УДК 004.4:004.056.5

РАЗРАБОТКА И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДИКИ ЗАЩИТЫ ПЕРСОНАЛЬНОГО КЛЮЧА БИТКОИН-КОШЕЛЬКА ОТ УТЕЧКИ ДАННЫХ

Стариков В.Э., Телятников А.О., Короченцев В.А., Пилипенко И.А., Черкесова Л.В.
Донской государственный технический университет, Ростов-на-Дону, e-mail: vkbdstu@gmail.com

В статье рассмотрена одна из самых нашумевших на данный момент криптовалют, а именно – биткоин. Биткоин – это цифровая валюта нашего поколения, которая еще называется криптовалютой. Данная валюта не используется Центральным банком. Биткоины могут быть использованы в качестве оплаты услуг и товаров продавцам. В ходе рассмотрения было выяснено, что такое биткоин, как начать пользоваться Биткоином и как его добывать. Вследствие рассмотрения данных вопросов была проанализирована криптостойкость данной криптовалюты и выявлена возможность улучшения защиты. На основе данных исследований авторами была предложена программная реализация методики защиты от утечки персонального ключа от биткоин-кошелька с помощью алгоритма RSA. Благодаря шифрованию пароля с помощью алгоритма RSA мы получаем более защищенный кошелек, то есть в нашем кошельке используются не только стандартные алгоритмы защиты нашего кошелька , но и защищенный пароль, к которому злоумышленник не сможет добраться. Путем тестирования было определено, что криптостойкость нашего пароля, который зашифрован с помощью алгоритма RSA повышается примерно на 30%.

Ключевые слова: криптовалюта, биткоин, электронные деньги, алгоритм RSA, защита биткоина

DEVELOPMENT AND SOFTWARE IMPLEMENTATION OF THE PROTECTION METHOD FOR THE PERSONAL KEY OF THE BITKOIN – WALLET FROM DATA LEAKAGE

Starikov V.E., Telyatnikov A.O., Korochentsev V.A., Pilipenko I.A., Cherkesova L.V.
Don State Technical University, Rostov-on-Don, e-mail: vkbdstu@gmail.com

The article discusses one of the most notorious cryptocurrencies at the moment, namely Bitcoin. Bitcoin is the digital currency of our generation, which is also called cryptocurrency. This currency is not used by the central bank. Bitcoins can be used as a payment for goods and services to sellers. During the review, it was found out what Bitcoin is, how to start using Bitcoin and how to mine it. In consequence of the consideration of these issues, the cryptoresistance of this cryptocurrency was analyzed and the possibility of improving protection was revealed. Based on the research data, the authors proposed a software implementation of a method to protect against the leakage of a personal key from a bitcoin wallet using the RSA algorithm. By encrypting the password using the RSA algorithm, we get a more secure wallet, that is, our wallet uses not only the standard security algorithms of our wallet, but also a secure password to which the attacker cannot reach. Through testing, it was determined that the encryption of our password, which is encrypted using the RSA algorithm, increases by about 30 percent.

Keywords: cryptocurrency, bitcoin, electronic money, RSA algorithm, protection of bitcoins

История биткоина насчитывает более чем десятилетние исследования в области криптографии и распределённых компьютерных сетей. Биткоин, появившийся в 2008 г. благодаря японцу *Сатоши Накамото*, уже давно стал цифровой валютой XXI в., т.е. криптовалютой. Подобная валюта не используется Центральным банком. Биткоины могут быть использованы лишь в качестве оплаты услуг и товаров продавцам [1]. Биткоины существуют только как записи о транзакциях между различными адресатами. Каждая транзакция сохраняется в книге учётов, называемой цепочкой блоков (blockchain – англ., блокчейн – рус., см. рис. 1). Поэтому баланс в явном виде узнать не предоставляется возможным. Его необходимо вычислить, посмотрев на блокчейны, относящиеся к адресу владельца.

Транзакция состоит из трех типов данных:
– input – биткоин-адрес отправителя;
– amount – количество биткоинов;
– output – биткоин-адрес получателя.

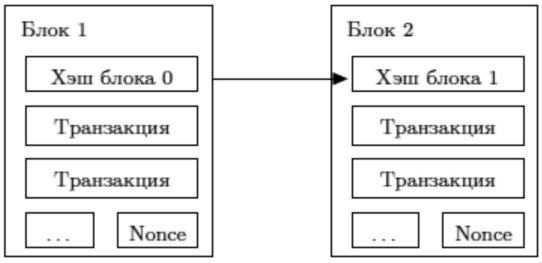

Рис. 1. Цепочка блоков биткоинов (блокчейн)

Для передачи биткоина отправителю необходимо знать имя, закрытый ключ, подписать заявку на перевод, включающую три упомянутых типа данных: *input*, *amount* и *output*. Обработка перевода осуществляется посредством *майнинга*. Вычислительные машины добавляют заявку в блок транзакций. Далее происходит процесс дешифрования, в результате которого получателю доставляются пересылаемые биткоины.

