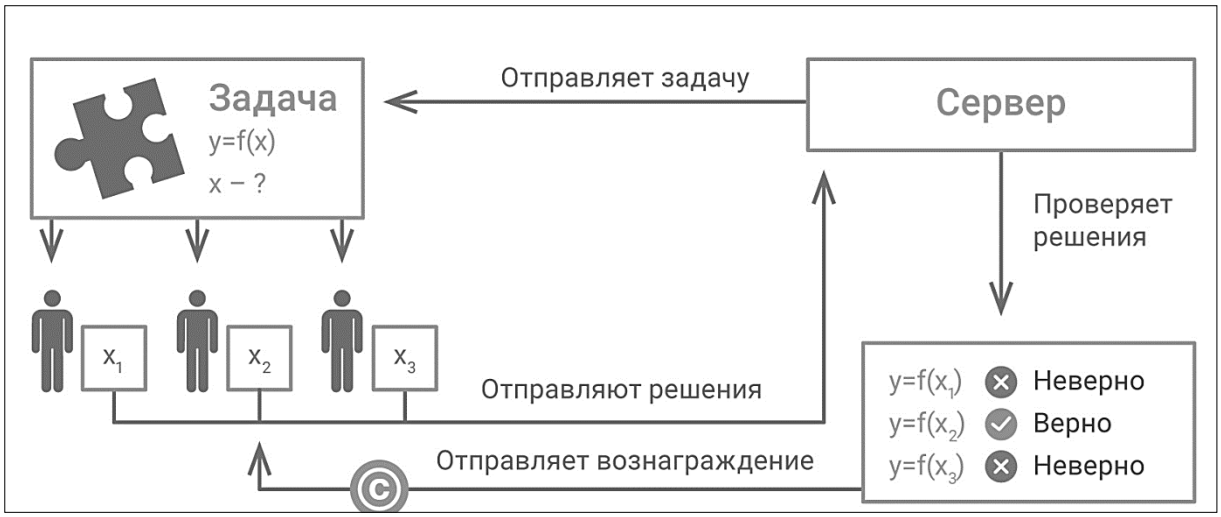

Рис. 3. Принцип работы RPoW

Криптовалюта

Время шло, и люди начали задумываться, а как можно правильно использовать данные системы. Конечно, для ценных бумаг данная система подходила как нельзя хорошо, но почему нельзя сделать точно также, но уже использовать онлайн аналог денег. Тогда и была придумана криптовалюта. По факту она является некой разновидностью цифровой валюты, но не имеющей особой материальной или даже электронной форм. Грубо говоря, это некое число, которое обозначает количество данных расчетных единиц.

«Криптовалютный» рынок децентрализован, то есть нет единого центра регулировки обращения валюты. Хотя плюсом является то, что в нем скорость платежей намного выше, чем в реальном мире. Более того анонимность стоит на первом месте, из-за чего нельзя узнать участников рыночных отношений.

Время прошло, и появились токены. Это единицы учета не являющиеся криптовалютой. Можно сказать, что это некий аналог ценных бумаг. Также стоит не забывать, что доступ к токенам можно получить только через специальные приложения, доступ к которым открывается только после введения электронной подписи. Поэтому токены считаются безопасными инвестициями.

Разбирая тему токенов, нельзя обойти стороной NFT. Это тоже токен, но выпущенный в едином экземпляре. Грубо говоря, уникальная в своем роде ценная бумага. Поэтому стоимость NFT на рынке очень высока.

Смарт-контракты

В переводе с английского — это умный контракт, компьютерная программа, или строчки кода, благодаря которым удается отслеживать исполнения обязательств сторон

и обеспечивать безопасность транзакции. Принцип работы довольно прост. Участники согласуют условия договора, прописывают его в смарт-контракте, и ставят цифровые подписи. Смарт-контракт в свою очередь определяет процент выполнения контракта и при достижении установленного порога закрывает сделку. В ином случае на участника, не выполнившего обязательства накладываются санкции (рис. 4).

Рис. 4. Смарт-контракт

Solana

Самым известным блокчейном несомненно является Bitcoin. Уже несколько лет его рыночная цена торгуется больше 20тыс$. Но, к сожалению, Bitcoin ограничен. Всего насчитывается около 21 миллионов Bitcoin-ов. Поэтому в необозримом будущем Bitcoin закончится.

