Индекс УДК 004.75
Код ГРНТИ 49.33.35
DOI: 10.22204/2410-4639-2026-129-01-103-112

А.А. ИГОНИН*

Безопасный и дешёвый криптокошелёк на базе доверенной SIM-карты

В работе приведена современная классификация блокчейн сетей и узлов, а также клиентов блокчейн, выполняющих функции криптокошельков. Рассмотрен функционал аппаратного устройства электронной подписи на базе доверенной SIM-карты и возможности интеграции аппаратного устройства с различными программными криптокошельками, перечислены конкурентные преимущества подобного технического решения.

Ключевые слова: блокчейн, криптокошелёк, доверенная SIM-карта

Исходная идея использования распределённого публичного реестра или базы данных на основе технологии электронной подписи последовательной цепи блоков (далее — блокчейн) в качестве децентрализованного платёжного средства (децентрализованных финансов, DeFi) в дальнейшем привела к стремительному развитию во многих отраслях и сферах экономического взаимодействия различных хозяйствующих субъектов. В значительной мере данному росту сопутствовало создание и работа основанных на смарт-контрактах (*smart contract*) децентрализованных приложений (DApp), создаваемых разработчиками с помощью некоторого языка программирования, совместимого с той или иной блокчейн-платформой.

В настоящее время успешные примеры использования децентрализованных приложений отмечаются в сфере финансовых транзакций (автоматическое выполнение условий перевода средств, обеспечение кредитования, депозиты и прочее) [1, 2], логистике и поставках (автоматизация процессов поставок, отслеживание товаров и обеспечение выполнения условий договоров) [3], страховании (автоматическое выполнение условий страховых выплат при наступлении определённых событий) [4], процедурах токенизации активов (выпуск различных цифровых активов и управление ими) [5], игровой индустрии (управление внутриигровыми активами, правила распределения призов и наград) [6].

Разрабатывается всё больше блокчейн-решений с различными характеристика-

* **Игонин Андрей Александрович** — заместитель начальника отдела, АО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН».
E-mail: info@ipmce.ru

ми, ориентированными на разные области применения. Блокчейн-платформы развиваются и совершенствуются, предлагают новые способы организации различных бизнес-процессов, делая их более прозрачными, безопасными, децентрализованными и также, при правильной имплементации, экономически более выгодными по сравнению с классическим подходом, основанным на традиционных (фиатных) средствах платежей и клиент-серверных решениях.

С точки зрения разработчика, блокчейн модель или сеть может обладать уникальной архитектурой и собственным фреймворком (эталонный клиент блокчейн), а может быть так называемым клоном некоторой существующей блокчейн-платформы с различными внесёнными изменениями в протокол сети. Первый вариант принято называть **нативным** (*native*) блокчейном или блокчейном на собственных решениях, а второй — **форком** (*fork*) исходного блокчейна. При этом также принято различать так называемые «мягкие» форки (*softfork*) и «жёсткие» форки (*hardfork*). «Мягкий» форк является полностью совместимым с исходной версией протокола блокчейн, и внесённые изменения технически всегда возможно отменить. «Жёсткий» форк несовместим с исходным кодом как минимум в части майнинга криптовалюты. Как следствие, «жёсткий» форк приводит к созданию новой криптовалюты, неспособной работать в одной сети с оригиналом.

По отношению совместимости (возможности кроссплатформенных взаимодействий) все блокчейн-платформы можно разделить на классы эквивалентности. Определение совместимости различных блокчейн требует проведения анализа их протоколов по следующим направлениям:

- стандарты токенов;
- механизмы консенсуса;
- смарт-контракты;
- протоколы обмена данными при взаимодействии узлов.

Все блокчейн сети также принято подразделять на два основных типа, получивших своё наименование по аналогии с ключами ассиметричных криптосистем:

- **открытый** (публичный) блокчейн;
- **закрытый** (приватный) блокчейн.

Своеобразным мостом между Пользователями и протоколом блокчейн сети выступает **блокчейн клиент** — программное обеспечение и/или физическое устройство, которое позволяет «подключаться» к сети блокчейн. Примеры эталонных блокчейн клиентов: Geth для сети Ethereum [7], Bitcoin Core для сети Bitcoin [8].

