УДК 004.75.056

С.Н. Гриняев, Р.А. Злотин, А.И. Милушкин, Д.И. Правиков, И.А. Селионов,
А.Ю.Щербаков, Ю.Н. Щуко

К вопросу о создании универсального защищенного доверенного цифрового актива (токена)

Рассмотрена проблема разработки универсального защищенного доверенного цифрового актива нового поколения на основе универсальной структуры данных и новой парадигмы доверия и защищенности.

Ключевые слова: *доверие, токен, блокчейн, код аутентификации, распределенное хранение данных, информационная безопасность, аукцион, шифрование, контроль целостности, смарт-контракт, средства разработки для токенов, цифровой финансовый актив, транзакция, оператор платформы*

ВВЕДЕНИЕ

В настоящее время актуален вопрос «цифровой трансформации» российской экономики, формирования доверенной и корректной цифровой среды разработки и применения цифровых национальных технологий. Сегодня в этой области остро ощущается «давление» иностранных криптовалютных технологий, в том числе технологии оборота токенов, цифровых активов, технологии распределенного хранения данных, включая распределенные реестры (блокчейн). Кроме того, регистрируются активные попытки создания на базе технологий распределенного реестра и разного рода криптовалют реальных систем, обеспечивающих решение широкого спектра задач. Вместе с тем, как показал ряд исследований, несмотря на заявленные качества, реализованные системы не обладают свойствами информационной безопасности, что определяет их исследовательский характер.

Неразумное копирование западных технологий может иметь весьма пагубные последствия для технологической безопасности и независимости России, особенно в условиях создания «цифровой экономики», включая влияние на устойчивость российского бизнеса как на национальном уровне, так и на международной арене [1], поэтому необходимо создание технологической платформы для цифровой трансформации, которая удовлетворяла бы следующим требованиям:

- доверенность (универсальная открытая структура и открытый программный код) [2];
- национальная криптографическая локализация (использование национальных стандартов и готовность к получению соответствующих сертификатов у регуляторов);
- универсальность (возможность использования как в технологии цифровых активов, так и в работе с товарами и продукцией, а также для обеспечения государственного заказа и закупок).

Активное изучение технологий распределенного реестра отечественными специалистами привело к появлению собственных наработок в различных научно-технических коллективах. Результатом этого стало объединение усилий представителей академической и вузовской науки, поддержанных ведущими технологическими компаниями. Настоящая работа является результатом не только теоретических проработок, но и их прототипированием, что, в случае поддержки, создает возможность реализации оригинальных отечественных информационных технологий, способных положительно повлиять на развитие цифровой экономики в Российской Федерации.

ЛЕММА БЕЗОПАСНОСТИ СУБЪЕКТНО-ОБЪЕКТНЫХ СИСТЕМ

Установлено, что внедрение технологии блокчейн, несмотря на заверения различных разработчиков, порождает новые виды угроз, которые были достаточно подробно рассмотрены в статье [3] на сайте *Forklog*. В качестве примера можно привести ситуацию со смарт-контрактом, описываемую в различных источниках. В определенный момент выполнения смарт-контракта появляется необходимость получения для дальнейших вычислений значения текущего курса доллара. Технически это реализуется через «ораклиз», который обращается к сайту считающегося доверенным источника. В случае захвата данного сайта злоумышленниками появляется возможность осуществления различного рода атак на систему, на-

чиная от недоступности сайта и заканчивая манипуляцией значением курса доллара.

Неформально суть проблемы заключается в том, что пока смарт-контракт оперирует данными и другими элементами внутри блокчейн-платформы (например, мы имеем в виду только операции с криптовалютой), можно говорить об определенной безопасности. Вместе с тем, если попытаться расширить сферу применения распределенных реестров, то неизбежное взаимодействие с внешней средой приводит к возникновению различного рода угроз безопасности.

Формально утверждение о небезопасности взаимодействия с внешними источниками данных можно сформулировать в виде леммы.

Пусть существует система B, состоящая из n субъектов и m объектов:

$$B = (S, O) : |S| = n, |O| = m .$$

Для системы задано разграничение доступа в виде Декартова произведения множества субъектов и множества объектов на множество прав доступа:

$$(S \times O) \to R .$$

Данное отображение полностью описывает возможности множества субъектов по отношению к множеству объектов (в приведенных выше терминах задание такого отображения обеспечивает замыкание системы). Описываемая система считается безопасной, если данное отображение обладает двумя основными свойствами – полнотой и непротиворечивостью. Полнота означает, что право доступа определено для каждой пары (субъект–объект), непротиворечивость означает, что при задании прав доступа не существует такой пары (субъект–объект), для которой конкретное право доступа одновременно и запрещено, и разрешено.

Пусть порождается некий субъект S_i с определенными правами доступа R_{ik} по отношению к существующему объекту O_k. Порождение субъекта S_i в системе B возможно из объекта-источника O_j, при этом субъект порождается некоторым другим субъектом S_e (например, атомом-экзекутором или иной исполнительной средой выполнения смарт-контракта).