Сейчас целесообразно рассказать о новом блокчейн-проекте Solana. Его еще называют блокчейном нового поколения. Сразу отмечу, что в отличие от Bitcoin, Solana работает на основе DPoS технологии (Delegated Proof of Stake). Сеть была запущена в 2014 году. Блокчейн на основе DPoS имеет ряд нововведений, в отличие от старого поколения. В Solana присутствует место голосованию стейкхолдеров, держателей криптовалюты. Они передают права управления сетью другим людям, которые впоследствии будут поддерживать сеть от имени участников рыночных отношений.

Большим плюсом является масштабируемость проекта. DPoS способен обрабатывать намного больше транзакций в секунду чем PoS/PoW. Также Solana обеспечивает глобальный источник в блокчейне при помощи второго протокола PoH или Proof-of-history. Можно сказать, что эта функция записывает и сохраняет хронику транзакций в блокчейне, а также собирает все в единый центр. Таким образом можно отследить любые транзакции, которые были совершены участниками сети [2].

Создание кошелька и токена

Технологиям BlockChain и их возможностям посвящено большое количество публикаций, поэтому нет особой необходимости рассматривать абсолютно все виды блокчейнов, тем более принципы их работы.

Давайте приступим к практической реализации полученных сведений. Создадим кошелек в недавно упомянутой выше сети Solana. Блокчейн, работающий на принципах DPoS, поддерживает кошельки Sollet и Ghost, в частности, Sollet, который можно использовать как расширение для браузера.

К сожалению, все в мире платно, как и простое создание токена в сети Solana. В ней на себя роль комиссии берет SOL, который торгуется на отметке 300$. Но разработчики

имеют бесплатный доступ к ним. Перейдем в сеть для разработчиков.

Вторым пунктом станет создание токена.

Подготовительные действия

Все нижеописанные действия выполняем в командной строке Windows.

Шаг первый: установим набор инструментов сети Solana, при помощи команды *curl https://release.solana.com/v1.8.4/solana-install-init-x86_64-pc-windows-msvc.exe --output C:\solana-install-tmp\solana-install-init.exe --create- dirs.*

А дальше запускаем процесс и нажимаем Enter *C:\solana-install-tmp\solana-install-init.exe v1.8.4*

После небольшого ожидания мы получаем уведомление об успешном завершении процесса. Готово. Теперь мы имеем на руках все инструменты для дальнейшей работы (рис. 5).

```
Microsoft Windows [Version 10.0.22000.318]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Stepa>cd Desktop

C:\Users\Stepa\Desktop>mkdir solana_crypton2

C:\Users\Stepa\Desktop>cd solana_crypton2

C:\Users\Stepa\Desktop\solana_crypton2>solana-keygen new --outfile solana-keypair.json
Generating a new keypair

For added security, enter a BIP39 passphrase

NOTE! This passphrase improves security of the recovery seed phrase NOT the
keypair file itself, which is stored as insecure plain text

BIP39 Passphrase (empty for none):

Wrote new keypair to solana-keypair.json
========================================================================
pubkey: CV8YhhtHAvGi1JhvEoWXPD56EaMo3f5ZzS7ZF2ckHiDg
========================================================================
Save this seed phrase and your BIP39 passphrase to recover your new keypair:
upgrade verb music cross require poet robot advice glance tourist average ethics
```

Рис. 5. Процесс создания ключей

Первым шагом к созданию токенов будет создание папки. Назовем ее Solana_crypton2. Вторым шагом будет генерация ключей с помощью инструмента *solana-keygen new --outfile solana-keypair.json*

Сохраняем информацию и переходим в сеть для разработчиков с помощью команды *solana config set --url https://api.devnet.solana.com*, а ключи сохраняем при помощи команды *solana config set --keypair solana- keypair.json*

Создание токена

Шаг третий: создаем токен при помощи команды *spl-token create-token.* И сохраняем информацию о токене.

Создание аккаунта для работы с токеном

Четвертым шагом станет создание аккаунта для изменения и управления нашими токенами. Все выполняется с помощью команды *spl-token create- account адрес токена.* Снова сохраняем все данные (рис. 6).