Приходящая на смену клиент-серверной модели Web2.0 новая форма цифровой инфраструктуры Web3.0 [9], где основной акцент сделан на децентрализации, прозрачности и пользовательском контроле, предполагает использование вычислительной модели взаимодействия блокчейн, в которой данные и приложения защищаются не различными централизованными посредниками, а децентрализованной сетью [10].

Узлами или нодами блокчейн принято называть устройства блокчейн сети, которые в совокупности отвечают за хранение копий распределённого реестра блокчейн, проверку транзакций и общение компонентов сети друг с другом. Данные узлы представляют собой «строительные кирпичи» архитектуры блокчейн, и от степени их защищённости зависит безопасность децентрализованных приложений и самой сети в целом.

С точки зрения протокола в различных блокчейн сетях могут быть реализованы и одновременно сосуществовать разные типы узлов. При этом в зависимости от практической реализации их функциональные характеристики могут пересекаться. Однако общепринятой является следующая классификация узлов блокчейн сети:

1. **Полные ноды или суперноды** (***full nodes, supernodes***)

Суперноды хранят полную копию всей цепи блоков блокчейн, а также участвуют в проверке и подтверждении (валидации)

транзакций, обеспечивают следующий функционал:

- проверка транзакций на соответствие правилам блокчейн сети (проверка электронных подписей, «двойных трат» кошельков и прочих условий);
- распространение информации о новых блоках транзакций по всей блокчейн сети, обеспечение синхронизации блокчейн для всех участников;
- поддержка безопасности путём участия в алгоритме консенсуса и голосовании о валидности новых блоков транзакций, обеспечение защиты блокчейн сети от различных атак и некорректных данных.

2. **Архивные ноды**

Архивные ноды хранят не только текущее состояние блокчейн, но и всю историю изменений. В отличие от полных нод обладают урезанным функционалом. Используются для запроса исторических данных, а также для восстановления состояния сети на любой момент времени. Как правило, имеют высокие требования к аппаратному обеспечению.

3. **Лёгкие ноды (*light nodes*)**

Лёгкие ноды вместо полной копии всего реестра блокчейн хранят только заголовки блоков. В отличие от полных нод обладают урезанным функционалом. Другие особенности:

- рассчитаны для использования в устройствах с ограниченными ресурсами, например, для абонентских терминалов;
- могут использоваться для проведения транзакций и проверки их состояния без необходимости загружать весь реестр блокчейн.

4. **Валидаторы (*validators*)**

Основной функционал нод-валидаторов заключается в проверке и подтверждении (валидации) транзакций, а именно:

- поддержание консенсуса блокчейн сети: валидаторы согласовываются между собой относительно состояния блокчейн сети и правильности транзакций, предлагая или голосуя за включение конкретных транзакций в блокчейн сеть;
- проверка транзакций: валидаторы проверяют каждую транзакцию на соответствие правилам протокола и на наличие достаточного количества средств для её осуществления, отклоняя при этом недопустимые транзакции и блокируя попытки мошенничества;
- формирование новых блоков: в некоторых блокчейн сетях валидаторы также отвечают за создание новых блоков, содержащих недавно проведённые транзакции.

В узком смысле валидаторами называют производителей блоков с алгоритмом консенсуса Proof of Stake.

5. **Майнинговые ноды или производители блоков (*mining nodes, block producer nodes*)**

Основной функционал майнинговых нод заключается в формировании и добавлении новых блоков в блокчейн сеть. Майнинговые ноды используют специализированное аппаратное обеспечение и потребляют значительное количество электрической энергии. В узком смысле майнинговыми нодами называют производителей блоков с алгоритмом консенсуса Proof of Work.

6. **Узлы Remote Procedure Call или провайдеры (*RPC nodes*)**

Основной функционал узлов RPC заключается в обеспечении доступа к сети блокчейн для различных клиентов сети блокчейн. Узлы RPC часто используются теми, кто не имеет или не может запустить свою собственную суперноду или лёгкую ноду. Любой Пользователь при подключении своего клиента блокчейн через провайдера неявно доверяет его честности, поскольку никакой работы по самопроверке не проводится. Данные узлы также именуются RPC-провайдерами, в частности провайдерами криптокошельков.

Отметим, что по своей сути блокчейн сеть предназначена для обслуживания конечных Пользователей, поэтому важной частью технологии блокчейн являются клиенты блокчейн, которые принято обозначать термином криптокошельки (*wallets*).

