К РАЗВИТИЮ МЕТОДОЛОГИИ СОЗДАНИЯ ДОВЕРЕННЫХ И ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Гостев Сергей Сергеевич
К.т.н., заместитель директора по науке, Концерн «Гранит» (Москва)
Гриняев Сергей Николаевич
Д.т.н., с.н.с., РГУ нефти и газа (НИУ) имени И. М. Губкина
Щербаков Андрей Юрьевич
Д.т.н., профессор, РГУ нефти и газа (НИУ) имени И. М. Губкина
Правиков Дмитрий Игоревич
К.т.н., РГУ нефти и газа (НИУ) им. И. М. Губкина
dip@gubkin.pro

Аннотация. В статье проведен анализ основных свойств, рассматриваемых применительно к блокчейн-технологиям. Показано, что в общем случае свойства «равноправия», «независимости» и «децентрализованности» не обеспечиваются существующими криптовалютными системами. На основании анализа сформулированы требования к перспективным системам, построенным на основании технологии распределенного реестра. Приведено описание разработанного протокола функционирования защищенного доверенного распределенного реестра, а также структур данных, используемых в данном распределенном реестре.

Ключевые слова: блокчейн технологии, свойства безопасности, требования к безопасности, защищенный доверенный распределенный реестр.

ABOUT METHODOLOGY DEVELOPMENT FOR CREATING TRUSTED AND SECURE INFORMATION SYSTEMS BASED ON THE DISTRIBUTED REGISTRY TECHNOLOGY

S. Gostev
S. Grinyaev
A. Scherbakov
D. Pravikov

Summary. The article analyzes the main properties of the blockchain technologies. It is shown that in general, the properties of "equality", "independence" and "decentralization" are not provided by existing cryptocurrency systems. On the basis of the analysis, the authors formulated requirements to the systems based on the technology of the distributed register. The authors defined the description of the developed protocol of the protected trusted distributed registry, as well as data structures used in this distributed registry.

Keywords: blockchain technology, security properties, security requirements, protected trusted distributed registry.

Введение

В последние годы в области построения доверенных и защищенных информационных систем большой интерес вызывает использование технологии распределенных реестров (блокчейн) в целях решения широкого круга задач, начиная от организации децентрализованных платежных систем и закачивая задачами интеграции цифровых платформ и объединения разнородных баз данных [1].

Необходимо заметить, что методология создания доверенных и защищенных информационных систем на основе распределенных реестров испытывает определенные теоретические трудности. Это связано с тем, что технология блокчейн развивалась от практических потребностей путем «проб и ошибок».

В настоящее время существует ряд действующих проектов, в первую очередь блокчейн криптовалюты Bitcoin, блокчейн Etherium, который исправил множество недостатков проекта Bitcoin [2], попытки синтезировать "конструкторы» распределенных реестров — проекты типа Hyperledger Fabric.

У всех этих проектов имеется ряд принципиальных недостатков, вызванных «болезнями роста» — когда информационная технология растет и развивается от практики. Аналогом процесса является развитие теории вероятностей от практических навыков по анализу статистики событий до непротиворечивой аксиоматики А. Н. Колмогорова в области вероятностной меры. Несмотря на то, что в области информатики никогда невозможно будет отказаться от движения «от практики», теоретическое осмысление вопроса тем не менее настоятельно необходимо.

Теоретические проблемы существующих распределенных реестров

Первичным теоретическим заблуждением проектов распределенных реестров является тезис о том, что информационная система на основе распределенного реестра может быть первично построена «равноправно», «независимо» и «децентрализовано».

Под «равноправностью» понимается, как правило, равноправие участников, некоторая их одинаковость с точки зрения собственных возможностей, изначального недоверия друг к другу, также с точки зрения модели угроз той системы, в которую интегрирована технология распределенного реестра.

Независимость системы декларируется с точки зрения невлияния некоторых «регуляторов» на нее и децентрализованность с точки зрения распределенности ресурсов в первую очередь, их доступности.

Однако, очевидно, что полная равноправность невозможна в первую очередь из-за того, что у практической реализации по меньшей мере части компонентов системы имеется «автор», который априорно имеет больше знаний о систем и возможности по ее доработке и изменению [3].

Далее, у системы имеет условный «оператор», а практически — владелец, который разворачивает и поддерживает технические средства информационной системы, в которую интегрирована технология распределенного реестра. Владелец или автор практически единолично вносят изменения-форки (fork), которые могут полностью изменить систему, а с другой стороны — держат ее под контролем владельца. К этой же области относится сопровождение программного обеспечения распределенного реестра и исправление ошибок в нем.