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token create-token
Creating token 6gSf4aLj7A85qqDYaC5DsAad2hiamjt3xdECg7NKcFkx

Signature: 2xFRcvRyFJEEBZW5mmo2o6kFZSVSrLuQPpsfAwHR94RuPC64w456HPVsCxZRhSymCe6Lw7TqRKNLcuEGhQdqhaXP


C:\Users\Stepa\Desktop\solana_crypton2>spl-token create-account 2xFRcvRyFJEEBZW5mmo2o6kFZSVSrLuQPpsfAwHR94RuPC64w456HPVs
CxZRhSymCe6Lw7TqRKNLcuEGhQdqhaXP
error: Invalid value for '<TOKEN_ADDRESS>': Не удается найти указанный файл. (os error 2)

C:\Users\Stepa\Desktop\solana_crypton2>spl-token create-account 6gSf4aLj7A85qqDYaC5DsAad2hiamjt3xdECg7NKcFkx
Creating account J51S4AVucXEaUHKeWCPWzbyH1FKFtXmbw6fp2hiJMUi

Signature: 43P77ybZMEgM92rek33Kf8b5mVu4BMTsEbU5xZw93WZ7o248XhgruvkGrhYYRKX6F5n9w84FRyeB8C5KVvgxsasi


C:\Users\Stepa\Desktop\solana_crypton2>spl-token mint 6gSf4aLj7A85qqDYaC5DsAad2hiamjt3xdECg7NKcFkx 10000000
Minting 10000000 tokens
  Token: 6gSf4aLj7A85qqDYaC5DsAad2hiamjt3xdECg7NKcFkx
  Recipient: J51S4AVucXEaUHKeWCPWzbyH1FKFtXmbw6fp2hiJMUi

Signature: Yaec74RiWXPiJVwfD3HgXA2d69douiW1QSH3DbWzyVzeKTaaLqgdDoHr8MCp4ZUqPVuQuVfQ6EZvji1fQhy3caK


C:\Users\Stepa\Desktop\solana_crypton2>
```

Рис. 6. Процесс создания аккаунта и эмиссия токенов

Шаг пятый: теперь произведем эмиссию токенов в желаемом количестве *spl-token mint адрес токена количество.*

А при помощи команды *spl-token accounts* мы можем узнать всю информацию про аккаунт (рис. 7).

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token accounts
Token                                         Balance
------------------------------------------------------------
6gSf4aLj7A85qqDYaC5DsAad2hiamjt3xdECg7NKcFkx  10000000
```

Рис. 7. Token аккаунт

Операции с токеном

Для того чтобы выполнять различные операции над токенами мы можем зайти в меню help при помощи команды *spl-token -h.* Там мы найдем все возможные операции над нашими токенами (рис. 8).

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token -h
spl-token-cli 2.0.15
SPL-Token Command-line Utility

USAGE:
    spl-token [FLAGS] [OPTIONS] <SUBCOMMAND>

FLAGS:
    -h, --help       Prints help information
    -V, --version    Prints version information
    -v, --verbose    Show additional information

OPTIONS:
    -C, --config <PATH>           Configuration file to use [default: C:\Users\Stepa\.config\solana\cli\config.yml]
        --fee-payer <KEYPAIR>     Specify the fee-payer account. This may be a keypair file, the ASK keyword
                                  or the pubkey of an offline signer, provided an appropriate --signer argument
                                  is also passed. Defaults to the client keypair.
    -u, --url <URL_OR_MONIKER>    URL for Solana's JSON RPC or moniker (or their first letter): [mainnet-beta, testnet,
                                  devnet, localhost] Default from the configuration file.
        --output <FORMAT>         Return information in specified output format [possible values: json, json-compact]

SUBCOMMANDS:
    account-info       Query details of an SPL Token account by address
    accounts           List all token accounts by owner
    address            Get wallet address
    approve            Approve a delegate for a token account
    authorize          Authorize a new signing keypair to a token or token account
    balance            Get token account balance
    bench              Token benchmarking facilities
    burn               Burn tokens from an account
```

Рис. 8. Виды операций над токенами

Трансфер

Теперь поговорим немного о трансферной части. Для отправки наших токенов на другой аккаунт пропишем команду *spl- token transfer ваш адрес и количество адресов получателя --fund-recipient* (рис. 9).

Согласитесь достаточно интересно вручную создавать и управлять активами. В дальнейшем на этом можно сделать прибыль (рис. 10).

Создание NFT

Разобравшись с токенами, попробуем создать что-то новое, а именно NFT. Используя уже имеющийся набором инструментов создадим свой уникальный актив. Таким образом наш токен должен быть неделим и в единственном экземпляре, а создание таких же NFT нужно заблокировать (рис. 11). При помощи команд *spl- token create-token –decimals 0*, *spl-token create-account адрес токена* и *spl-token mint адрес 1* мы как раз выполним установленные требования. А командой *spl-token authorize адрес mind –disable* ограничим эмиссию (рис. 12).

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token create-token --decimals 0
Creating token D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z

Signature: 2V48ki8WXCNrmsuSzFfVk3wyRPoLREzeabMePipCXftEb3HJctLvLXATju4LffAkKvy2QtMoSBeyRrq49zdDDqXc


C:\Users\Stepa\Desktop\solana_crypton2>
```