В США биткоины всегда находились под пристальным интересом властей, так как с их помощью осуществлялись тайные переводы нелегальных средств, скрывалась прибыль от налоговых служб, и др.

Политика в отношении биткоинов в настоящее время меняется. На данный момент нужны транзакции, соединённые с классическими валютами, которые должны быть привязаны к личности владельцев биткоинов.

Процесс добычи биткоинов

Когда формируется блок транзакций, активизируется процесс, называемый *майнингом*, который подтверждает его достоверность. После этого к блоку применяют математическую формулу, делая исходную последовательность ещё более непродолжительной. Итогом этих процессов считается малогабаритная последовательность, а также усечённые шаблоны букв и чисел, которые определяются понятием *хэш* (рис. 2).

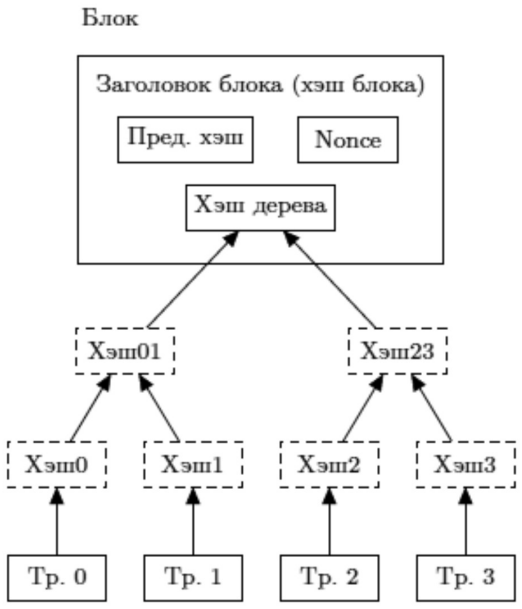

Рис. 2. Хэш – дерево транзакций

Любой новый блок формируется с применением *хэш-блока* перед ним. Это один из методов доказательства точности блока. Данная процедура формирует так называемую *восковую печать*, которая свидетельствует, что данный и предыдущий блоки являются точными [2].

Допустим, кто-то принял решение вмешаться в блок. Если это так, то все узнают об этом благодаря наличию восковой печати, и увидят фальсификацию.

Процесс добычи происходит следующим образом:

– Сделка вводится в блок.

– Майнеры проводят проверку, реальна ли транзакция.

– Они выбирают заголовок последнего блока и вставляют его в новый блок как хэш.

– Майнеры решают математическую задачу.

– Если решение обнаружено, то новый блок прибавляется к цепочке уже существующих блоков, а потом распространяется по всей сети.

Майнеры не пробуют провести проверку лишь данной транзакции – они работают над проверкой почти всех транзакций. Все без исключения транзакции блокируются в блоки с виртуальным блокированием.

Майнеры запускают компьютерную программу, чтобы найти *ключ*, открывающий данную блокировку. Как только программа отыщет его, раскроется окно, транзакция будет испытана и проведена [2].

Но осуществить данные задачи нелегко. По сути, число попыток, которое предполагает найти *верный ключ*, составляет около 1,7 млрд а вознаграждение за биткоин вручают приблизительно каждые 10 минут.

Ключом к триумфу считается наличие правильных инструментов.

В период процесса добычи (майнинга) общество трудятся с целью контроля транзакций и обеспечения их точности. Такой процесс является весьма трудоёмким, и применяет сложные математические формулы.

Процесс майнинга биткоинов

Для начала нужен биткоин-кошелек, у которого имеется личный, неповторимый биткоин. Подобный кошелек – это закодированный онлайн-счёт в банке, удерживающий вознаграждение майнера в период хода добычи. К самому кошельку необходимы правильные инструменты. Они существенно поменялись за последние несколько лет.

Раньше майнеры использовали элементарные процессоры для добычи биткоинов, так как в то время базисные рабочие станции были достаточно мощными, чтобы осуществлять необходимые задачи. Однако позднее майнеры обнаружили более надежную альтернативу – добычу на графических картах [3].

Графические процессоры были практически в 100 раз быстрее, чем обычные процессоры. При добыче биткоинов именно самый быстрый результат приводит к большим достижениям. Чтобы размножать различные криптоконверсии, также используются графические процессоры.

