ИНФОРМАЦИОННЫЙ АНАЛИЗ

УДК 004.032.056

С.Н. Гриняев, Д.И. Правиков, К.А. Разгуляев, А.А. Рязанова, Д.В. Хан, А.Ю.Щербаков

Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра*

Рассмотрена проблема создания универсального методологического подхода к формированию и обоснованию архитектуры и протокола квантового распределенного реестра на основе квантовых коммуникаций и специализированного протокола обмена квантовыми ключами.

Ключевые слова: *квантовая криптография, код аутентификации, распределенные реестры, блокчейн, протокол, консенсус, ключи, электронная подпись, обмен ключами, безопасность, шифратор*

ВВЕДЕНИЕ

При разработке, создании и эксплуатации транзакционных систем, составляющих значительную часть действующих информационных систем, возникает целый ряд проблем. Это связано с интенсивной цифровизацией, высоким и постоянно растущим объемом трафика, увеличением количества включенных в сеть пользователей и агентов, генерирующих транзакции, формированием моделей и бизнес-процессов прямого взаимодействия элементов информационной системы.

Практически любая транзакция, в первую очередь, финансовая, с точки зрения её участников должна обладать следующими априорными свойствами:

1) идентификация отправителя / получателя транзакции;

2) подтверждение полномочий отправителя / получателя;

3) определение наличия финансовых или иных ресурсов для совершения финансовой транзакции;

4) определение наличия финансовых ресурсов для оплаты совершения финансовой транзакции (комиссии);

5) протоколирование и невозможность отказа от совершенной транзакции;

6) возможность обращения к третьей стороне для разрешения возможных конфликтов в рамках национального или международного правового поля;

7) возможность контроля совершения финансовых транзакций.

Существующие финансовые системы обладают вышеописанными свойствами, обеспечивающими безопасность транзакций для их участников. При этом традиционные институты в виде банков встроены в эти системы и несут определенную и исторически сложившуюся функциональную нагрузку.

Развитие технологий распределенного реестра в определенной степени обусловлена попытками обеспечить безопасность за счет соответствующих свойств и возможностей информационных технологий. Как представляется, выбор пользователей будет осуществлен в пользу тех систем, которые смогут обеспечить заданный уровень безопасности при условии сокращения времени совершения транзакций и снижении накладных расходов.

Таким образом, у агентов или пользователей в отношении больших транзакционных систем возникают обобщенные требования:

- невозможность подмены/вброса/изъятия транзакций;
- защищенная и доверенная среда передачи данных и проведения транзакций;
- выстраивание региональных, локальных замкнутых экосистем и периметров для государств, корпораций, сообществ;
- транзакции в режиме реального времени/экономически целесообразные транзакции;
- возможность передачи материальных ценностей, а не только токенов и цифровых документов, через общедоступную транспортную сеть.

В классическом виде транзакция производятся посредством инфраструктуры, требующей наличия большого количества посредников и процедур, что ведет к увеличению стоимости транзакции, возможности посредников, монополистов влиять на процесс ее осуществления. Так, финансовые транзакции

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90042

Рис. 1. Трансформация финансовых транзакций в киберфизической среде

осуществляются с помощью банков, платежных систем и других посредников, следствием чего является удорожание и возрастание времени платежей и переводов. При этом надо учитывать, что сегодня финансовая транзакция неотличима от любой другой цифровой транзакции и использует единую киберфизическую инфраструктуру с общими требованиями безопасности.

Технологии распределенных реестров позволяют организовать транзакции между цифровыми агентами на принципах прямого взаимодействия, сокращая время и стоимость транзакций за счет устранения посредников (рис. 1).

Сегодня системы распределенных реестров проектируются, по большей части, как приватные сети для корпоративных целей, т. е. с ограниченным числом участников, имеющих доступ к общей системе журналирования (записи информации о происходящих с каким-то объектом или в рамках какого-то процесса событиях в журнал/файл) или организации обмена сообщениями, а также обладающих определенными правилами и инструментами организации записей, включая протоколы консенсуса, верификационные ноды (узлы или компьютеры сети), инфраструктуру. Одной из проблем в использовании приватных (корпоративных распределенных реестров) является обеспечение безопасности транзакций.

Основные отличия инфраструктуры распределенных реестров (блокчейна):

- обязательная криптографическая идентификация всех участников сети (по публичному ключу или производному идентификатору);
- повсеместное использование электронной подписи; все пересылаемые сообщения шифруются и подписываются;
- для усиления защиты от скомпрометированных или злонамеренных узлов используются более сложные избыточные схемы передачи сообщений.