Криптокошелёк — это программное обеспечение и/или физическое устройство, которое позволяет Пользователям одновременно взаимодействовать с различными блокчейн сетями, предоставляя доступ к криптовалютам, хранящимся в сетях путём выполнения транзакций.

В отличие от узлов, которые выполняют функции хранения копии распределённого реестра блокчейн, проверки криптовалютных транзакций и общения между собой, криптокошельки обеспечивают хранение криптографических ключей Пользователей, подписание, отправку и получение транзакций, а также мониторинг баланса и истории транзакций.

Криптографические ключи Пользователей, хранящиеся в криптокошельках, предоставляют собой пары закрытых и открытых ассиметричных ключей, выработанных согласно заданным стандартам протоколов сетей блокчейн с использованием, как правило, алгоритмов ассиметричной криптографии на группе точек эллиптических кривых. Закрытые ключи необходимы для формирования электронной подписи (ЭП) транзакций Пользователя, открытые — для идентификации Пользователя в сетях блокчейн и проверки ЭП транзакций.

С точки зрения формы существования криптокошельки подразделяются на:

- **программные** (обладают только цифровой формой);
- **аппаратные** (представляются в виде физического носителя (например, USB-токен));
- **бумажные** (документ, на котором напечатан закрытый ключ (как правило, в виде QR-кода)).

Если рассматривать криптокошелёк как средство хранения криптографических ключей, необходимое владельцам криптовалют для доступа к различным сетям блокчейн и управления своими криптовалютами, то все криптокошельки можно разделить на следующие группы.

Горячие криптокошельки существуют только в цифровой форме, постоянно подключены к сети, доступ к средствам Пользователей можно получить через браузер или мобильное приложение. Такие криптокошельки удобны для быстрых транзакций, но уязвимы для различных угроз информационной безопасности.

Примеры: MetaMask [11], Coinbase Wallet, Exodus.

Холодные (жёсткие) криптокошельки для доступа к средствам не требуют прямого подключения к сети, для хранения криптовалют используются в автономном режиме. Подразделяются на аппаратные холодные кошельки (подключаются к сети опосредовано, только когда нужно осуществить транзакцию) и бумажные холодные кошельки (зачастую используются как резервные копии аппаратного или программного криптокошелька). Считаются более безопасными с точки зрения получения доступа к закрытым ключам Пользователей.

Примеры: Ledger [12], Trezor, KeyStone.

Как горячие, так и холодные криптокошельки относятся к так называемым **некастодиальным** криптокошелькам. В отличие от них существуют также **кастодиальные** криптокошельки (*custodial wallet*) — для которых управление ключами доверено третьей стороне, например, криптовалютной бирже или специализированному сервису.

Основным удобством кастодиальных кошельков является невозможность утраты доступа к нему вследствие потери Пользователем пароля, ключа или seed-фразы. Однако платой за это является полная зависимость и прозрачность Пользователей для третьей стороны.

Использование горячих кошельков оправдано для совершения повседневных транзакций, а основной капитал следует хранить на холодных кошельках.

Криптокошельки можно также классифицировать по степени их автономности и способу взаимодействия с сетью блокчейн:

- **Толстый криптокошелёк или полноценный клиент** предназначен для проверки всей истории транзакций блокчейна (каждая транзакция каждого

Пользователя за всё время существования блокчейна начиная с блока генезиса). Фактически толстый кошелёк является супернодой с добавлением функционала криптокошелька Пользователя. Опционально, полноценные клиенты могут также хранить подтверждённые ранее транзакции и предоставлять данные другим программам блокчейна. Полноценный клиент использует значительные компьютерные ресурсы, но при этом он обеспечивает пользователям полную автономность.

- **Тонкий криптокошелёк или облегчённый клиент (клиент с упрощённой проверкой платежей, *Simplified-Payment-Verification*, SPV)** подключается к какому-либо узлу сети (например, узлу RPC) для получения и отправки информации о транзакциях, но в то же время обеспечивает локальное хранение пользовательского секретного ключа криптокошелька, частичную проверку получаемых транзакций и независимое создание исходящих транзакций.
- **API-криптокошелёк или сторонний API-клиент** предназначен для взаимодействия с сетью блокчейн через систему API сторонних разработчиков, а не путём прямого подключения. Такой криптокошелёк может храниться у Пользователя или на сторонних серверах, но при этом будет полностью доверять удалённому серверу, который будет передавать ему точную информацию и обеспечивать его конфиденциальность и анонимность.