Программируемая полевая матрица (FPGA) даёт разработчикам аппаратного обеспечения возможность приобретения

чипов по размеру, и их настройки для добычи биткоинов ещё до их помещения в свое оборудование. Так как эта разработка намеренно настроена для добычи биткоинов, то она функционирует значительно лучше, чем обычные и графические процессоры [4].

Специализированные интегральные схемы (ASIC) считаются новым шагом в разработке биткоинов. Они созданы для обеспечения мощности майнинговых работ на скоростях дробления и используют малое количество электроэнергии, что является преимуществом для большинства майнеров, получающих большие счета за электроэнергию, которые и поглощают их прибыль. Чтобы сделать подобные микросхемы менее дорогостоящими и трудоемкими, разрабатывать их нужно для конкретной задачи. Однако почти все майнеры биткоинов уверены, что затраты на скорость стоят их инвестиций. По сути, устройства ASIC могут функционировать на скоростях до 2 Терабайт в секунду [5].

Значительная часть аппаратного обеспечения, которое использовалось в начале эры биткоинов, больше не имеет к ним отношения – оно устарело и работает слишком медленно. Новые варианты обладают большим ценовым тегом.

Цель исследования: разработка методики защиты персонального ключа биткоин-кошелька от утечки данных.

Способы защиты кошелька биткоинов от потери владельцем:

1. Создание резервной копии. Для обладателя кошелька биткоинов огромную важность имеет резервная копия. Суть состоит в том, что некоторые адреса, для сохранности вносимых изменений в транзакции, иногда не будут показываться владельцу. Поэтому и нужно создавать резервную копию кошелька.

2. Множественная аутентификация. Сейчас быстро развиваются сервисы, поддерживающие переводы биткоинов (как денежных средств) с применением множественной аутентификации. В результате этой возможности, несколько пользователей смогут частично применять для аутентификации одного адреса *общий ключ*. Так, если кому-то понадобится перевести куда–то свои биткоины, то нужно будет, дополнительно к его аутентификации для совершения транзакции, получить ещё несколько аутентификаций от других пользователей. Количество необходимых аутентификаций устанавливается во время создания адреса.

3. Создание офлайн-кошелька. Для такого метода необходимо иметь два компьютера, которые будут иметь некоторые части одного и того же кошелька. Первый компьютер должен быть отключен от любой сети. На нем и будет храниться полный кошелек и можно будет оформлять транзакции. Второй компьютер должен быть подключен к сети, а также иметь установленный «наблюдающий» кошелёк (не имеющий возможности создавать авторизованные транзакции). Таким образом, можно будет безопасно выполнять новые транзакции. Все транзакции должны подписываться на компьютере, отключенном от сети, то есть злоумышленник не сможет подписать транзакцию, а следовательно, и не сможет похитить чужие средства.

Шифрование кошелька

Если провести все описанные ранее рекомендации невозможно, то для защиты биткоин-кошелька можно использовать программу, разработанную авторами. Суть разработки заключается в следующем:

Необходимо придумать надежный пароль и зашифровать им свой кошелек. Это обеспечит надежную защиту вашего кошелька.

Первоначально нужно убедиться в сохранности пароля, иначе доступ к кошельку будет безвозмездно утерян. Существуют риски, при которых пароль быть может забыт владельцем, поэтому обычно рекомендуют сохранить бумажную копию пароля в надежном месте, например в сейфе.

Любой пароль, который содержит только буквы или узнаваемые слова, может быть сочтён слабым и легким для взлома. Сильный пароль должен содержать буквы, цифры, знаки препинания и должен быть длиной хотя бы 16 символов. Самые надёжные пароли генерируются специальными программами, разработанными специально для этой цели. Надёжные пароли гораздо сложнее запомнить, поэтому и нужны бумажные копии в сохранном месте. Одним из надёжных способов хранения пароля является зашифрованный текстовый файл, доступ к которому может получить только владелец файла, зная секретный ключ.

Описание алгоритма

В начале работы программы создаются открытый и закрытый ключи с помощью алгоритма RSA. В первую очередь нужно импортировать RSA из Crypto.PublicKey. Далее генерируется ключ RSA на 256 байт (рис. 3). Для генерации личного (приватного) ключа вызывается метод ExportKey, в который, в качестве параметров, передается ранее сформированный код доступа. Этот код будет использован стандартом PKCS, чья схема шифрования будет использована для защиты сгенерированного ключа (рис. 4). После выполнения этого алгоритма данные записываются в файл.

