Секция «Компьютерное право и информационная безопасность»

Применение технологии распределённых реестров в целях обеспечения информационной безопасности

Научный руководитель – Крылов Григорий Олегович

Тараненко Дмитрий Александрович
Аспирант
Финансовый университет, Факультет анализа рисков и экономической безопасности, Информационная безопасность, Москва, Россия
E-mail: ostrvi@mail.ru

Введение

Технология распределенных реестров[1] представляет новые возможности для повышения защищенности информационных массивов, обрабатываемых в базах данных и информационных системах с низким уровнем доверия участников[2], посредством своей ключевой особенности - отсутствия единого центра управления, другими словами - децентрализации. Основным же недостатком централизованных информационных ресурсов можно назвать уязвимость узлов, выполняющих роль ядра системы, при успешной атаке на них скомпрометированной окажется вся информационная система целиком, что может привести к огромному ущербу, как к материальному, так и репутационному. Блокчейн позволяет избежать вышеуказанных рисков, поскольку каждый узел сети составляет и записывает обновления реестра независимо от остальных нод.

В отличие от распределенных баз данных каждый узел блокчейна хранит всю историю изменений реестра и валидирует добавление любых изменений в систему распределенного реестра с помощью алгоритма консенсуса, который математически гарантирует невозможность подделки данных при установленной доле доверенных узлов. Однако ни один узел не способен изменить записи в реестре таким образом, сто другие ноды не узнают об этом. Исходя из вышеизложенного, данные хранящиеся в блокчейне, становятся доверенными, а вносимые в них изменения - прозрачными.

1. Субтехнологии блокчейна

В соответствии с дорожной картой развития «сквозной» цифровой технологии «системы распределенного реестра» [n1] определены субтехнологии систем распределенного реестра:

a. Субехнология организации и синхронизации данных - совокупность методов и инструментов, направленных на определение, организацию и усовершенствование взаимосвязей между частями и элементами распределенных баз данных, а также на обеспечение их согласованности и приведение к соответствию;

b. Субехнология обеспечения целостности и непротиворечивости данных (консенсус) - совокупность методов и инструментов, направленных на приведение в соответствие имеющихся данных в децентрализованной сети к единой внутренней логике и структуре по заранее определенным правилам, а также обеспечение синхронизации и согласования данных между участниками децентрализованной сети;

c. Субехнология создания и исполнения децентрализованных приложений и смарт-контрактов - совокупность методов и инструментов, направленных на создание приложений, обеспечивающих взаимодействие неограниченного количества узлов распределенного блокчейна, и на разработку, поддержание и выполнение компьютерных алгоритмов, предназначенных для автоматизации процессов исполнения смарт-контрактов. Децентрализованные приложения обладают прозрачной и открытой логикой, обеспечивающей гарантированное исполнение заданных функций в рамках блокчейна.

В контексте рассмотрения возможностей применения технологии распределенных реестров в целях обеспечения информационной безопасности государственных информационных систем можно следующим образом определить для чего необходимо использовать рассмотренные выше субтехнологии.

Субехнология обеспечения целостности и непротиворечивости данных (консенсус) отвечают за пропускную способность блокчейна, обеспечение неизменности данных, возможность обеспечения полной конфиденциальности транзакций, поддержку криптографии по ГОСТ[3], защищенность от киберугроз и захвата вычислительных мощностей сети.

Субтехнология создания и исполнения децентрализованных приложений и смарт-контрактов отвечает за цифровизацию процессов, а также определяет возможности гибкой настройки прав и ролей различных пользователей.

Субехнология организации и синхронизации данных отвечает за время синхронизации и развертывание полных узлов, требования к вычислительным мощностям для развертывания полных нод, а также их количество, допустимое к функционированию в рамках системы на основе блокчейна.

Кроме того, для каждой субтехнологии блокчейна можно определить ключевые технические характеристики, на основании которых легче оценить эффективность решений на базе технологии распределенного реестра и их применимость в конкретных бизнес-процессах.

Для субехнологии обеспечения целостности и непротиворечивости данных (консенсус):

- пропускная способность, количество транзакций в секунду;
- безопасность, доля вычислительных мощностей сети или узлов, которые необходимо скомпрометировать, чтобы захватить сеть;
- децентрализация или количество узлов, участвующих в алгоритме консенсуса.

Для субехнологии создания и исполнения децентрализованных приложений и смарт-контрактов:

- среднее время интеграции блокчейна в бизнес-процессы;
- среднее время аудита смарт-контрактов.

Для субехнологии организации и синхронизации данных:

- размер блока блокчейна;
- среднее время валидации блоков;
- возможность использования ГОСТ криптографии.

Исходя из рассмотренных выше особенностей технологии распределенного реестра можно сделать вывод, что применение блокчейна для обеспечения информационной безопасности ГИС[4], должно повысить их надежность и доступность, кроме того, увеличить защищенность ГИС от кибератак.