Возможны три случая:

1. Субъект S_i совпадает с существующим субъектом ($i \le n$), при этом права доступа совпадают с существующими правами. Случай тавтологии (тривиальный).

2. Субъект S_i совпадает с существующим субъектом ($i \le n$), при этом права доступа не совпадают с существующими правами. Таким образом нарушается свойство непротиворечивости.

3. Субъект S_i не совпадает с существующими субъектами ($i > n$), при этом права доступа заданы только для объекта O_k. В этом случае нарушается свойство полноты.

Таким образом, появление для замкнутой системы дополнительной активной сущности приводит к нарушению ее безопасности. Как следствие, большинство блокчейн систем, обеспечивающих оборот и использование криптомонет, в настоящее время не могут считаться безопасными.

ДОВЕРЕННЫЙ ЦИФРОВОЙ АКТИВ *OURCOIN*

С целью демонстрации подходов к созданию технологий распределенного реестра, обладающих свойствами информационной безопасности были сформулированы предложения по созданию защищенной криптовалюты *OURCOIN*.

Криптовалюта *OURCOIN* − цифровой финансовый актив – имущество в электронной форме, созданное платформой *OURCOIN* с использованием криптографических средств, являющееся мерой стоимости, признаваемой таковой неограниченным кругом лиц.

Дадим определения терминов, которые будут нами использоваться при описании работы системы.

Токен *OURCOUN* – цифровой финансовый актив − имущество в электронной форме, созданное платформой *OURCOIN* с использованием криптографических средств, удостоверяющее меру прав, предоставляемых офертой проекта *OURCOIN* его владельцу. Токен фиксируется в электронном виде (в виде специализированного файла, либо в виде звена или атома блокчейна), снабжается уникальным номером, имеет номинал, время создания и время действия (срок валидности), сетевое имя владельца и допускает проверку неизменности всех своих параметров.

Участник реестра цифровых транзакций платформы *OURCOIN* (участник; допустимы синонимы: абонент, пользователь, клиент) – физическое или юридическое лицо, прошедшее на платформе OURCOIN валидацию (идентификацию личности/принадлежности) и получившее от нее уникальное сетевое имя и осуществляющее цифровые транзакции в соответствии с правилами ведения реестра цифровых транзакций.

Сетевое имя – уникальная последовательность шестнадцатеричных цифр длиной 32 знака (при байтовой записи 16 байт), которая присваивается участнику и связана с его персональным ключом.

Персональный ключ участника – случайное число, вырабатываемое при первичной или повторной регистрации участника, служащее для получения (фиксации) и проверки кодов аутентификации токенов/криптовалюты.

Код аутентификации (КА) токена/криптовалюты – информация, включенная в токен/криптовалюту и позволяющая убедиться в неизменности его параметров, а также восстановить содержание параметров при их повреждении или намеренном изменении. Далее по тексту статьи синонимично с КА используется термин «подпись». Код аутентификации (подпись) может быть личным (сформированным пользователем), транспортным (сформированным для передачи токенов между участниками системы и служащим для проверки неизменности полученного токена) и корневым (сформированным центром учета транзакций, определение которого дано ниже).

Центр эмиссии токенов (ЦЭТ) – юридическое лицо, использующее уникальное программное обеспечение платформы *OURCOIN* с целью выработки первичных обезличенных токенов, характеризующихся только номером, номиналом и временем действия.

Центр учета транзакций (ЦУТ) − юридическое или физическое лицо, являющееся участником реестра цифровых транзакций и осуществляющее дея-

тельность по валидации и учету цифровых записей в реестре цифровых транзакций в соответствии с правилами ведения реестра цифровых транзакций, присваивающее токенам/криптовалюте код аутентификации и направляющее их пользователям.

ЦУТ является прототипом уполномоченного оператора инвестиционной платформы, о котором упоминается в законопроектах по цифровой экономике, принятых Государственной Думой РФ в первом чтении (в частности, проект Федерального закона «Об альтернативных способах привлечения инвестиций (краудфандинге)»). В перспективе ЦУТ может играть роль оператора платформы государственных услуг, нотариальных услуг, оборота отечественной криптовалюты, обеспечения судебной защиты в РФ транзакций, совершаемых в распределенном реестре.

Транзакция – гражданско-правовая сделка по передаче цифровых прав на токен/криптовалюту и/или его части, совершенная участником/участниками. *С технической точки зрения* ***транзакция*** представляет собой отраженный в материальном виде в системе процесс передачи части или всего номинала токена от одного абонента к другому. Транзакция характеризуется ее инициатором, получателем, а в части размера – переводом, сдачей и комиссией. При этом сумма номиналов перевода, сдачи и комиссии всегда равна номиналу исходного токена.