Другая важнейшая особенность работы протоколов распределенных реестров – это внутренняя экономика, которая позволяет использовать в протоколах стимулы в виде вознаграждения или штрафы – в случае наличия доказательств некорректного или злонамеренного функционирования. Это обеспечивает возможность построения открытых сетей, в которых узлы могут динамически подключаться без разрешения третьей стороны.

Протоколы распределенных реестров требуют большой пропускной способности сети, особенно для функционирования алгоритмов распределенного консенсуса. Повышение защищенности их работы напрямую связано с количеством передаваемых сообщений и может требовать kN-kN^2-kN^3 сообщений на итерацию (блок) в зависимости от выбранной модели, где N – число узлов, поддерживающих работу протокола, k =1,2,…, n – параметр протокола.

Отличительной особенностью предлагаемой технологии с использованием квантовых коммуникаций является оптимизация сетевой инфраструктуры для работы протоколов распределенных реестров, и в некоторых аспектах – прямая интеграция. Эта инфраструктура позволяет создавать защищенную масштабируемую распределенную транзакционную платформу, устойчивую к большинству возможных атак, с существенно более высокой стоимостью проведения атаки.

На базе такой инфраструктуры (как закрытой, так и открытой) реализуются базовые сервисы, такие как финансовые транзакции с различными экономическими моделями и финансовыми активами, сохранение хешзначений и временных меток данных в распределенном реестре, менеджмент профилей, заключение договоров и многое другое.

КВАНТОВЫЕ КОММУНИКАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ

В настоящее время происходит формирование международных стандартов технологий распределенных реестров, в рамках которых предусматривается, что обмен данными между устройствами требует верификации для демонстрации того, что транзакции не были подменены или взломаны в процессе передачи. Поэтому сенсорам «умных устройств» необходимо иметь криптографически доказанный источник сообщения, проверенный на аппаратном уровне. Такая верифика-

ция должна быть обеспечена в течение всего времени функционирования системы и распределена в пространстве (не должна зависеть от местоположения «умного устройства») [1].

Телекоммуникационная составляющая распределенных реестров – организация каналов связи на физическом и логическом уровнях – является в этом смысле как инфраструктурой для обеспечения эффективности и надежности обмена в распределенном реестре, так и потенциальным инструментом манипулирования, контроля, взлома транзакций (особенно в сетях общего пользования, не в рамках выделенных периметров) [2].

Одна из ключевых проблем для телекоммуникационной инфраструктуры и распределенных реестров – возможность создания устойчивого квантового компьютера, способного взломать любую систему распределенного реестра за счет существенно более высокой производительности по сравнению с традиционными компьютерами, что, в свою очередь, требует использования криптографических алгоритмов, устойчивых к квантовым вычислениям [3].

В связи с этим, одним из перспективных направлений в работе с данными угрозами является использование технологий квантовой рассылки ключа для обеспечения безопасности транзакций в распределенных реестрах. Перечислим некоторые направления и работы по данной тематике:

- использование квантовых ключей для цифровой подписи транзакции в ряде работ российских и иностранных исследователей [4, 5]. Данная концепция предполагает, что каждая пара нод (узлов) или агентов соединена по классическому каналу и одновременно по авторизованному квантовому каналу. Каждая пара нод может устанавливать последовательность секретных ключей, используя квантовое распределение ключей. Эти ключи в дальнейшем используются для подписи сообщений;
- улучшение протоколов консенсуса, где ноды реестра используют протокол *Proof of Infrastructure*, получая преимущества по энергозатратам на консенсус, а конечные пользователи – квантовые ключи для шифрования транзакций перед отправкой в сеть;
- квантовый биткойн, подразумевающий реализацию цифровой валюты, существующей в виде квантового состояния кубита [6], где любая транзакция влечет за собой изменение состояния кубита, а передача состояния осуществляется за счет квантовой спутанности, однако на данный момент подобная концепция (в отличие от квантового распределенного реестра) возможна лишь как математическая конструкция, которую невозможно реализовать физически в силу отсутствия необходимых технологий, – для большинства протоколов необходима реализация квантовой памяти, хранение квантовых состояний, что на сегодняшний день пока недоступно.

Квантовая рассылка ключа позволяет безопасно генерировать и передавать секретные абсолютно стойкие ключи на основе использования законов квантовой физики. Обнаружение перехвата при этом может быть выполнено за счёт использования одиночных фотонов для кодирования сигналов.

Согласно законам физики одиночный фотон нельзя незаметно измерить, разделить или скопировать.

Любое подслушивание в канале сразу обнаруживается, так как вносит в процесс передачи информации многочисленные легко обнаруживаемые ошибки [7].

Квантовые коммуникации позволят избавиться от необходимости больших вычислительных мощностей для формирования блоков, позволят закрыть информацию на центрах обработки данных и сохранить ее целостность.