Кроме того, за скобки выносится телекоммуникационноя часть системы — та, которая доносит информацию клиентов (пользователей) до оператора (операторов) распределенных реестров. В современном мире именно телекоммуникации являются инструментом контроля и ограничения децентрализованности и вполне понятно — чтобы построить полностью независимую информационно-телекоммункационную систему — это полностью продублировать каналы связи, обеспечивающие передачу информации в ней, что является возможным только для проектов глобального уровня.

Таким образом, «равноправие», «независимость» и «децентрализованость» является мифами, которые неосознанно или сознательно распространяются блокчейн-сообществом [4].

Надо обратить внимание и на то, что в основу «доверия» к системам распределенных реестров положены криптографические задачи, например, задача построении коллизий хеш-функции или ассиметричные криптографические алгоритмы.

Задача доверенного обмена открытыми ключами для обеспечения корректного их использования, например, для обеспечения переводов с одного кошелька на другой решается только при помощи сертификатов — подписания открытого ключа в доверенном центре. А наличие доверенного центра перечеркивает децентрализованность полностью в первую очередь с точки зрения доступности, поскольку удостоверяющий центр может полностью регулировать выдачу сертификатов открытых ключей.

С другой стороны, «багаж» ассиметричной криптографии не позволяет выстроить быстродействующие и легко управляемые системы распределенных реестров в первую очередь из-за низкой скорости ассиметричных криптографических алгоритмов. Кроме того, в умах неспециалистов ассиметричная криптография является панацеей для решения всех задач, что создает исходно ложные парадигмы проектирования защищенных систем.

Другой важной проблемой является тезис о том, что незамкнутая система не может быть защищенной с точки зрения формальной доказательности этого факта [5]. Исходя из этого, пользователи системы должны быть поименованы, а с другой — являться анонимными относительно друг друга. Кроме того, в системе в обязательном порядке должны присутствовать механизмы (с точки зрения системно-аналитических моделей компьютерных систем — субьекты) разграничения доступа, а в общем случае — реализации произвольно заданной политики безопасности.

В это связи уместно привести пример неработоспособности семейства ассиметричных криптографических алгоритмов для решения задач анонимизации. Один из известных принципов построения анонимного имени для субъекта или объекта распределенного реестра — вычисление хеш-функции от открытых данных (имени или паспортных данных пользователя). Легко видеть, что перебор исходной информации (например, по базам данных паспортов) позволяет с невысокой трудоемкостью найти реальное имя по хеш-значению.

Основные требования к системе, включающей распределенный реестр

Исходя из изложенного, система распределенных реестров должна в обязательном порядке обеспечивать:

- формирование приватного элемента для пользователя с гарантированными вероятностными свойствами, т.е. пользователь должен иметь приватный идентификатор или ключ, никому не известный кроме него, выработанный при помощи датчика случайных чисел с гарантированными статистическими свойствами;
- формирование сетевого имени (идентификатора, которым пользователь представляется в системе) на основе указанного выше приватного элемента, исключающего возможность выявления связей между сетевым именем и множеством открытых данных о физическом лице или организации;
- безопасное хранение приватного элемента у пользователя для обеспечения защищенности от несанкционированного доступа к нему;
- наличие «точки входа» для пользователей — оператора распределенного реестра, который на основе заданных регламентов обеспечивает обработку информации пользователей
- авторизацию пользователя для оператора при помощи криптографических процедур, использующих приватный элемент пользователя;
- безопасный транспорт (как минимум с сохранение неизменности информации, получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;
- контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр;
- формирование подтверждений у оператора распределенного реестра факте помещения информации в распределенный реестр (например, путем выдачи заверенных оператором квитанций пользователям);
- наличие механизма формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса);
- реализацию у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра) в распределенном реестре.

Только реализация данных свойств позволит сделать систему, включающую распределенный реестр, защищенной.

Необходимо также уточнить модель нарушителя, которая неявно используется при формировании указанных свойств. В данном случае речь идет о модели внешнего нарушителя (модель Н2) — нарушитель, который может читать и изменять информацию в каналах связи (в телекоммуникационной компоненте информационно-телекоммуникационной системы). Полагаем, что владелец системы (оператор распределенного реестра) является доверенным лицом или организацией, заинтересованным в корректной и безопасной работе всей системы. Как мы показали выше, это предположение является базовым для построения системы.

Краткое описание протокола защищенного доверенного распределенного реестра

Введем следующие обозначения

Xi — пользователь распределенного реестра,

Ai — цифровая информация, описывающая пользователя РР,

Kpi — персональный ключ (персональная информация) пользователя РР,

Ksi — сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с оператором РР,

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,

INFOij — информация i-го пользователя, сформированная на рабочем месте пользователя и направляемая для хранения и обработки в РР, имеющая условный номер j,

Kvij — квитанция, сообщающая о результате обработки j-го информационного блока для i-го пользователя

Vm — запрос на извлечение информации из РР,

Ko — ключ оператора, служащий для заверения цепочки данных в РР,

I=Im(x, k) — функция вычисления имитовставки от информации x на ключе k.