Система движения (оборота) токенов/криптовалюты – система, состоящая из абонентов, ЦЭТ и ЦУТ, обеспечивающая жизненный цикл токенов в материальной форме.

Жизненный цикл токена (ЖЦ) – период времени, устанавливаемый платформой OURCOIN с момента его эмиссии и уничтожения.

С технической точки зрения ***жизненный цикл токена*** включает следующие элементарные компоненты: эмиссию, направление пользователю, участие в транзакциях, завершение существования. В качестве составных элементов ЖЦ выступают объединение и расщепление токенов.

Уничтожение токенов не представляет финансовой опасности для клиентов и не уничтожает меры стоимости, а служит для обеспечения технических свойств платформы по аналогии с эмиссией и оборотом бумажных денег.

ВИДЫ ТОКЕНОВ В СИСТЕМЕ

Прототокен 1 – часть токена, выработанная ЦЭТ и характеризующаяся только номером, номиналом и временем действия. Не может участвовать в транзакциях, поскольку не имеет владельца.

Прототокен 2 – часть токена, снабженная именем участника и кодом аутентификации ЦУТ, а также транспортным КА, который дает возможность проверить неизменность токена при его получении абонентом.

Токен имеет свойства прототокенов 1 и 2 и снабжен КА и личной подписью владельца. Только токен участвует в транзакциях.

Таким образом, прототокен 2 получается при формировании КА ЦУТ и транспортного КА для прототокена 1, а токен – при формировании личного КА для прототокена 2.

Токен-комиссия – токен, имеющий в качестве КА ЦУТ и кода владельца одно и то же значение, он образуется при транзакциях, за которые ЦУТ взимает комиссию.

Нулевой токен – токен, получающийся в ходе транзакции, когда сдача с транзакции для ее инициатора равна нулю.

Биржевой токен – токен, используемый для биржевых операций с другими цифровыми активами, который характеризуется интегральной стоимостью, переданной абонентом-владельцем абоненту-брокеру или абоненту-бирже, не превышающей совокупной стоимости токенов, принадлежащих данному владельцу; может также использоваться для клиринга биржевых операций в заданный период.

СТРУКТУРА ТОКЕНА

Токен представляет собой защищенные от изменения данные фиксированной длины 128 байт. Структура данных, составляющих токен, представлена в табл.1.

Таблица 1

Структура данных, составляющих токен

Индекс от начала токена в байтах	Длина поля в байтах	Название поля	Примечание
0	4	Заголовок	
4	8	Номер токена	Номер токена, выработанный центром эмиссии токенов (ЦЭТ)
12	16	Контрольная информация E(Mi,Kt)	Представляет собой номер токена, дату его создания и номинал (Mi), зашифрованные на ключе токена Kt, хранящемся в ЦЭТ
28	4	Тип токена	В настоящее время в системе обращается токен с типом 1
32	4	Номинал токена целый (рубли)	
36	4	Номинал токена дробный (копейки)	

Индекс от начала токена в байтах	Длина поля в байтах	Название поля	Примечание
40	4	Параметр эмиссии	В данном проекте равен 256
44	4	Дата создания токена в формате (дд)(мм)(гг-2000) (3 байта, каждая скобка 1 байт)	
48	4	Дата валидности токена в формате (дд)(мм)(гг-2000) (3 байта, каждая скобка 1 байт)	
52	4	Уровень иерархии токена	У прототокенов 1 и 2 равен 0, для токена равен 1, при каждой транзакции увеличивается на единицу
56	8	Резервное поле тела токена	
64	16	Сетевое имя владельца токена	
80	8	Код аутентификации ЦЭТ	
88	8	Транспортный КА	
96	8	КА владельца	
104	24	Резервное поле для КА	

ОПИСАНИЕ ВАРИАНТА ПРОТОКОЛА ДВИЖЕНИЯ ЦИФРОВОГО АКТИВА

1. Центр эмиссии токенов (ЦЭТ) выпускает прототокен 1, который является началом цепочки для транзакций и передаёт его в Центр учета транзакций (ЦУТ).

2. ЦУТ снабжает его своей (корневой) подписью, транспортной подписью пользователя и отправляет пользователю (прототокен 2).

3. Пользователь проверяет транспортную подпись прототокена 2, подписывает своей личной подписью и возвращает токен в ЦУТ.

4. ЦУТ заносит токен в базу данных и одновременно передает в ЦЭТ на архивное хранение.

5. Если формируется платеж, то пользователь создает транзакцию из 4-х звеньев-кандидатов: исходная монета, сдача, перевод и комиссия. Все они подписаны транспортной подписью ЦУТ, а сдача − ещё и личной подписью отправителя платежа.

6. ЦУТ проверяет все четыре звена на правильность (совпадение суммы, корректность транспортной подписи и номера транзакции, а также наличие первого звена в своей базе), после чего передает ЦЭТ запрос на выпуск двух новых прототокенов с суммой сдачи и перевода и номером, совпадающим с номером первого звена.