В зависимости от среды функционирования криптокошельки также можно условно разделить на следующие категории:

- **Десктопный криптокошелёк** является исторически первым типом криптокошелька. Именно такой криптокошелёк обычно разрабатывается в качестве эталонного варианта. Многие Пользователи работают с десктопными криптокошельками по причине предлагаемых ими «богатых» возможностей, автономности и управляемости. Однако работа в распространённых операционных системах связана с известными недостатками в плане обеспечения безопасности, поскольку данная среда функционирования часто оказывается плохо настроенной и незащищённой.
- **Мобильный криптокошелёк** в настоящее время можно назвать наиболее распространённым типом криптокошелька. Эти приложения работают в операционных системах абонентских терминалов или планшетов, и зачастую представляют собой оптимальный выбор для начинающих Пользователей. Многие из этих кошельков рассчитаны в основном на простоту и удобство использования, но есть и полнофункциональные мобильные кошельки для опытных Пользователей. Чтобы не загружать и не хранить большие объёмы данных, многие мобильные кошельки получают информацию с удалённых узлов. Это снижает уровень анонимности, поскольку позволяет третьим лицам получать сведения о пользовательских адресах и балансах. Также обладает недостатками десктопного криптокошелька.
- **Веб криптокошелёк**. Доступ к вебкошелькам открывается через браузер, а сам криптокошелёк находится на сервере стороннего сервиса. Большинство подобных систем лишают Пользователей контроля над своими ключами в обмен на простоту использования. Однако некоторые из этих сервисов используют клиентский код, запускаемый в браузере, что даёт возможность сохранить контроль над ключами блокчейна в руках владельца, хотя его зависимость от сервиса всё равно ставит конфиденциальность под угрозу.
- **Аппаратные устройства подписи или аппаратные криптокошельки** представляют собой, как было указано ранее, оборудование для хранения ключей и подписания транзакций с помощью специализированного аппаратного и микропрограммного обеспечения. Обычно они подключаются к десктоп-

ному, мобильному или веб-кошельку через USB-кабель, беспроводной интерфейс (NFC) или камеру для работы с QR-кодами. Поскольку все операции с криптовалютами выполняются исключительно внутри специализированного оборудования, такие кошельки менее уязвимы для различных типов атак.

Стоит отметить, что подавляющая часть блокчейн-сообщества в качестве криптокошельков в основном использует «удобные» решения, основанные на плагинах, интегрируемых в различные браузеры. Криптографические ключи в таких криптокошельках содержатся в криптоконтейнерах, стойкость которых основывается на сложности пароля Пользователя. Кроме того, в момент формирования ЭП для хэш-значения транзакции криптографические ключи считываются в оперативную память среды функционирования в явном или маскированном виде, и, как следствие, могут быть перехвачены хакерскими программами.

В последнее время «медийной» критике также подвергается практика использования изготовленных известными производителями аппаратных и бумажных криптокошельков. Опасения вызывает возможная реализация угроз внутреннего нарушителя на производстве данных устройств и носителей информации, особенно в свете наличия спроса на персональные или учётные данные покупателей, а также предложения таких сведений в даркнете.

В связи с чем предлагается к рассмотрению модель, обладающая удобством использования программного криптокошелька, наряду с безопасностью классического аппаратного криптокошелька на основе USB-токена, но превосходящая его с точки зрения обеспечения анонимности, а также итоговой стоимости приобретения устройства.

Далее подробно рассмотрим вопросы обеспечения безопасности реализации криптокошелька на базе SIM-карты.

Под программным обеспечением (ПО) криптоядра SIM-карты будем понимать специальное программное обеспечение (СПО), предназначенное для исполнения на аппаратном средстве среды функционирования (АС СФ), представленном микросхемной картой (МК).

Под SIM-картой будем понимать МК HUADA CIU98M25 с предустановленным в неё ПО криптоядра.

Основное предназначение криптоядра SIM-карты заключается в обеспечении аутентификации в ядре сети подвижной радиосвязи согласно рекомендации по стандартизации Р 1323565.1.003-2024, а также взаимодействии с различными электронными Сервисами, использующими возможности ЭП Владельцев SIM-карт (например, сервисами электронного документооборота), и устройствами IoT на основе поддерживаемых SIM-картой криптографических функций хэширования, шифрования, имитозащиты, проверки и формирования ЭП.