2. Блокчейн, как СКЗИ[5] для защиты информации в ГИС

Федеральное казначейство[6] можно рассматривать, как транзакционную, учетную, контрольную, информационную систему в области финансовой деятельности публично-правовых образований. Казначейство России для обеспечения своей деятельности в соответствии с законодательством Российской Федерации в части правоприменительной функции по обеспечению исполнения федерального бюджета, кассовому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, предварительному и текущему контролю за ведением операций со средствами федерального бюджета главными распорядителями, распорядителями и получателями средств федерального бюджета использует ГИС. Федеральное казначейство является оператором большого количества ГИС [n2], таких как:

- Государственная информационная система о государственных и муниципальных платежах;

- Государственная автоматизированная информационная система «Управление»;
- Официальный сайт Единой информационной системы в сфере закупок;
- Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет»
- Государственная информационная система «Независимый регистратор»;
- Официальный сайт для размещения информации о государственных (муниципальных) учреждениях.

Федеральное казначейство в целях обеспечения информационной безопасности государственных информационных систем, оператором которых является, в ходе их развития и эксплуатации руководствуется требованиями, определенными приказом ФСТЭК России от 11 февраля 2013 г. № 17. Ниже рассмотрим возможности применения технологии распределенных реестров для обеспечения соответствия требованиям информационной безопасности ГИС.

Поскольку в блокчейне применяется шифрование, механизм создания ключевых элементов и сами ключевые элементы, а также хеширование, мы действительно можем сказать, что технология распределенных реестров относится к СКЗИ [n3].

Если рассматривать технологию распределенных реестров как средство защиты информации, не составляющей государственную тайну, и применяемое в ГИС, то необходимо определить, какие меры защиты он реализует в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 [n4].

1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ), а именно ИАФ.1-ИАФ.6 [n4].
2. Управление доступом субъектов доступа к объектам доступа (УПД), а именно УПД.1-УПД.5, УПД.11-УПД.16 [n4].
3. Регистрация событий безопасности, а именно (РСБ), а именно РСБ.1-РСБ.7 [n4].
4. Обеспечение целостности информационной системы и информации (ОЦЛ) [n4].
5. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС), а именно ЗИС.6, ЗИС.11-ЗИС.13 [n4].

В зависимости от того, в каких информационных системах планируется применение технологии распределенных реестров, к ней предъявляются различные требования, некоторые из которых на данный момент не выполняются.

Так, например, для внедрения в системы защиты персональных данных к СКЗИ необходимо применять такие обязательные параметры, как:

- СКЗИ должны иметь заключение об оценке влияния на среду функционирования;
- для защиты персональных данных необходимо использовать СКЗИ, имеющие действующий сертификат соответствия ФСБ[7] России.

Для получения сертификата соответствия ФСБ России необходимо соблюсти одно важное условие: все алгоритмы хэширования и шифрования должны соответствовать российским ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 [n5]. Следовательно, для внедрения технологии распределенных реестров с целью обеспечения информационной безопасности в информационных системах персональных данных и ГИС, необходима разработка блокчейна, основанного на отечественных алгоритмах шифрования и хеширования.

Вывод

Технология распределенного реестра обеспечивает фундаментально иной подход к информационной безопасности, ключевым фактором которого является децентрализация. Когда контроль доступа, сетевой трафик и даже сами данные больше не хранятся в одном месте, киберпреступникам становится гораздо сложнее их использовать. Новые угро-

зы будут возникать постоянно и внедрение блокчейна в систему защиты информации ГИС может послужить повышению их надежности и доступности.

[1] Далее по тексту термины технология распределенных реестров и блокчейн будут применяться взаимозаменяемо

[2] Далее по тексту термины участник, узел и нода будут применяться взаимозаменяемо

[3] Государственный стандарт

[4] Государственные информационные системы

[5] Средство криптографической защиты информации

[6] Далее по тексту термины Федеральное казначейство и Казначейство России будут применяться взаимозаменяемо

[7] Федеральная служба безопасности

Источники и литература

1) Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» – [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/6670/ (дата обращения: 23.11.2020).

2) Официальный сайт Казначейства России – [Электронный ресурс]. URL: https://roskazna.gov.ru/gis/ (дата обращения: 23.11.2020).

3) Применение технологии блокчейн в информационных системах. Часть 1. Защищенный электронный документооборот / Г.П. Акимова [и др.] // Системы высокой доступности. - 2018. - Т. 14. - № 1. - С. 3-7 – [Элек-тронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=32795839 (дата обращения: 23.11.2020).

4) Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 13 фев. 2013 г. № 17 – [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 23.11.2020).

5) Применение технологии блокчейн в информационных системах. Часть 2. Подтверждение авторства и обеспечение целостности / А.Ю. Даниленко [и др.] // Системы высокой доступности. - 2018. - Т. 14. - № 1. - С. 9-11. – [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=32795840 (дата обращения: 23.11.2020).