7. ЦЭТ создает новые прототокены 1 на перевод и сдачу и направляет их в ЦУТ.

8. ЦУТ подписывает перевод (прототокен 1) корневой и транспортной подписями и передает получателю платежа, а сдачу − также корневой и транспортной подписями и передает отправителю.

9. Отправитель и получатель подписывают сдачу и перевод (прототокены 2) соответственно своими личными подписями и возвращают токены в ЦУТ.

Транзакция завершена. Далее операции с новыми токенами возможны.

Каждый токен всегда имеет три подписи (корневую, транспортную и личную), прототокены либо токены с дефектом одного из признаков валидности (подписи, КА) в транзакциях между пользователями не участвуют.

МЕХАНИЗМЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ ДОВЕРЕННОГО ТОКЕНА

Как было отмечено, в настоящее время существует целый ряд угроз безопасности блокчейн технологий и реализованных на их основе криптовалют, связанных с их системной архитектурой. Информационная безопасность должна обеспечиваться не только правильно выбранными и реализованными криптографическими схемами, но и другими решениями, обеспечивающими устойчивость и надежность функционирования прикладной системы.

Проблема заключается в том, что обычная монета обладает свойством неделимости и физическая передача означает изъятие у одного лица и появление ее у другого. В отличие от физической монеты токен по своей природе − это двоичная последовательность, которая в ходе обращения многократно копируется. На определенном уровне обобщения считается, что дублированием можно пренебречь. Вместе с тем, как показали исследования, наличие дублей может быть источником уязвимостей для всей системы.

В качестве исходного примера рассмотрим платеж криптомонетой поставщику товара с участием доверенного центра (необходимость существования такого центра обоснована в других работах). Такой платеж означает перечисление криптоденег с возможной уплатой комиссии и получение сдачи. С точки зрения создания распределенных систем получается система с тремя независимыми точками обработки транзакций. В силу того, что в системе платежей криптомонетами планируется использование стандартной (бытовой) вычислительной техники, без повышенных требований по надежности, постоянное функционирование точек обработки транзакций не гарантируется. Использование сети Интернет для организации взаимодействия точек как наиболее

доступной среды передачи означает использование негарантированных каналов связи.

Как следствие, в процессе осуществления описанного платежа возникает модель угроз, связанных с (не)работоспособностью точки обработки транзакций и каналов связи и, как следствие, со сбоями в прикладной системе, связанными с обработкой в независимых точках сложных транзакций. Так, в выбранном примере владелец криптокошелька должен дождаться завершения процедуры проверки и реализации токена, чтобы в случае отказа не попытаться использовать его повторно.

Указанные проблемы решаются введением в структуру токена четырех полей и механизмов их обработки: статус токена; признак токена; время изменения статуса токена; лимит времени ожидания в новом статусе. Рассмотрим назначение полей более подробно.

1. Статус токена. Должен принимать следующие значения:

1) может быть использован (аналог – монета лежит в кармане);

2) в обработке (монета передана для проверки, условное изъятие у владельца);

3) не может быть использован (монета доступна владельцу, но проверка показала наличие проблем с монетой);

4) монета истрачена.

2. Признак токена. В это поле в точке проверки заносится результат проверки. Например, несовпадение контрольной суммы токена. Более детально значения данного поля будет определено при проектировании модуля проверки.

3. Время изменения статуса токена – точное значение времени, когда токен получил новый статус. Например, начальный статус «может быть использован» присваивается после посылки токена в точку проверки, в криптокошельке значение статуса меняется на «в обработке», устанавливается время изменения статуса, а также лимит ожидания в новом статусе.

4. Лимит ожидания в новом статусе. Данное поле вводится из следующих соображений. Предположим, токен отправлен в точку проверки и на стороне кошелька имеет текущий статус «в обработке»; на стороне точки проверки произошел сбой оборудования, решение по токену не принято и, возможно, из-за потери данных не будет принято никогда. Для исключения потери монеты вводится лимит ожидания, после окончания которого токен возвращается в исходный статус, но в его признаке ставится отметка, что решение по нему не было принято из-за исчерпания лимита времени. Предполагается, что в данном примере дальнейшие разбирательства должны проводиться с привлечением операторов платформы.

На основании описанной структуры полей возможно предложить алгоритм оплаты криптомонетой со сдачей.

Шаг 0. Исходное состояние. Копия файла с данными токена находится в кошельке. Статус токена – «может быть использован». Признак токена – «отсутствует». Время изменения статуса равно времени, когда последний пользователь получил токен. Лимит времени = -1 (без лимита). Копия файла с данными токена находится в Центре учета транзакций (ЦУТ), значения полей идентичны значениям в копии в кошельке.