Программное обеспечение среды функционирования SIM-карты содержит:

1) операционную систему (ОС) оператора сети подвижной радиосвязи (далее — ОСПРС), предоставляющую основной функционал для абонентского терминала;
2) динамическую библиотеку (ДБ) коммерческих организаций, предоставляющую дополнительный функционал, отсутствующий в ОС, для абонентского терминала.

МК, на которой функционирует ПО криптоядра, оснащена 32-разрядным процессором SC000 архитектуры ARM v6-M, который поддерживает два режима работы: привилегированный и непривилегированный.

Привилегированный режим процессора доступен только для ПО криптоядра. ПО СФ (как ОС, так и ДБ) доступен только непривилегированный режим процессора.

ПО криптоядра предоставляет ОС и ДБ ограниченный и управляемый доступ к операциям записи и стирания в энергонезависимой памяти МК.

Для изоляции ресурсов памяти МК, используемых ПО криптоядра, от ПО СФ применяется модуль защиты памяти (memory protect unit, MPU). Более подробно, при

подаче питания (или сигнала сброса) на МК происходит передача управления ОС. Перед передачей управления ПО криптоядра включает MPU и настраивает его таким образом, что ОС не имеет доступа (ни на запись, ни на чтение) к областям памяти (энергонезависимой и оперативной), используемым ПО криптоядра. Также ОС не имеет доступа к областям памяти, используемым ДБ.

При каждом вызове ОС функций ДБ происходит перехват управления и передача его ДБ. После перехвата управления и перед его передачей ПО криптоядра перенастраивает MPU таким образом, что ДБ не имеет доступа (ни на запись, ни на чтение) к областям памяти (энергонезависимой и оперативной), используемым ПО криптоядра. Также ДБ не имеет доступа к областям памяти, используемым ОС.

Поскольку ОС и ДБ выполняются в непривилегированном режиме процессора, они не могут выключить или перенастроить MPU.

Для доступа к аппаратным функциям МК используется специальная область адресного пространства МК, доступная только ПО криптоядра. Изоляция (на чтение и на запись) данной области адресного пространства от ПО СФ также осуществляется при помощи MPU.

Получая управление, ОС или ДБ не имеют доступа (ни на запись, ни на чтение) к специальной области адресного пространства, используемого для управления аппаратными функциями МК. Также они не могут изменить настройки доступа MPU, поскольку выполняются в непривилегированном режиме процессора.

Таким образом, с точки зрения возможности извлечения ключевой информации непредусмотренным разработчиками ДБ способом обеспечивается аналогичный криптоядру уровень безопасности, который соответствует требованиям, предъявляемым к СКЗИ по классу КС3. А с учётом того, что формирование ключевой информации для нужд ДБ будет выполняться криптоядром SIM-карты на основе верифицированных безопасных криптографических алгоритмов с использованием принципа диверсификации источников случайных последовательностей (передача в защищённом виде в криптоядро SIM-карты на этапе её производства и эксплуатации нескольких случайных последовательностей в процессе взаимодействия с независимыми СКЗИ), можно утверждать, что SIM-карта с предустановленной ДБ будет представлять собой доверенное, высоконадёжное и недорогое аппаратное устройство подписи криптокошелька, предназначенное для массового использования.

Более того, разработчики ДБ могут предусмотреть поддержку широкого спектра криптовалют за счёт реализации различных схем ЭП:

- RSA,
- Schnorr,
- ElGamal (включая ГОСТ, ECDSA, KCDSA, EDS, SM2),

использующих вычисления как в кольцах вычетов, так в различных эллиптических кривых (ЭК), например:

- NIST,
- SECP,
- BrainPool.

Кроме того, разработчики ДБ могут предусмотреть поддержку расширенного функционала криптокошельков за счёт реализации правил различных протоколов блокчейн. Например, стандартов:

- Bitcoin Improvement Proposals (BIP-32) [13],
- BIP-39,
- BIP-44 и других.

При этом единственным естественным ограничением для реализации всего вышеперечисленного будет являться только размер flash-памяти, выделяемый в доверенной SIM-карте под нужды ДБ.