Назовем важные преимущества квантовых коммуникаций:

- гарантированная защита от прослушивания в каналах связи, а также невозможность подмены данных в процессе передачи;
- безопасная передача секретного ключа в стандартных телекоммуникационных каналах, что позволяет передавать и менять новые ключи с максимальной частотой и не использовать классические средства передачи ключа, в том числе, для мобильных и автономных устройств, обеспечивая безопасность управляющих сигналов и сигналов связи;
- отсутствие необходимости создавать бронированное оптоволокно и применения специальных средств защиты телекоммуникаций для спецслужб и военных, а также корпораций с собственными сетями;
- возможность замены VPN и любых программных средств обеспечения безопасности каналов передачи за счет применения средств шифрования на физическом уровне (при перехвате злоумышленником квантовый ключ разрушается, а попытки получить доступ к информации выявляются автоматически).

ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕННОГО РЕЕСТРА

Основная идея квантового распределенного реестра (квантового блокчейна) – создавать протокол обмена информацией и ее взаимной верификации для различных алгоритмов консенсуса в системе, в которой при помощи квантового распределения ключа и симметричного шифрования обеспечивается защита от ключевых угроз, например, от прослушивания транзакций. При этом в такой системе вычислительные ноды соединены между собой квантовыми каналами связи (рис. 2).

Таким образом, мы имеем N пользователей и M нод, пользователи подключены к одной или нескольким нодам. Ноды, в свою очередь, соединены между собой по матрице связности SV размера MxM, при этом элемент $SV\ ij$ матрицы SV равен 1, если нода i соединена с нодой j квантовым каналом связи.

Требования и положения к хранению квантовых ключей и обеспечению криптографических процедур

Очевидно, если ноды связаны квантовым каналом, то у них имеются в некоторый момент синхронизированные квантовые криптографические ключи $KNODE\ ijt$, где i и j – номера связанных нод, а t – момент времени.

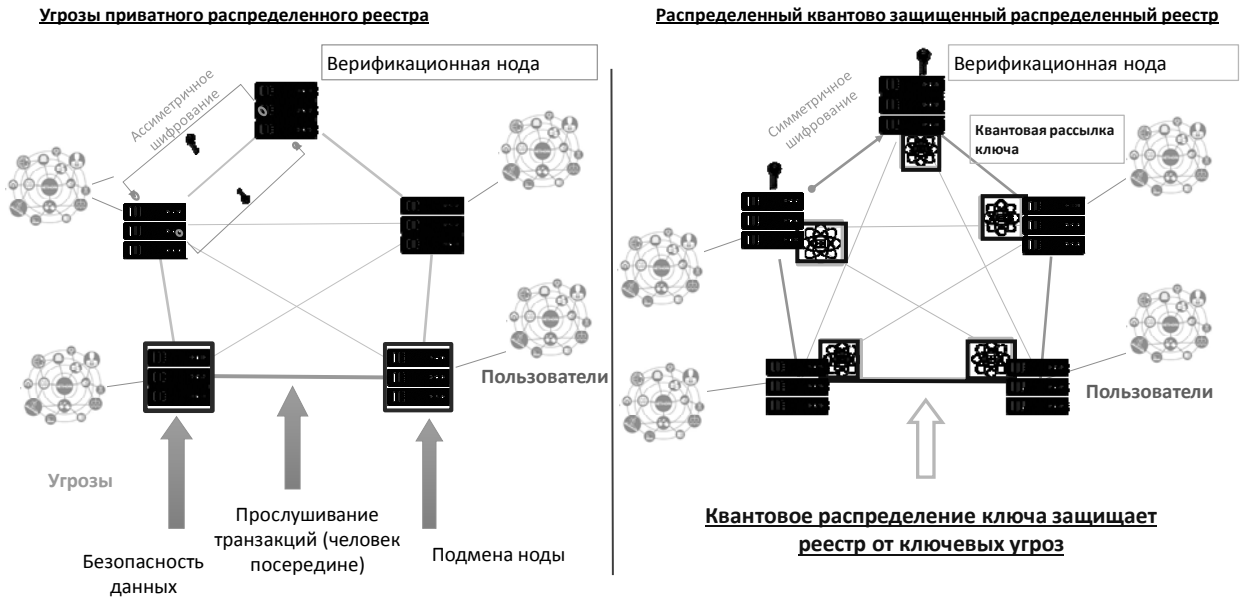

Рис. 2. Угрозы приватной сети распределенного реестра и квантово защищенный реестр

Также очевидно, что для нод желателен режим накопления ключей и сохранения их в неизвлекаемой памяти квантового шифратора, который содержит вычислитель, производящий операции шифрования и расшифрования на хранимых в его памяти неизвлекаемых ключах, выработанных по квантовому протоколу. При этом на вход шифратора поступает информация для шифрования или расшифрования и номер ключа, находящегося в неизвлекаемой памяти. Тогда связка с распределенным реестром может строиться на основе симметричных алгоритмов.