Шаг 1. Запрос на разделение в ЦУТ. Статус токена на стороне кошелька устанавливается «в обработке». Время изменения статуса устанавливается равным времени поступления запроса на разделение. Лимит времени = $t_{пор}$. Запрос с параметрами разделения отправляется в ЦУТ. Копия файла с данными токена в ЦУТ имеет значения полей, идентичные значениям на шаге 0.

Шаг 2. Прием запроса в ЦУТ. ЦУТ находит копию токена на своей стороне и устанавливает его статус «в обработке». В кошелек отправляется подтверждение статуса «в обработке» в виде квитанции. На основании получения квитанции в копии файла токена на стороне кошелька устанавливается признак «ЦУТ принял заявку».

Шаг 3. Направление запроса в Центр эмиссии токенов (ЦЭТ). На основании параметров заявки ЦУТ запрашивает генерацию трех (в общем случае) монет, сумма номиналов которых равна номиналу исходной монеты. Значения полей такие же, как для шага 2 (признак действует только для стороны кошелька).

Шаг 4. Генерация монет в ЦЭТ. ЦЭТ генерирует три обезличенные монеты с заданными номиналами. Статус всех трех монет – «не может быть использована». Копии файлов всех трех монет пересылаются в ЦУТ.

Шаг 5. Управление монетами в ЦУТ. Получив три монеты из ЦЭТ, ЦУТ проверяет их на соответствие запросу. Если соответствие подтверждается, ЦУТ на своей стороне присваивает исходной монете статус «истрачена», а трем новым монетам назначает новых владельцев с учетом их назначения (получатель, сдача, комиссия) и статус «может быть использована». В ЦЭТ направляется квитанция на подтверждение приема и обработки монет.

Шаг 6. Возврат сдачи. На стороне кошелька отправителя осуществляется прием копии файла криптомонеты-сдачи в кошелек. Кошелек меняет статус исходной монеты с «в обработке» на статус «истрачена».

МОДУЛИ РЕАЛИЗАЦИИ ПЛАТФОРМЫ УПРАВЛЕНИЯ ТОКЕНАМИ

Модуль первичного формирования ключа пользователя, его ключевого контейнера и сетевого имени (*InitUs*)

Формат использования: *InitUser FileUserID UserPIN RealName<RandomString>,*

где: *FileUserID* – имя файла с закрытым при помощи пароля персональным идентификатором пользователя (может быть связано с именем пользователя, но не должно совпадать с именем файла Realname);

UserPIN – пароль (пин-код или метод его ввода, например, чтение из *USB*-токена) для закрытия персонального идентификатора пользователя;

RealName – текстовый файл длиной не более 160 байт для размещения данных пользователя;

<RandomString> − необязательный параметр для улучшения работы датчика случайных чисел («разгонная строка»).

Модуль создает файл random.bin для дальнейшего использования датчика случайных чисел и файл с закрытым при помощи пароля персональным идентификатором пользователя (фактически – защищенный контейнер для хранения и передачи персонального идентификатора/ключа пользователя). Кроме того, модуль формирует сетевое имя, которое размещается в файле RealName.net в читаемом человеком виде (в виде 32 символов шестнадцатеричного кода). Первые 8 цифр определяют также имя файла, в котором сетевое имя находится в бинарном формате.

Модуль возвращает типизированные ошибки, необходимые для интеграции вызовов модулей во внешние приложения или смарт-контракт.

Возвращаемые ошибки:

«-1» – ошибка при тестировании модулей защиты;

«-2» – ошибка формата вызова (неверное количество аргументов);

«-3» – файл идентификатора (*FileUserID*) уже существует или не существует файла реального имени;

«-4» – ошибка формирования случайного числа;

«-5» – ошибка обновления случайного числа;

«-6» – ошибка записи файла пользователя (*FileUserID*);

«-7» – ошибка контрольного чтения файла пользователя (*FileUserID*).

В платформе выделяются два абонента с зафиксированными именами контейнеров – 000 – контейнер Центра эмиссии токенов (ЦЭТ) и 007 – контейнер Центра учета транзакций (ЦУТ).

Пример формирования системы из трех пользователей, ЦЭТ и ЦУТ приведен в следующей последовательности команд (смарт-контракт):

```
md 01
md 02
md 03
md CET
md CRT
copy alisa 01\alisa
initus 01\1 alisa 01\alisa 123
copy *.net 01\*.*
del *.net
copy boris 02\boris
initus 02\2 boris 02\boris 456
copy *.net 02\*.*
del *.net
copy ivan 03\ivan
initus 03\3 ivan 03\ivan 789
copy *.net 03\*.*
del *.net
initus 000 boss
copy 000 CET\000
del 000
copy gentoken.exe CET\gentoken.exe
initus 007 crt
copy 007 CRT\007
del 007
copy sendtok.exe CRT\sendtok.exe
```

Полагаем, что исполняемые модули, копируемые в создаваемые директории, есть в корневой директории. При этом также имеются текстовые файлы alisa, boris и ivan, содержащие реальные имена абонентов в системе.