Предполагаемые сценарии взаимодействия доверенной SIM-карты и клиента блокчейн существенно зависят от наличия того или иного транспортного канала связи между ними. Например, возможна реализация не слишком удобного для Пользователей решения, связанного с извлечением

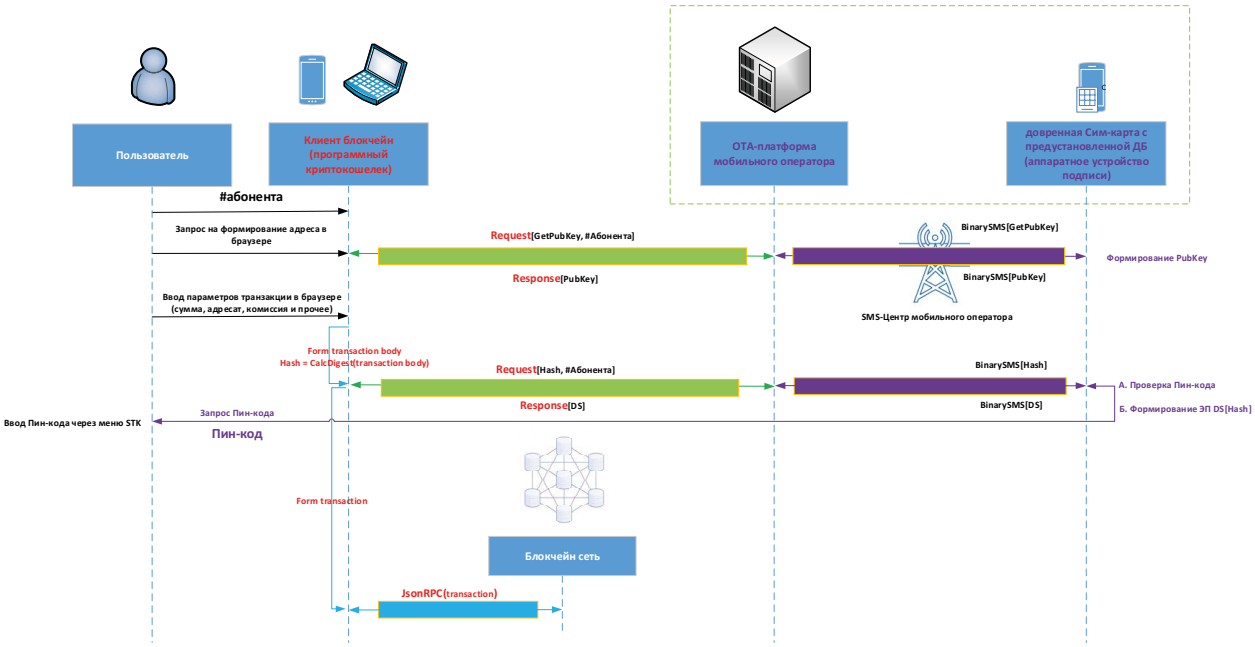

Рис. 1. *Сценарии взаимодействия Владельца доверенной SIM-карты с криптокошельком с использованием ОТА платформы ОСПРС*

доверенной SIM-карты из абонентского терминала и помещением её в специальный считыватель, соединённый с ПК.

Для приёма и передачи команд взаимодействия также возможно использование беспроводных каналов связи. На рис. 1 представлен универсальный сценарий взаимодействия с задействованием инфраструктуры ОСПРС. Универсальность обеспечивается инвариантностью относительно используемой ОС абонентского терминала.

Минимальный функционал, который должна обеспечивать ДБ доверенной SIM-карты:

- формирование и хранение ключей ЭП;
- ответ на запрос получения ключей проверки ЭП;
- ответ на запрос подписания хэш-значения транзакций.

Стоит отметить, что в рамках предложенного сценария обеспечивается только безопасность использования ключей ЭП, но не гарантируется, что Пользователь будет подписывать именно ту самую транзакцию, которая отображается на экране планшета, абонентского терминала или монитора ПК, поскольку за это отвечает выбранный Пользователем программный криптокошелёк, который потенциально может содержать уязвимости либо может использоваться в потенциально небезопасной среде.

Для решения данной проблемы существует возможность усложнения сценария взаимодействия с добавлением следующих участников:

- клиент блокчейн (Сервис) на базе АПК HSM, напрямую взаимодействующий с доверенной SIM-картой и выполняющий доверенное вычисление хэш-значений транзакций;
- специальное устройство с возможностью доверенного ввода и отображения информации (trusted monitor).