Информация в ноду может поступать как от пользователя распределенного реестра, так и от другой ноды. В первом случае нода должна иметь *Ksi* – сетевой ключ пользователя, на котором производится информационный обмен с распределенным реестром, либо с другими пользователями напрямую, если они подключены к одной ноде, либо через другие ноды. При этом нода может верифицировать полученную от пользователя информацию следующим образом:

1) нода *m* получает информацию от *i*-го пользователя и расшифровывает или проверяет ее при помощи кода аутентификации (КА, имитовставки) при помощи ключа *Ksi*;

2) нода *m* передает в другую ноду *f* полученную от пользователя информацию, дополняя ее КА. При этом используется механизм, согласно которому нода вырабатывает случайный ключ *Rmft*, шифрует его на *KNODE ijt* и помещает результат в звено распределенного реестра, после чего на *Rmft* вычисляет код аутентификации пользовательской информации и также помещает его в то же звено;

3) для проверки нода извлекает из звена распределенного реестра зашифрованный ключ Rmft, расшифровывает его на квантовом ключе внутри шифратора и проверяет на нем код аутентификации пользовательской информации;

4) в системе накапливается заверенная нодами информация, которая может быть проверена на квантовых ключах нод, хранящихся в неизвлекаемой памяти квантовых шифраторов, обслуживающих ноды, по номеру квантового ключа и может быть использована для построения произвольной модели консенсуса (по признаку прохождения информации через ноду).

Краткое описание протокола

Введем следующие обозначения:

Xi – пользователь распределенного реестра;

Ai – цифровая информация, описывающая пользователя;

Kpi – персональный ключ (персональная информация) пользователя;

Ksi – сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с нодой;

Ci – ключевой контейнер пользователя, представляющий собой персональную информацию пользователя (персональный или сетевой ключ), закрытый на пароле пользователя при помощи обратимой криптографической процедуры;

Si – сетевое имя пользователя, однозначно связанное с *Ai*;

KNODE ijt – синхронизированные квантовые криптографические ключи, где *i* и *j* – номера связанных нод, а *t* – момент времени;

INFOij – информация *i*-го пользователя, сформированная на его рабочем месте, и направляемая для хранения и обработки в распределенный реестр, имеющая условный номер *j*;

Kvij – квитанция, сообщающая о результате обработки *j*-го информационного блока для *i*-го пользователя;

Vm – запрос на извлечение информации из распределенного реестра;

I=Im(x, k) – функция вычисления имитовставки от информации *x* на ключе *k;*

y=E(x,k) – функция шифрования информации *x* на ключе *k*;

x=D(y,k) – обратная операция – функция расшифрования информации *y* на ключе *k*.

Таким образом мы имеем дело с симметричными криптографическими алгоритмами, когда для шифрования и расшифрования используется один и то же ключ.

Легко заметить, что функция вычисления имитовставки обладает возможностью как авторизации пользователя, так и контроля целостности передаваемой и хранимой информации. В связи с этим мы называем функцию вычисления и проверки имитовставки кодом аутентификации.

Полагаем, что пользователь системы имеет персональный вычислитель (ноутбук, смартфон или выделенный криптокомпьютер), подключенный при помощи каналов связи (телекоммуникационной среды) к одной из нод.

Для регистрации в системе пользователь *Xi* при помощи датчика случайных чисел с гарантированными статистическим свойствами создает ключи *Kpi* – персональный ключ (персональная информация) пользователя распределенного реестра и *Ksi* – сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с нодой и формирует контейнеры *Ci1=E(Kpi,Pi1)* и *Ci2=(Ksi,Pi2)*, где *Pi1, Pi2* – пароли пользователей для защиты соответствующих контейнеров.

Далее пользователь формирует сетевое имя как *Si=E(C, Kpi*Ai)*, где $*$ – функция смешивания персональной информации и описания пользователя, *C* – избранная константа. После формирования сетевого имени и контейнера *Ci2* эти данные синхронизируются между пользователем и нодой, к которой он подключен. Для подготовки данных для отправки их в распределенный реестр пользователь может применять электронную подпись на своем персональном ключе.

Однако наличие двух ключей (*Kpi* – персонального ключа *i*-го пользователя распределенного реестра и *Ksi* – сетевого ключа пользователя) позволяют достигать свойства эквивалентности симметричного кода аутентификации (КА) электронной подписи. Для этого КА под одной и той же информацией должен быть сформирован дважды – на *Kpi* и *Ksi*. Тогда оператор может проверить авторство и подлинность, но не сможет изменить содержание, поскольку оно зафиксировано пользователем и может быть проверено только им.