Модуль эмиссии токенов – *gentoken* (*Generate Token*)

Формат использования: *GenToken UserPIN Номинал токена,* где:

UserPIN – пароль (пин-код или метод его ввода, например, чтение из *USB*-токена) для восстановления персонального идентификатора (ключа) ЦЭТ. Для приведенного макета он будет методом или строкой boss;

Номинал токена – десятичное число, не превышающее 999999.

Данный модуль также создает файл random.bin для дальнейшего использования датчика случайных чисел и файл *Glob.tcn* с закрытыми при помощи персонального идентификатора пользователя с именем 000 эмитированными токенами и ключами эмиссии, индивидуальными для каждого эмитированного токена. Предполагается, что ключевой контейнер 000 уже создан процедурой (модулем) *UnitUs*. Результатом работы данного модуля будет обезличенный токен заданного номинала, имеющий расширение *.tc0.

Модуль передачи токенов пользователям GetCrtK (Get Center Registration Transaction Keys)

Для передачи токенов пользователям необходимо сформировать транспортные ключи. Этот процесс выполняется либо абонентом самостоятельно, либо в ЦУТ при помощи модуля *GetCrtK* (*Get Center Registration Transaction Keys*).

Формат использования: *GetCRTK Файл сетевого имени UserPIN,* где:

Файл сетевого имени – файл, полученный процедурой InitUs длиной 16 байт, содержащий бинарное сетевое имя пользователя (абонента);

UserPIN – пароль (пин-код или метод его ввода, например, чтение из *USB*-токена) для закрытия транспортного ключа Центра эмиссии токенов (ЦЭТ). Этот пароль далее будет использоваться для защиты контейнера с транспортным ключом (имеет расширение *.007). Центр учета транзакций (ЦУТ) должен иметь ключи всех пользователей, поэтому пользователи могут выработать транспортные ключи самостоятельно и направить их в ЦУТ, а пароль сообщить ЦУТ отдельно (по смс, письмом или голосом). Либо пользователи высылают в ЦУТ бинарный файл своего сетевого имени, и ЦУТ формирует транспортные ключи пользователей и также отдельно (по другим каналам) сообщает им их пароли. С точки зрения безопасности это равноценная схема, поскольку пользователи не знают пароля друг друга, а ЦУТ является доверенной стороной (доверенным компонентом системы).

Модуль передачи эмитированного токена пользователю

Формат использования: *SendTok[.exe] CrtPIN CrtKeyFile(.007) CrtKeyPIN TokenFile,* где:

CrtPIN – пароль (пин-код или метод его ввода, например, чтение из *USB*-токена) для закрытия контейнера 007 ЦУТ. Этот пароль далее будет использоваться для раскрытия контейнера с ключом ЦУТ для снабжения токена КА ЦУТ;

CrtKeyFile(.007) – имя ключа пользователя, которому передается токен. Он содержит сетевое имя пользователя, которое помещается в соответствующее поле токена;

CrtKeyPIN − пароль, который далее будет использоваться для раскрытия контейнера с транспортным ключом (имеет расширение *.007);

TokenFile – имя обезличенного токена, направляемого пользователю с ключом *CrtKeyFile*(.007), который получен при помощи описанной выше процедуры *GetCrtK* (*Get Center Registration Transaction Keys*).

Результатом работы данного модуля является направленный токен с расширением *.tc7. Этот токен еще не принят пользователем (т.е. не заверен его КА).

Модуль заверения токена

Для заверения токена используется процедура *FixToken[.exe] CrtKeyFile CrtKeyPIN UserFile UserPIN TokenFile,* где:

CrtKeyFile(.007) – имя ключа пользователя, которому передается токен;

CrtKeyPIN – пароль (пин-код или метод его ввода, например, чтение из *USB*-токена) для раскрытия контейнера сетевого ключа пользователя. Указанный в методе *CrtKeyPIN* пароль далее будет использоваться для раскрытия контейнера с транспортным ключом (имеет расширение *.007);

UserFile – имя файла с закрытым при помощи пароля персональным идентификатором пользователя (контейнером) (может быть связано с именем пользователя, но, как было указано, не должно совпадать с именем файла *Realname*);

UserPIN – пароль для раскрытия контейнера пользователя;

TokenFile – имя направленного токена, который заверяется пользователем.

После заверения токен имеет 3 кода аутентификации: ЦУТ (корневой), транспортный и личный пользовательский и может использоваться для проведения транзакций (например, для передачи части его номинала другому пользователю).

РАСШИРЕНИЕ ПОНЯТИЯ ДОВЕРЕННОГО ТОКЕНА В ОБЛАСТИ ДОВЕРЕННОЙ ЦИФРОВОЙ ЕДИНИЦЫ

Развитием описанного подхода является разработка универсальной доверенной цифровой единицы (*Universal Digital Proof Unit – UDPU*), которая является развитием технологии токенов в области учета движения товаров и распределенного хранения, а также обеспечения работы транзакционных систем, включая системы электронных платежей, в том числе и трансграничные.