Таким образом, конкурентными преимуществами имплементации предложенной модели являются:

- повышение уровня безопасности использования ключей ЭП за счёт защищённого от НСД доверенного компонента SIM-карты;
- выполнение генерации ключей ЭП с использованием встроенных верифицированных безопасных криптографических алгоритмов, реализующих принцип диверсификации источников случайных последовательностей: на ос-

нове передаваемых в защищённом виде в доверенную SIM-карту на этапе её производства и эксплуатации случайных последовательностей в процессе взаимодействия с независимыми СКЗИ класса не ниже КС3.

ЛИТЕРАТУРА

1. Сотниченко Е.А., Ахмед Н.И., Баранова Е.В. Использование блокчейн-технологий в экономическом секторе: потенциал и будущее направление // Прогрессивная экономика. 2025. № 10. С. 299–321. DOI: 10.54861/27131211_2025_10_209.
2. Китанин С.С., Чемерис О.С., Прокопов М.А. Внедрение блокчейн-технологий в финансовом секторе экономики // Экономика, предпринимательство и право. 2025. Т. 15. № 4. С. 2963–2976. DOI: 10.18334/epp.15.4.122927.
3. Фальченко О.Д., Стремоусова Е.Г. Оценка эффективности внедрения технологии блокчейн для оптимизации транспортной логистики // Национальные интересы: приоритеты и безопасность. 2025. № 8 (449). С. 182–203. DOI: 10.24891/mmlieq.
4. Асяева Э.А. Блокчейн-технологии в страховании: перспективы и ограничения // НИР. Экономика фирмы. 2025. Т. 14. № 4. С. 60–64. DOI: 10.12737/2306-627X-2025-14-4-60-64.
5. Андрюшин С.А. Токенизация реальных активов: классификация, платформы, приложения, возможности и проблемы развития // Russian Journal of Economics and Law. 2024. Т. 18. № 1. С. 88–104. DOI: 10.21202/2782-2923.2024.1.88-104.
6. Смоликова Т.М. Блокчейн-революция в играх: формирование новой культуры цифрового взаимодействия // Sciences of Europe. 2024. № 145. С. 21–27. DOI: 10.5281/zenodo.129094601.
7. go-ethereum: Official Go implementation of the Ethereum protocol [Электронный ресурс]. URL: https://geth.ethereum.org
8. Bitcoin Core [Электронный ресурс]. URL: https://bitcoincore.org
9. Web3 в большом бизнесе: тренды, теория и практика [Электронный ресурс]. URL: https://sber.pro/publication/web3-v-bolshom-biznese-trendi-teoriya-i-praktika
10. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. 2008. URL: https://bitcoin.org/bitcoin.pdf
11. MetaMask [Электронный ресурс]. URL: https://metamask.io
12. LEDGER [Электронный ресурс]. URL: https://ledger.com
13. BIPs (Bitcoin Improvement Proposals) [Электронный ресурс]. URL: https://bips.xyz

Secure and Cheap Crypto Wallet Based on a Trusted SIM Card

Andrey Aleksandrovich Igonin — Deputy Head of the Department, IPMCE "Institute of Precision Mechanics and Computer Engineering named after S.A. Lebedev RAS".
E-mail: info@ipmce.ru

The article provides a modern classification of blockchain networks and nodes, as well as blockchain clients that perform the functions of crypto-wallets. The functionality of an elec-tronic signature hardware device based on a trusted SIM card and the possibilities of inte-grating the hardware device with various software crypto-wallets are considered, and the competitive advantages of such a technical solution are listed.