Таким образом, двойное обеспечение транзакции или ее части двумя КА позволит наделить систему свойствами электронной подписи, но при этом не использовать ассиметричные криптографические процедуры и не разворачивать инфраструктуру удостоверяющих центров.

Далее пользователь формирует запрос *Zij = Im([INFOij,Si,Tk],Ksi)* и направляет его в ноду. Нода проверяет КА пользователя под запросом, тем самым проводя как аутентификацию отправителя, так и проверку целостности данных.

В том случае, если *INFO* содержит имена отправителя и/или получателя информации *Ssi* и *Srj,* для этих имен выполняются процедуры: *y1= E(Ssi, Ksi)* и *y2=E(Srj,Ksi).* Благодаря этому имена отправителя и получателя становятся недоступными для нарушителя, а оператор распределенного реестра, используя процедуру расшифрования *D* и ключ *Ksi*, имеет возможность получить реальные имена пользователей.

Далее для информации *INFO* вычисляется код аутентификации на ключах *Rmft* и информация и код помещаются в распределенный реестр, как описано выше. Ключи должны иметь нумерацию по номеру пользователя, номерам нод, для которых они обеспечивают взаимодействие, моменту времени внутри системы и номеру записи в реестре.

При отведении на поле номера по 16 байт общий объем служебного номерного поля составит 5x16=80 байт, к которым присоединяется зашифрованный ключ проверки транзакции с имитовставкой для проверки правильности его расшифрования. Тогда любая транзакция реестра может быть проверена нодами по номеру поля с использованием накопленных квантовых ключей.

Существенным преимуществом этого протокола является то, что для фиксации целостности каждого элемента распределенного реестра используется отдельный ключ, что полностью снимает ключевую нагрузку на код аутентификации, вычисленный по алгоритму имитовставки.

Для создания цепочки блоков в информацию для вычисления имитовставки необходимо добавить код аутентификации предыдущего блока.

В протоколе существенно важна необходимость реализации для квантового шифратора надежного алгоритма контроля качества случайных последовательностей.

Таким образом, квантовый шифратор, защищающий обмен трафиком между нодами и взаимодействующий с распределенным реестром, должен удовлетворять требованиям:

- наличие аппаратных или аппаратно-программных датчиков случайных чисел высокого качества;
- наличие механизма контроля качества случайных последовательностей, используемых для формирования ключей, в том числе и квантовых;
- возможность накопления и хранения в неизвлекаемой памяти по меньшей мере тех квантовых ключей, которые использованы при формировании записей распределенного реестра;
- обеспечение выполнения криптографических процедур с ключами, хранящимися в неизвлекаемой памяти и входными данными, при этом никакая информация о ключе не должна выходить за пределы шифратора;
- однозначная идентификация по номеру ключей для выполнения операций;
- использование отдельного ключа для вычисления кода аутентификации каждого звена распределенного реестра.

ПРИМЕР РЕАЛИЗАЦИИ АРХИТЕКТУРЫ КВАНТОВОГО БЛОКЧЕЙНА

Рассмотрим уровни реализации приватной сети распределенного реестра в физической сети, защищенной квантовыми коммуникациями (рис. 3).

Сетевой уровень предполагает физическую передачу данных по защищенным каналам, а уровень распределенного реестра – набор протоколов, географически распределенных верификационных нод, обеспечивающих логику работы реестра. Уровень приложений обеспечивает бизнес логику, конечные пользовательские интерфейсы.

Таким образом, решение, назовем его условно системой «квантовых коммуникаций», представляет распределенный реестр, включающий набор верификационных нод, защищённых квантовыми коммуникациями, позволяющими создавать стойкую к атакам доверенную среду, предназначенную для организации транзакций в режиме реального времени и организации безопасного канала передачи данных между верификационнными нодами.

При этом подсистема квантовой рассылки ключа предназначена для управления процессом генерации случайных битовых последовательностей между отправителем и получателем, между верификационными нодами.

Система «квантовых коммуникаций» выполняет следующие функции:

- предотвращение несанкционированного доступа к квантовым каналам связи между верификационными узлами путем контроля параметров квантового канала: уровня ошибок при передаче квантовых бит (*QBER*) на боковых частотах;
- формирование случайных битовых последовательностей на основе параметров квантового канала для кодирования и декодирования информации при обмене данными между верификационными узлами.

Для реализации инфраструктуры квантового защищенного распределенного реестра следует обеспечить безопасную передачу данных по каналу между центрами обработки данных (ЦОДами) – «точка-точка», между серверами внутри ЦОДа, между серверами в ЦОДах, по каналу для оконечных устройств, а также накопление ключей в ЦОДе и на стороне клиента, выборку ключей оконечным устройством пользователя и реализацию протоколов взаимодействия публичной и приватной сети.