Универсальная доверенная цифровая единица (УДЦЕ) – это зафиксированная в электронном (цифровом) виде (в виде специализированного файла, либо в виде звена или атома блокчейна) мера учета хранения и перемещения данных, включая персональные цифровые активы, электронные или безналичные деньги, цифровые права, электронные документы и другую цифровую информацию, снабженная уникальным номером, временем создания и временем действия (сроком валидности), сетевым именем владельца и другими параметрами, необходимыми для хранения и обмена информацией и допускающая проверку неизменности всех своих параметров.

Дадим определения терминов, которые будут нами использоваться при описании работы системы.

Владелец УДЦЕ – идентифицированный уникальным сетевым именем участник системы (допустимы синонимы: абонент, пользователь, клиент) системы учета и оборота УДЦЕ, при этом его сетевое имя в обязательном порядке включено в ее состав.

Сетевое имя – уникальная последовательность шестнадцатеричных цифр, однозначно связанная с персональным ключом пользователя и его реальным именем. Сетевое имя вырабатывается при помощи криптографической процедуры.

Персональный ключ пользователя – случайное число, вырабатываемое при первичной или повторной регистрации пользователя, служащее для получения (фиксации) и проверки кодов аутентификации УДЦЕ.

Код аутентификации (КА) УДЦЕ – информация, включенная в состав универсальной доверенной цифровой единицы и позволяющая убедиться в неизменности его параметров, а также восстановить содержание параметров при их повреждении или намеренном изменении.

Центр эмиссии (ЦЭ) – выделенный абонент, вырабатывающий по запросам других абонентов либо самостоятельно первичные обезличенные УДЦЕ.

Центр учета (центр регистрации транзакций, ЦУТ, ЦРТ) – выделенный абонент, снабжающий УДЦЕ кодом аутентификации и направляющий их пользователям. Кроме того, ЦУТ (ЦРТ) регистрирует движение УДЦЕ от одного абонента к другому.

Транзакция – отраженный в материальном виде в системе процесс передачи всей УДЦЕ или ее части от одного абонента к другому. Транзакция характеризуется ее инициатором (отправителем) и получателем.

Система движения (оборота) УДЦЕ – система, состоящая из абонентов, ЦЭ и ЦУТ, обеспечивающая жизненный цикл в материальной форме.

Жизненный цикл – включает следующие элементарные компоненты: эмиссию, регистрацию, направление пользователю, участие в транзакциях, завершение существования. В качестве составных элементов ЖЦ выступают объединение и расщепление УДЦЕ, а также перевод их в машиночитаемую форму в виде двумерного кода.

Применение УДЦЕ позволяет решить такие актуальные задачи в области цифровых активов и финансов, биржевой деятельности и учета движения товаров, как:

- создание токена − цифровой монеты, которая абсолютно устойчива к хищению за счет наличия неизменного имени владельца;
- полное блокирование угроз, связанных с использованием зарубежных криптографических алгоритмов;
- создание цифровых акций и векселей произвольного (при этом неизменяемого и самовосстанавливаемого) номинала;

Таблица 2

Преимущества Универсальной доверенной цифровой единицы

№	Свойство	Чем обеспечивается
1	Управляемая анонимность транзакций	Оригинальным протоколом транзакций, в котором содержание транзакции может быть зашифровано или открыто, при полном закрытии никакой информации о транзакции получить невозможно
2	Управляемая анонимность имен	Имена могут образовываться таким образом, что по сетевому имени невозможно определить реальное имя
3	Анонимность УДЦЕ	Содержит только сетевое имя владельца
4	Высокая криптографическая защищенность УДЦЕ и транзакций	Использованием российских криптографических алгоритмов
5	Возможность использования любого блокчейна	Протокольной независимостью от алгоритма работы блокчейна и возможностью помещения данных в звено блокчейна и их извлечения из звена блокчейна любого вида
6	Полный трекинг транзакций с сохранением анонимности владельца	Оригинальной структурой УДЦЕ и их учета в виде впервые используемой блок-матрицы (развитие блокчейна в 2D)
7	Возможность восстановления транзакций и УДЦЕ даже при утрате приватной информации от хранилища (кошелька)	Особенностью протокола транзакций с четырехзвенным подтверждением и использованием ключей парной связи
8	Возможность работы с центром учета транзакций и без него (как централизованная, так и децентрализованная схема)	Особенностью протокола транзакций
9	Возможность управления жизненным циклом УДЦЕ (в частности, предельным сроком жизни по времени)	Оригинальной структурой УДЦЕ и протоколом транзакций
10	Полная защита от повторного использования	Хранением УДЦЕ в блок-матрице
11	Отсутствие необходимости в удостоверяющих центрах	Симметричной ключевой системой
12	Возможность проведения транзакции с подтверждением информации получателем (защита от ошибочных перечислений на кошельки)	Особенностью протокола транзакций с четырехзвенным подтверждением приема
13	Технологическая независимость от лидеров криптовалютного рынка и контролирующих органов стран –инициаторов санкций	Оригинальным протоколом, использованием российских криптоалгоритмов
14	Независимость от действующего рынка криптовалют и токенов	Оригинальным протоколом, использованием российских криптоалгоритмов
15	Широкая область применения	Возможностью трансформации в машиночитаемую форму (двумерный код)