Keywords: blockchain, crypto-wallet, trusted SIM card

REFERENCES

1. Sotnichenko E.A., Akhmed N.I., Baranova E.V. Ispolzovanie blokcheyn-tekhnologiy v ekonomicheskom sektore: potentsial i budushchee napravlenie // Progressivnaya ekonomika. 2025. № 10. S. 299–321. DOI: 10.54861/27131211_2025_10_209 (in Russian).
2. Kitanin S.S., Chemeris O.S., Prokopov M.A. Vnedrenie blokcheyn-tekhnologiy v finansovom sektore ekonomiki // Ekonomika, predprinimatelstvo i pravo. 2025. T. 15. № 4. S. 2963–2976. DOI: 10.18334/epp.15.4.122927. (in Russian)
3. Falchenko O.D., Stremousova E.G. Otsenka effektivnosti vnedreniya tekhnologii blokcheyn dlya optimizatsii transportnoy logistiki // Natsionalnye interesy: prioritety i bezopasnost. 2025. № 8 (449). S. 182–203. DOI: 10.24891/mmlieq (in Russian).
4. Asyaeva E.A. Blokcheyn-tekhnologii v strakhovanii: perspektivy i ogranicheniya // NIR. Ekonomika firmy. 2025. T. 14. № 4. S. 60–64. DOI: 10.12737/2306-627X-2025-14-4-60-64 (in Russian).
5. Andryushin S.A. Tokenizatsiya realnykh aktivov: klassifikatsiya, platformy, prilozheniya, vozmozhnosti i problemy razvitiya // Russian Journal of Economics and Law. 2024. T. 18. № 1. S. 88–104. DOI: 10.21202/2782-2923.2024.1.88-104 (in Russian).
6. Smolikova T.M. Blokcheyn-revolyutsiya v igrakh: formirovanie novoy kultury tsifrovogo vzaimodeystviya // Sciences of Europe. 2024. № 145. S. 21–27. DOI: 10.5281/zenodo.129094601 (in Russian).
7. go-ethereum: Official Go implementation of the Ethereum protocol [Electronic resource]. URL: https://geth.ethereum.org
8. Bitcoin Core [Electronic resource]. URL: https://bitcoincore.org
9. Web3 v bolshom biznese: trendy, teoriya i praktika [Electronic resource]. URL: https://sber.pro/publication/web3-v-bolshom-biznese-trendi-teoriya-i-praktika (in Russian)
10. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. 2008. URL: https://bitcoin.org/bitcoin.pdf
11. MetaMask [Electronic resource]. URL: https://metamask.io
12. LEDGER [Electronic resource]. URL: https://ledger.com
13. BIPs (Bitcoin Improvement Proposals) [Electronic resource]. URL: https://bips.xyz

Image

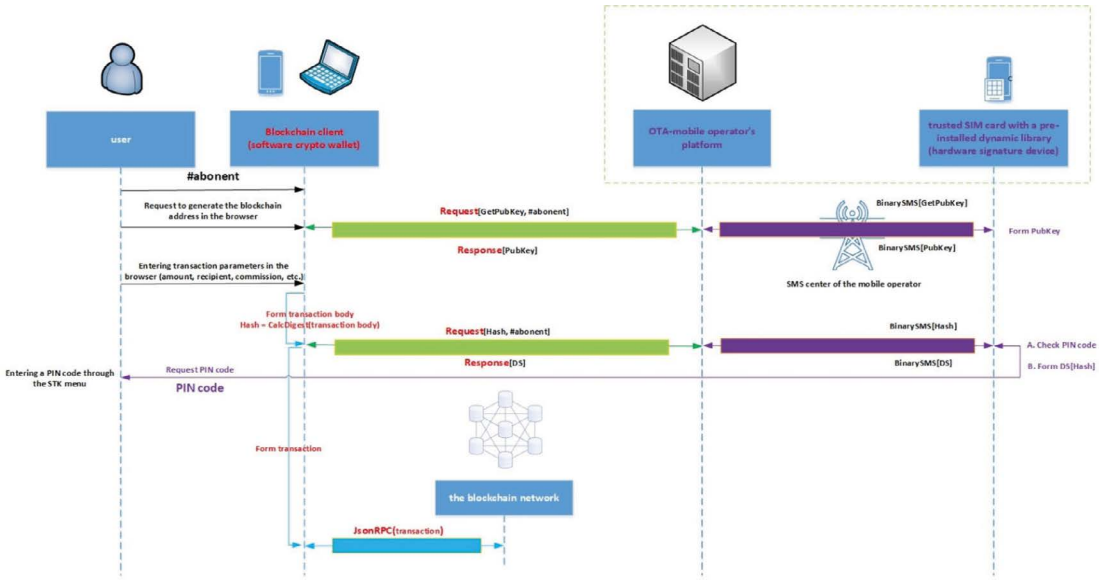

Fig. 1. *Scenarios for the interaction of a trusted SIM-card owner with a crypto wallet using the OTA-mobile operator's platform*