Базовая схема использования квантовых ключей сервисами распределенного реестра в рамках системы «квантовых коммуникаций» представлена на рис. 4.

Работы по созданию описываемого решения осуществляются в рамках Центра компетенций технологии распределенных реестров СПбГУ, консорциума при Центре, а также партнерами в лице регионального инжинирингового центра Сейфнет Технопарка Санкт-Петербург, компании «Финдинамика». Ведется разработка прототипа решения, предназначенного для организации платежных транзакций в режиме реального времени и предоставления безопасного канала передачи данных между верификационнными нодами, которое включает набор верификационных нод распределенного реестра *Stellar*, устройства рассылки квантового ключа, набор серверов, поддерживающих протоколы управления пользователями[1] и комплайнс[2]. Архитектура реализованного прототипа показана на рис. 5.

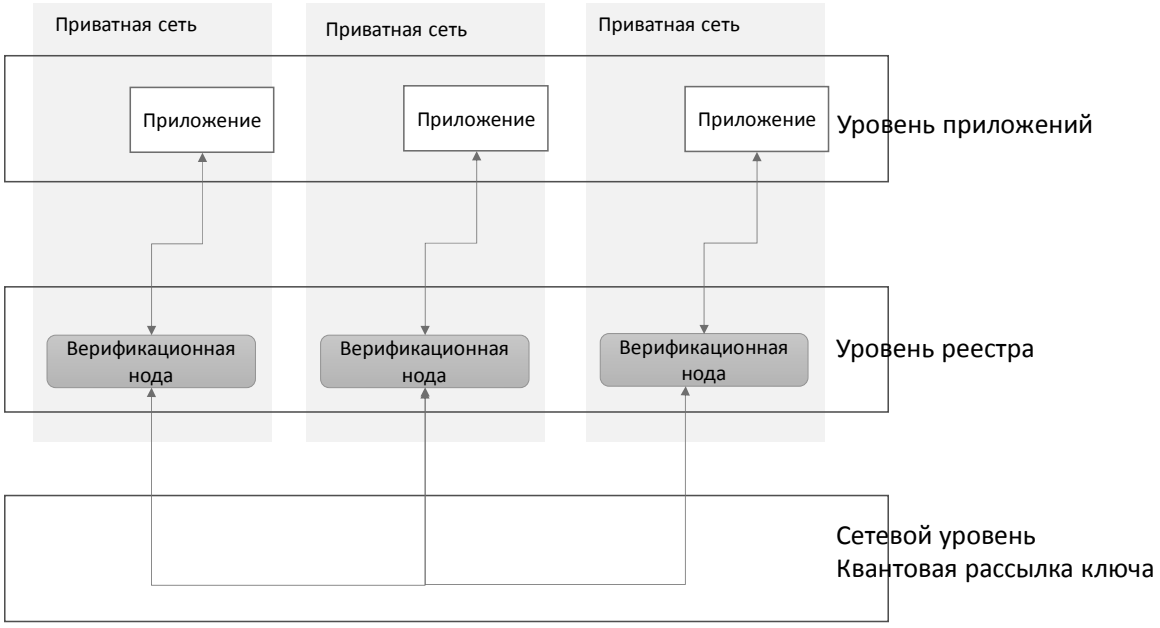

Рис. 3. Уровни реализации распределенных реестров с использованием квантовых коммуникаций

[1] Позволяет получить дополнительную информацию о данном пользователе и провести *KYC* (англ. «know your customer») – процедуру по идентификации, верификации и аутентификации пользователя, которая обеспечивает прозрачность совершаемых им действий и транзакций.

[2] Позволяет отслеживать и одобрять каждую транзакцию, связанную с выпущенным активом, а также применять набор ограничений. Используется для поддержки действий по борьбе с коррупцией и отмыванием средств, а также проверки агентов на право доступа и другие права. Это требуется, чтобы регулирующие учреждения или органы имели информацию о назначении транзакций и участниках деятельности в рамках прямого обмена данными, активами, финансами и др.