- обеспечение безопасных биржевых торгов при помощи номинирования валют (включая криптовалюты) к УДЦЕ;
- сквозное решение логистических задач как путем снабжения УДЦЕ товаров (в виде маркера двумерного кода), так и хранением УДЦЕ в распределенном реестре;
- защита информации при проведении транзакций, защите персональных и конфиденциальных данных, хранимых в распределенном реестре;
- возможность создания совершенных систем учета произведений искусства и удостоверения их подлинности.

Преимущества Универсальной доверенной цифровой единицы (УДЦЕ) отражены в табл. 2.

ВЫВОДЫ

Предлагаемая технология создания цифрового актива позволяет формировать весь необходимый спектр типов доверенных токенов и операций с ними. Целесообразно криптографические операции реализовывать на основе отечественных криптоалгоритмов для обеспечения свойств доверенности и возможности последующей сертификации и аттестации разработанных решений государственными регуляторами. Свойства доверенности токена или его развития – УДЦЕ − должны быть обеспечены во всех формах их преобразования и обращения, что достигается только благодаря применению соответствующей доверенной цифровой платформы. Таким образом, доверенная технология определяется свойствами доверенной цифровой единицы и доверенной цифровой платформы.

СПИСОК ЛИТЕРАТУРЫ

1. Биктимиров М.Р., Щербаков А.Ю. Проблемы синтеза доверенных систем // Труды ИСА РАН. – 2012. – Т. 53. – С. 264–271.
2. Правиков Д.И., Щербаков А.Ю. К вопросу об изменении парадигмы информационной безопасности // Системы высокой доступности. – 2018. – Т. 14, № 2. – С. 35–39.
3. Васильков Г. «Разбор основных экономико-технических угроз для блокчейн-приложений» // Интернет-журнал «Форклог». – URL: https://forklog.com/ razbor-osnovnyh-ekonomiko-tehnicheskih-ugroz-dlya-blokchejn-prilozhenij-prodolzhenie

Материал поступил в редакцию 03.07.18.

Сведения об авторах

ГРИНЯЕВ СЕРГЕЙ НИКОЛАЕВИЧ – доктор технических наук, старший научный сотрудник, декан Факультета комплексной безопасности топливо-энергетического комплекса Российского государственного университета нефти и газа (национальный исследовательский университет) им. И.М. Губкина, Москва
e-mail: gsn@gubkin.pro

ЗЛОТИН РОМАН АЛЬФРЕДОВИЧ – кандидат юридических наук, адвокат Адвокатской палаты Московской области, юридический консультант проекта *OURCOIN*, Москва
e-mail: rzlotin@yandex.ru

МИЛУШКИН АЛЕКСАНДР ИВАНОВИЧ – заместитель директора управляющей компании проекта "Технопарк Пушкино", г. Пушкино Московской области
e-mail: mialiv@techprom.biz

ПРАВИКОВ ДМИТРИЙ ИГОРЕВИЧ – кандидат технических наук, руководитель научно-образовательного центра новых информационно-аналитических технологий Факультета комплексной безопасности топливо-энергетического комплекса РГУ нефти и газа (национальный исследовательский университет) им. И.М. Губкина; научный сотрудник Института комплексной безопасности и специального приборостроения Российского технологического университета (ИКБиСП РТУ), Москва
e-mail: d_pravikov@mail.ru

СЕЛИОНОВ ИГОРЬ АНАТОЛЬЕВИЧ – заместитель директора управляющей компании проекта "Технопарк Пушкино", г. Пушкино Московской области
e-mail: uk@techprom.biz

ЩЕРБАКОВ Андрей Юрьевич – доктор технических наук, профессор, ведущий научный сотрудник ВИНИТИ РАН, главный научный сотрудник Центра развития криптовалют и цифровых финансовых активов ВИНИТИ РАН; научный консультант проекта "Технопарк Пушкино"
e-mail: x509@ras.ru

ЩУКО ЮЛИЯ НИКОЛАЕВНА – кандидат географических наук, ВРИО директора ВИНИТИ РАН, зав. отделом научной информации по комплексным межотраслевым проблемам ВИНИТИ РАН, Москва
e-mail: dir@viniti.ru