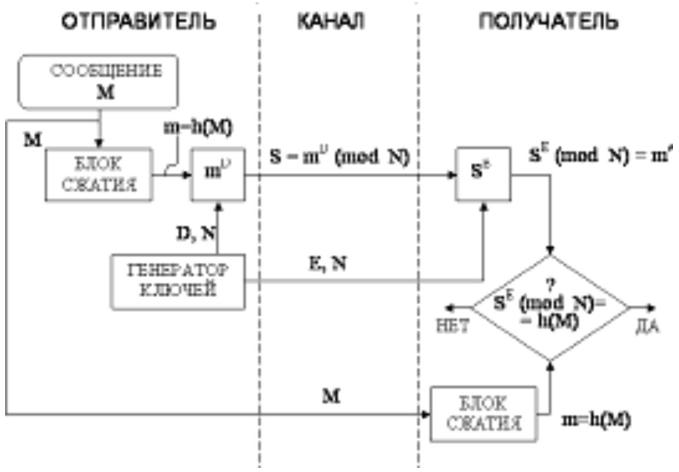

Рис. 3. Алгоритмическая схема RSA

Когда в распоряжении имеются публичный и личный ключи, с их помощью можно зашифровать файл, в котором содержится код доступа к биткоин-кошельку. Для шифрования нужно загрузить файл в программу для записи. Импортируется ключ и создается 16-битный ключ сессии. Ранее прочитанный из файла текст записывается в переменную. Далее с помощью алгоритма AES получают шифрованные данные. Их записывают в отдельные файлы.

```
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes
from Crypto.Cipher import AES, PKCS1_OAEP


with open('encrypted_data.bin', 'wb') as out_file:
    recipient_key = RSA.import_key(
        open('my_rsa_public.pem').read()
    )

    session_key = get_random_bytes(16)

    cipher_rsa = PKCS1_OAEP.new(recipient_key)
    out_file.write(cipher_rsa.encrypt(session_key))

    cipher_aes = AES.new(session_key, AES.MODE_EAX)
    data = open('text.txt', 'r')
    data = data.read()
    ciphertext, tag = cipher_aes.encrypt_and_digest(data)

    out_file.write(cipher_aes.nonce)
    out_file.write(tag)
    out_file.write(ciphertext)
```

Рис. 4. Шифрование файла, содержащего секретный ключ

Криптоанализ

Злоумышленник, получив доступ к компьютеру, на котором хранится зашифрованный файл, вполне может открыть его, прочитать и сохранить пароль от биткоин-кошелька. Однако та информация, которую он увидит, будет просто недоступна для восприятия. Ему необходимо будет каким-то образом расшифровать данные, но для этого ему требуется знать секретный ключ и алгоритм шифрования. Такими знаниями он не обладает и получить их не сможет, поэтому ему остаётся только отказаться от своей затеи.

Для демонстрации работы программы нужно показать, что владелец файла, зная секретный ключ, может прочитать информацию, хранящуюся в нем. Для работы алгоритма расшифрования нужно открыть зашифрованный ранее файл, для чтения в бинарном режиме. Далее импортируется приватный ключ.

Чтобы не возникло ошибки, в него нужно передать код доступа, который известен владельцу файла. Далее расшифровывается ключ сессии, создается заново ключ AES и расшифровываются первоначальные данные.

В конце работы алгоритма возвращается изначально зашифрованный файл, содержащий в себе информацию для доступа к биткоин-кошельку.

Результаты

Результатом работы программы будет зашифрованное содержимое файла с помощью алгоритма шифрования RSA.

Рис. 5. Пример работы программы

Выводы

Благодаря шифрованию пароля с помощью алгоритма RSA можно получить более защищенный кошелек биткоинов. Будут использованы не только стандартные алгоритмы защиты кошелька, но и защищенный с помощью алгоритма шифрования пароль, к которому злоумышленник не сможет добраться.

Криптостойкость пароля, зашифрованного с помощью алгоритма RSA, повышается на 30%. Не каждый злоумышленник продолжит попытки похитить биткоин-кошелек, поняв, что использовано дополнительное шифрование.

Так как потенциальный злоумышленник, даже имея открытый ключ и зная алгоритм шифрования, не сможет повторить закодированное сообщение, то у него нет шансов узнать пароль, а значит, и похитить кошелёк с биткоинами.

Список литературы

1. Свободная энциклопедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki (дата обращения: 20.06.2019).

2. Crypto Curancy Market Capitalizations [Электронный ресурс]. URL: http://coinmarketcap.com (дата обращения: 20.06.2019).

3. Форум Bitcoin: [Электронный ресурс]. URL: http://hit-labs.ru/ (дата обращения: 20.06.2019).

4. Coinspot Гид по Bitcoin [Электронный ресурс]. URL: http://coinspotru/analysis (дата обращения: 20.06.2019).

5. Официальный сайт Bitcoin [Электронный ресурс]. URL: https://bitcoin.org/en/how-it-works (дата обращения: 20.06.2019).