Легко видеть, что функция вычисления имитовставки обладает возможностью как авторизации пользователя, так и контроля целостности передаваемой и хранимой информации.

Для обеспечения информационного взаимодействия пользователей и оператора необходимо обеспечить функционирование сервера оператора (сервер приема-выдачи информации распределенного реестра), имеющего следующие области для передачи данных:

- область приема данных сервера, в которую пользователи передают данные для помещения в рас-

пределенных реестр и запросы для выгрузки данных из распределенного реестра,
- область данных, в которую перемещаются объекты ошибочного формата (например, не имеющие кода аутентификации пользователя),
- область данных, содержащая квитанции о помещении информации в распределенный реестр,
- область данных выгрузки данных по запросам пользователей.

Полагаем, что пользователь системы имеет персональный вычислитель (ноутбук, смартфон или выделенный криптокомпьютер), подключенный при помощи каналов связи (телекоммуникационной среды) к серверу приема-выдачи информации РР.

Для регистрации в системе пользователь Xi при помощи датчика случайных чисел с гарантированными статистическим свойствами создает ключи Kpi — персональный ключ (персональная информация) пользователя РР и Ksi — сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с оператором РР и формирует контейнеры Ci1=E(Kpi, Pi1) и Ci2=(Ksi, Pi2), где

Y=E(x, k) — алгоритм зашифрования данных x на ключе k,

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.

Приведем пример формирования данных при помощи алгоритма шифрования «Кузнечик».

Например, при задании Ai=Alisa Valerevna Melnikova получим Si=b944928487491bde8f5bba9a64b33f4d.

В данном случае сетевое имя имеет длину 32 шестнадцатеричных знака (16 байт), что соответствует длине блока открытого текста алгоритма «Кузнечик».

После формирования сетевого имени и контейнера Ci2 эти данные синхронизируются между пользователем и оператором РР.

Это означает, что контейнер Ci2 может быть сформирован и оператором РР и передан пользователю при его регистрации, возможно выполненой в рамках национального законодательства, при этом пароль для раскрытия контейнера передается лично пользователю при физическом посещении представителя оператора и авторизации пользователя с предъявлением соответствующих документов. Пароль может быть передан и по альтернативным каналам связи, например, смс при регистрации пользователя с учетом номера его мобильного устройства.

Для подготовки данных для отправки их в РР пользователь может использовать конструктор атомов РР [6], позволяющий создать зашифрованный, подписанный (снабженный имитовствкой) или открытый блок данный. При этом зашифрованный или подписанный блок формируется на персональном ключе пользователя и доступен только самому пользователю, что позволяет обеспечить дополнительно невозможность ознакомления оператора РР с информацией пользователя.

Далее пользователь формирует запрос Zij = Im([INFOij, Si, Tk], Ksi) и направляет его на сервер приема-выдачи данных. Сервер приема данных проверяет имитовставку пользователя по запросом, тем самым проводя как аутентификацию отправителя, так и проверку целостности данных.

При положительном результате проверки информация передается серверу записи в РР, который передает информацию для обработки в сервер оператора РР, хранящий ключ оператора Ko. Данный сервер записывает в систему хранения данных (СХД) блок Zij (цифровой контейнер). При положительном результате записи в СХД для пользователя формируется квитанция Kvij, содержащая номер блока, куда помещена информация пользователя, номер транзакции, время помещения в РР и подпись оператора под данными пользователя.

Приведем пример такой квитанции
DNum:3
TNum: c09f9ae8a8921d91b41691c061cd6b61
Sign: ad3fed45df10834c
File: a01
NetName: b944928487491bde8f5bba9a64b33f4d
AddTime:01:37:11~<13.01.2018

В данном случае квитанция удостоверяет для пользователя с сетевым именем NetName помещение файла a01 в звено распределенного реестра с номером 3 при этом имтовтавка в СХД, выработанная оператором РР, принимает значение Sign, а номер транзакции составляет значение Tnum, время формирования записи (звена РР) AddTime.

Для извлечения данных или для изменения прав доступа к записи (по умолчанию доступ к записи предоставляется пользователю, который ее выполнил) пользователь использует специальные запросы.

Приведем пример таких запросов.
access
dnum:1
+: b944928487491bde8f5bba9a64b33f4d

запрос означает, что доступ к записи с номером 1 дополнительно предоставлен (+) пользователю с сетевым именем «Alisa».

или
load
dnum:1

запрос означает, что из PP будет выгружена запись с номером 1.