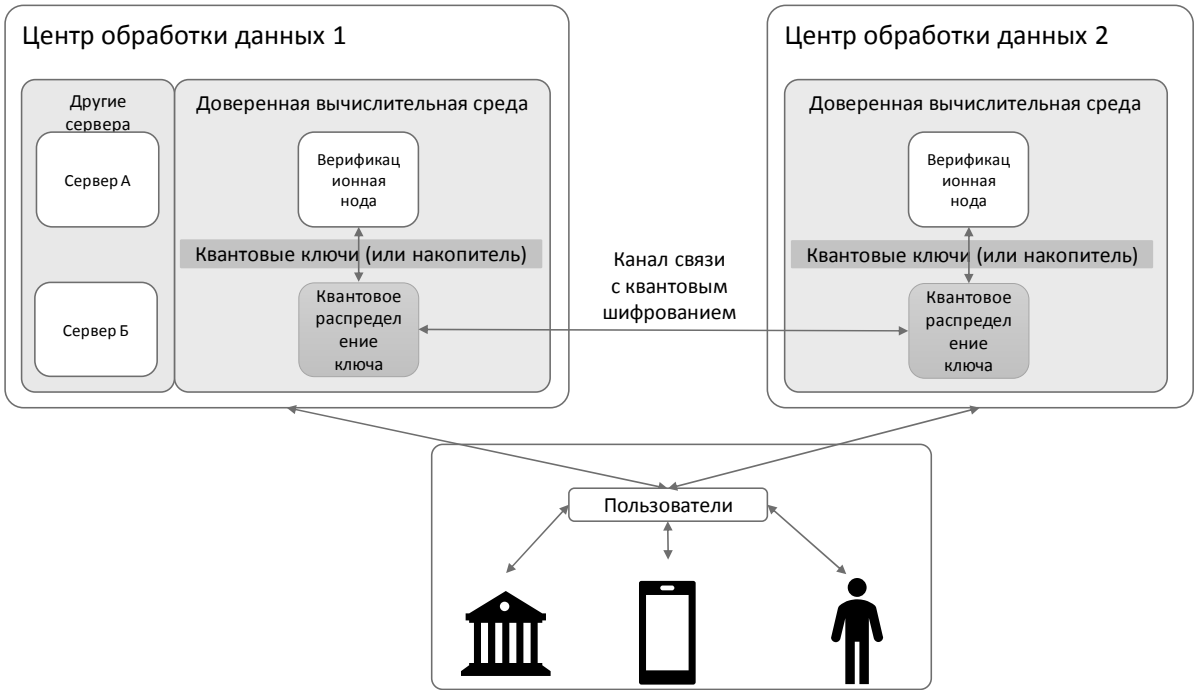

Рис. 4. Схема использования квантовых ключей сервисами распределенного реестра

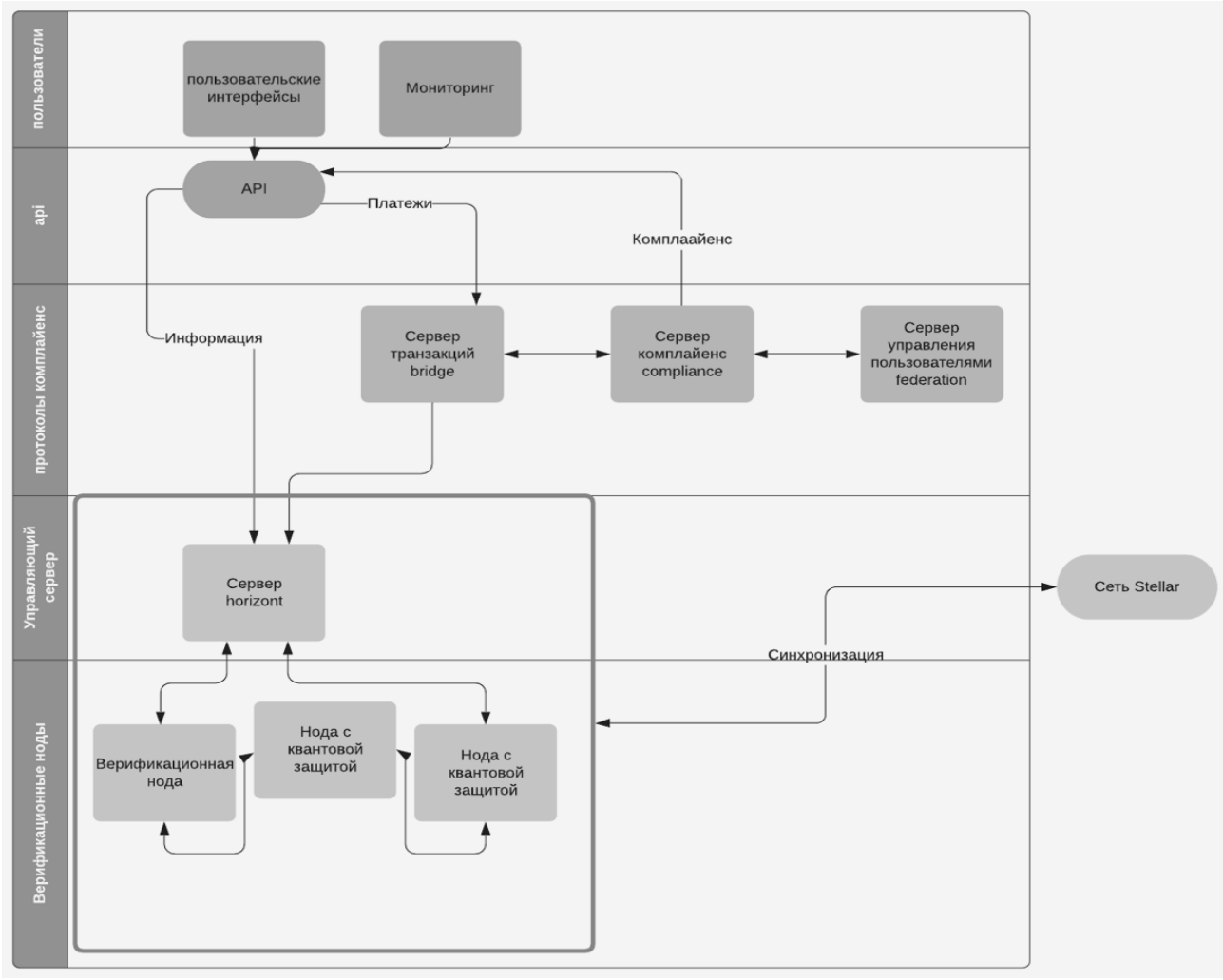

Рис. 5. Общая архитектура реализованного прототипа

ЗАКЛЮЧЕНИЕ

Сформулированные в настоящей статье методология, концепция и архитектура развертывания приватных распределенных реестров, защищенных квантовыми коммуникациями, могут быть использованы для прикладных решений в области финансов, логистики, хранения цифровых активов в корпорациях и государственных организациях, а также при интеграции научно-информационных процессов в информационных системах, а базовые требования к большим транзакционным системам и средствам квантовой криптографии (квантовым шифраторам) – для формулирования уточненных требований уполномоченными государственными организациями.

СПИСОК ЛИТЕРАТУРЫ

1. Permissioned Distributed Ledger (PDL). Applicability and compliance to data processing requirements // ETSI Group reports. – 2019. – URL: https://www.etsi.org
2. Касперская Н.И., Кузьменко В.В., Хайретдинов Р.Н., Щербаков А.Ю. О подходах к созданию универсального доверенного распределенного реестра, обеспечивающего неразглашение данных о системе // Безопасность информационных технологий. – 2019. – Т. 26, № 2. – С. 95-108.
3. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра». – 2019. – URL: https://digital.gov.ru/uploaded/ files/07102019srr.pdf
4. Kiktenko E.O., Pozhar N.O., Anufriev M.N., Trushechkin A.S., Yunusov R.R., Kurochkin Y.V., Lvovsky A.I., Fedorov A.K. Quantum-secured blockchain // IOP Publishing: Hybrid Open Access. – 2018. – № 3. – P. 17-29.
5. Sun X., Wang Q., Kulicki P., Sopek M. A simple voting protocol on quantum blockchain // International Journal of Theoretical Physics. – 2019. – № 58. – P. 275-281.