Рис. 9. Создание токена

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token create-account D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z
Creating account BGh4cS5RYgv79cDYjjqrRfsCdEERh3fYM15pH1oRZjMn

Signature: 2x5zRu1Efv8aSa4YayGhSbJmgwfCEFwJQRRfo5oNTUY8qisrA8jotPoQVTB8rfVH2697QwGJi7NfJ7pWwhgZX75z
```

Рис. 10. Создание аккаунта

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token mint D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z 1
Minting 1 tokens
  Token: D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z
  Recipient: BGh4cS5RYgv79cDYjjqrRfsCdEERh3fYM15pH1oRZjMn

Signature: 2aBJzuJQGRkRn4srDS4ELFUShebHqnz7CYSjFdhdeHTchZjkmcw91SzGVGZ79PWvMrKEBHeM5mXJa3xBmgSzEAuA
```

Рис. 11. Эмиссия токена в количестве одной штуки

```
C:\Users\Stepa\Desktop\solana_crypton2>spl-token authorize D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z mint --disable
Updating D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z
  Current mint authority: CV8YhhtHAvGi1JhvEoWXPD56EaMo3f5ZzS7ZF2ckHiDg
  New mint authority: disabled

Signature: EfpsoCdrsBZUtvzTMayC5jXMqEywCwdAibHnK8dJLdDFmFg5XPbFp6JdWZZ8HXwYEwZShNEWj4jkWxNrJxia1hf
```

Рис. 12. Ограничение на дальнейшую эмиссию

Одобрение токена

Создав токен и разобравшись в механике его работы, давайте попробуем извлечь из этого больше выгоды.

Последним шагом в создании токена будет являться его «одобрение». Для этого переходим на сайт Github-репозиторий, открываем репозиторий токен лист, а следом переходим в режим Fork (рис. 13) [3].