При запросе на извлечение данных или изменение прав доступа запрос Vm снабжается имитовставкой пользователя и передается в сервер оператора PP, который обращается к СХД в режиме чтения и по номеру записи, либо другой информации поиска (сетевом имени, дате) извлекает информацию и передает серверу приема-выдачи данных, либо формирует квитанцию о неуспешном поиске и невозможности извлечении данных.

Структура системы хранения данных

В целях обеспечения основных свойств распределенного реестра [7], следующих из названия технологии blockchein — «цепь» или «цепочка» блоков, блокчейн в первую очередь должен обеспечивать свойства цепи — неразрывность и прочность, которые являются парафразом свойства целостности.

Неразрывность определяется как свойство следования блоков (звеньев цепи) одного за другим, в заданной в процессе создания блокчейна последовательности, а прочность — невозможность замены или удаления звена из цепочки.

Если рассматривать блокчейн как системную целостность, то он должен состоять из отдельных элементов — звеньев, каждое из которых в свою очередь делится на элементарные компоненты (назовем их атомами блокчейна). В данном случае для СХД формируется последовательность записей в нотации языка С:

```
l1=fwrite(dnum,1, 16, fl);
l2=fwrite(ntran,1, 16, fl);
l3=fwrite(tdt,1, 8, fl);
l4=fwrite(buf,1, buflen, fl);
l6=fwrite(imi,1, 8, fl);
l5=fwrite(&buflen,4, 1, fl);
l7=fwrite(dnum1,1, 16, fl);
```

dmum — уже упомянутый нами выше номер записи (номер звена),

ntran — номер транзакции,
tdt — время и дата формирования звена,
buf — данные пользователя, записываемые в СХД длиной buflen,
dnum1=dnum+1, обеспечивающих неразрывность перехода к следующему звену,
imi=Im(dnum|ntran|tdt|buf, Ko) — имитовставка от конкатенации данных.

Кроме того, старшая область поля dnum заполняется значением imi от предыдущего звена, что позволяет добиться того же свойства, как и в блокчейне Bitcoin — зависимости хеш-значений (в данном случае вычисленных при помощи приватного элемента Ko) от всей последовательности предыдущих данных.

Приведем пример последовательного формирования описанных полей:

DNum:13
Полное значение: 6c006896973848d7000000000000000d
TNum:44f98f920985679580a8b7bee17de548
Sign: dabfd993c75f3366
File: a01
AddTime:01:10:48~<20.01.2018

и
DNum:14
Полное значение: dabfd993c75f3366000000000000000e
TNum: ec2120a826f51e32255daa1f6002f5a2
Sign: baa49fb79db3805b
File: a01
AddTime:01:11:09~<20.01.2018

Как легко видеть, поле imi предыдущего блока заполняет старшие разряды (8 байт) поля dnum текущего блока (предыдущий блок с номерами 13, текущий с номером 14), что позволяет обеспечить зависимость от всей предыдущей информации, помещенной в распределенный реестр.

Выводы

Сформулированная концепция создания доверенного защищенного распределенного реестра может являться методологической основой для формулирования ведомственных или национальных регулирующих требований в области цифровой экономики [8], а также послужить технической основой для разработки конкретных проектов в области защищенных систем, использующих распределенные реестры в сфере государственного управления, финансов и учетно-сервисных систем.

ЛИТЕРАТУРА

1. A. V. Zaitsev, S. S. Gostev, P. A. Cherkashin, Shcherbakov A. Yu. (2017) Regarding the Technology of Distributed Storage of Confidential Information in Centers of General-Purpose Data Processing, Automatic Documentation and Mathematical Linguistics, Vol. 51, No. 3, 117–119. ISSN0005–1055
2. Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org.
3. Биктимиров М. Р., Щербаков А. Ю. Проблемы синтеза доверенных систем // Труды ИСА РАН.— 2012.— Том 53.— С. 264–271.
4. Централизованные криптовалюты (2017). geektimes.ru/company/waves/blog/289379/
5. Pravikov D. I., Shcherbakov A. Yu. (2018) Changing the paradigm of information security, Highly available systems, 2, 35–39. ISSN2072–9472
6. Shcherbakov, A. Yu. (2018) About development tools for creation corporative distributed ledger (blockchain) Automatic Documentation and Mathematical Linguistics, 4, 30–34. ISSN0548–0027.
7. Биктимиров М. Р., Домашев А. В., Черкашин П. А., Щербаков А. Ю. Блокчейн: универсальная структура и требования // Научно-техническая информация. Сер. 2.— 2017.— № 11.— С. 1–4.
8. А. Ю. Щербаков. Синтез универсальной архитектуры и протокола криптовалюты в рамках национального проекта/ Системы высокой доступности, № 3, т. 13, 2017 — с. 15–18.