6. Jogenfors J. Quantum bitcoin: An anonymous and distributed currency secured by the No-Cloning Theorem of quantum mechanics // Information Coding Group, Department of Electrical Engineering, Linköping University, Sweden. – 2016. – URL: https://arxiv.org/pdf/1604.01383.pdf.
7. Bennett C., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. – Bangalore: Institute of Electrical and Electronics Engineers, 1984. – P. 175-179.

Материал поступил в редакцию 25.10.19.

Сведения об авторах

ГРИНЯЕВ Сергей Николаевич – доктор технических наук, декан Факультета комплексной безопасности ТЭК РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва
e-mail: gsn@gubkin.pro

ПРАВИКОВ Дмитрий Игоревич – кандидат технических наук, старший научный сотрудник, руководитель Научно-образовательного центра новых информационно-аналитических технологий РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва.
e-mail: d_pravikov@mail.ru

РАЗГУЛЯЕВ Кирилл Александрович – разработчик Центра компетенций технологии распределенных реестров СПбГУ, системный аналитик ООО «Квант-телеком», Санкт-Петербург
e-mail: kirill.razgulyaev@gmail.com

РЯЗАНОВА Алина Александровна – зам. начальника по международной деятельности Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН, Москва.
e-mail: a.ryazanova@c3da.org

ХАН Дмитрий Вячеславович – главный разработчик Центра компетенций технологии распределенных реестров СПбГУ, учредитель ООО «Финдинамика», Санкт-Петербург.
e-mail: dkhan@findinamika.com

ЩЕРБАКОВ Андрей Юрьевич – доктор технических наук, профессор, главный научный сотрудник РАН, начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН, Москва.
e-mail: x509@ras.ru