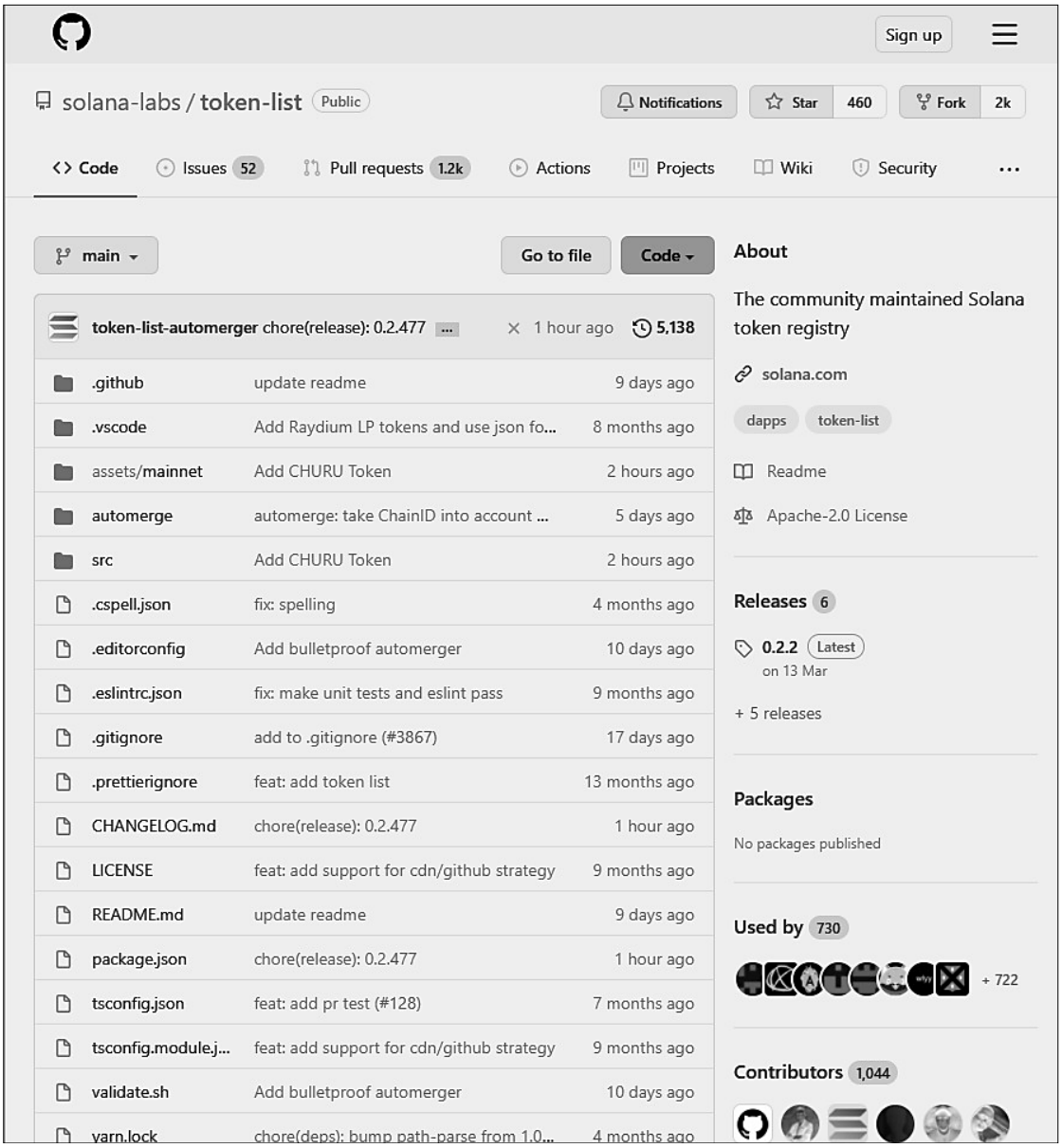

Рис. 13 Главная страница репозитория Github

Изменим файл под названием solana.tokenlist.json. Используем шаблон (рис. 14).

```
{
  "chainId": 101,
  "address": "D6wDidyDqRRhhPxVNJoBaMUnjZ3p9kU6xpQ8Cbe1Wx4Z",
  "symbol": "Cur",
  "name": "Cursach",
  "decimals": 0,
  "logoURI": "https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQjTIQKfnhpyHvWPnA9qfHe6pR44q_Ya_UeKg&usqp=CAU",
  "tags": [],
  "extensions":{
    "Discord": "https://discord.com/channels/@me"
  }
```

Рис. 14 Главная страница репозитория Github

После последнего шага остается лишь ждать, ведь рассмотрение и одобрение может быть получено лишь через пару месяцев.

Список литературы

1. Поппер Н. Цифровое Золото. Невероятная история Биткойна / Н. Поппер. Нью-Йорк: Вильямс, 2016. 350 с.

2.Coinmarket. Информация о криптовалютах. URL: https://coinmarketcap.com/ru/currencies/bitcoin/ (дата обращения: 31.08.2021 г.).

3. Github [Электронный ресурс]. Режим доступа: https://github.com/solana-labs/token-list (дата обращения: 01.09.2022 г.).

Московский государственный лингвистический университет
Moscow State Linguistic University

Сыктывкарский государственный университет им. Питирима Сорокина
Syktyvkar State University after the Pitirim Sorokin

Поступила в редакцию 04.08.2022

Информация об авторах

Филяк Петр Юрьевич – канд. техн. наук, директор Института информационных наук Московского государственного лингвистического университета, e-mail: p,filiak@linguanet.ru

Ярков Степан Сергеевич – студент бакалавриата направления подготовки «Информационная безопасность», Сыктывкарский государственный университет, e-mail: yarkov.stepan@inbox.ru

BLOCKCHAIN, CRYPTOCURRENCIES AND INFORMATION SECURITY

P.Yu. Filyak, S.S. Yarkov

An approach to ensuring information security based on the use of modern tools such as BlockChain technology is considered. An important factor in ensuring security is the device of both the Blockchain itself and various cryptocurrency networks. The text describes various types of blockchains, as well as the principles of their operation. The paper mentions such principles as PoW, RPoW, DPoS, PoH. The principles on which the blockchain is based show the degree of security of the network itself. An important factor is the auxiliary programs of the smart contract category, which are included in blockchains and ensure the reliability and security of transactions. The article presents options for implementing blockchain technology using scripts developed by the authors themselves, which are used in direct conjunction with the blockchain platforms on which they are based, without which blockchain technology cannot be implemented.

Keywords: BlockChain, PoW, RPoW, DPoS, PoH, cryptocurrency, smart contract, token, NFT, transaction, network, hash, Solana, Bitcoin, Ethereum.

Submitted 04.08.2022

Information about the authors

Petr Yu. Filyak – Cand. Sc. (Technical), Director of the Institute information Sciences, Moscow State Linguistic University, e-mail: p.filiak@linguanet.ru

Stepan S. Yarkov – Bachelor of Information Security, Syktyvkar State University, e-mail: yarkov.stepan@inbox.ru