DOI: 10.25728/mlsd.2023.0691

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ РАСПРЕДЕЛЁННОГО РЕЕСТРА

Беспалова Н.В.
Финансовый университет при Правительстве Российской Федерации, Москва, Россия
NVBespalova@fa.ru

Аннотация. Предметом исследования является технология распределенного реестра, позволяющая обеспечить безопасность хранения и передачи данных в информационных системах. В ходе работы были сформулированы преимущества технологии и предложены алгоритмические решения для ее оптимального функционирования.

Ключевые слова: распределенные системы, технологии распределенного реестра, информационная безопасность, безопасность платежей.

Введение

Современных тенденций развития информационных технологий и рост объемов информации, циркулирующей в обществе, влечет за собой проблему обеспечения безопасности. Решение этой проблемы является комплексной задачей и основывается на использовании различных автоматизированных средств по отслеживанию состояния безопасности. Одним из наиболее перспективных направлений на сегодняшний день, является повышение безопасности транзакций и хранение данных в сфере банковских услуг. Рост цифровых способов оплаты увеличивает спрос на решения для обеспечения безопасности платежей, направленных на защиту конфиденциальности данных и транзакций клиента для предотвращения утечки и модификации данных. Данные тенденции способствуют росту затрат на рынке безопасности платежей и по прогнозам в 2024 году, в соответствии с графиком на рисунке 1, могут составить порядка 33 млрд. долларов для мирового сообщества. [1]

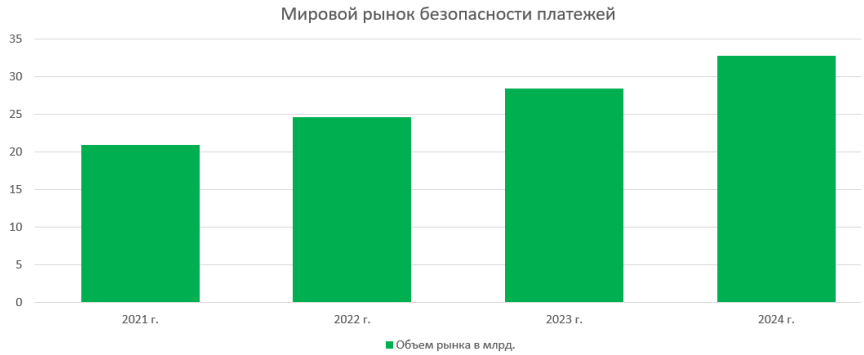

Рис. 1. Тенденции роста затрат в сфере безопасности платежей

Перспективную возможность развития финансовой системы в рамках повышения безопасности хранения и передачи данных представляют собой распределенные реестры.

1. Централизованные и распределенные программные системы

Программные системы по их внутренней архитектуре можно разделить на централизованные и распределенные. Распределенные системы представляют собой децентрализованные системы, состоящие из взаимосвязанных компонентов, каждый из которых связан со всеми прочими компонентами не напрямую, а через посредников. Распределённая и централизованная системы структурно антагонистичны, однако, несмотря на различия в подходах их организации, можно использовать их комбинации с целью получения преимуществ обоих архитектур. [2] Примером смешанной архитектуры являются централизованные пиринговые сети, в которых вычислительные станции пользователей при подключении к сети переходят в статус узла этой системы, получая равные права и обязанности с остальными узлами. Хотя ресурсы, предоставляемые участниками, могут иметь разную природу, все участники сети имеют доступ к одним и тем же функциям, предоставляемым системой, и несут одинаковую ответственность, при этом узлы применяются для создания установки информационных связей между компьютерами, а также для идентификации и координировании участников в сети, предоставляя информацию о узлах и сервисах. [3]

Данный подход, сохраняя преимущества распределенных систем (высокая вычислительная мощность, надежность, низкие расходы на поддержание инфраструктуры) нейтрализует основной их

недостаток, использование дополнительных вычислительных мощностей для внутрисистемной координации.

Использование пиринговых систем приводит к ускорению и упрощению процессов, связанных с использованием платёжных систем, систем оформления и отслеживания подлинности различных документов. [4]

Поскольку пиринговые системы напрямую связаны с использованием сетевых ресурсов, обеспечение безопасности и целостности данных является первостепенной задачей. Для систем хранения данных под целостностью понимается полнота, корректность и неизменность информации. Целостность в пиринговых сетях может обеспечиваться с использованием технологии распределённого реестра.

2. Технология распределённых реестров

Технология распределённых реестров – это способ организации обмена и хранения информации на базе криптотехнологий. Создание транзакций в распределенном реестре состоит из следующих этапов:

- узел предлагает обновление реестра, путём создания транзакции, подписанной закрытым ключом;
- участники сети проверяют корректность обновлений;
- если проверка прошла успешно, транзакция сохраняется и становится частью общего распределённого реестра; [5]
- данные, хранящиеся в общем реестре, не изменяются, а сохраняются отдельно с новым состоянием и ссылкой на предыдущее состояние, которая формируется непосредственно с использованием содержимого информации в виде хэш-суммы и позволяет осуществлять проверку целостности каждого хранимого состояния. Если данные несанкционированно изменяются, то сравнение хэш-сумм расчетной и сохраненной не совпадает, что сигнализирует об изменение в реестре и нарушении целостности. Проверка целостности основывается на необратимости вычисления хэш-сумм; [6]
- механизм идентификации и аутентификации пользователей сети осуществляется с использованием ассиметричной криптографии; [7]
- процесс согласования между участниками сети, не имеющие доверия к друг другу, называется консенсусом и основывается на хешировании данных. Механизмы консенсуса включают обязательную проверку валидности данных и обеспечивают отказоустойчивость системы. [8]

К преимуществам технологии распределённого реестра можно отнести децентрализацию, прозрачность, доверие, неизменяемость, доступность, безопасность транзакций и экономичность. По своей сути, распределенный реестр представляет базу данных, которая распределена между несколькими сетевыми узлами или вычислительными устройствами, на каждом из которых установлено соответствующее программное обеспечение. В отличие от централизованных реестров, наиболее часто используемых в банковской сфере, распределенные реестры позволяют осуществлять синхронную запись информации на всех компьютерах, подключенных к сети. [9]

Информационная безопасность систем основывается на характерных особенностях технологий распределённых реестров, децентрализованность позволяет бороться с DDoS-атаками, которые направлены на ограничение пропускной способности сетевого ресурса. При децентрализации, ресурсы распределены на различных узлах и для успешного проведения атаки необходимо вывести из строя абсолютно все составляющие. Фальсификация данных также затруднительна, поскольку сводится к модификации информации на всех узлах. Кроме того, благодаря хешированию, при добавлении или изменении строки данных, и новая, и предыдущая записи остаются доступными, что позволяет своевременно отследить попытки совершения атак на систему. [10]

Шифрованные соединения для защиты каналов опираются на инфраструктуру сертификации открытых ключей и удостоверяющие центры. При попытке установить безопасное соединение данные шифруются открытым ключом, расшифровка данных производится секретным ключом, безопасность и надежность пары открытый/ секретный ключ обеспечиваются удостоверяющим центром.[11]

В качестве практического решения проблемы обмена и хранения информации на основе технологии распределенного реестра можно предложить совокупность следующих криптографических решений: использование в качестве протокола установки защищенного канала протокола TLS (Transport Layer Security) версии 1.3 с поддержкой российских криптонаборов. Протокол TLS обеспечивает защиту в три этапа:

- Handshake (проверка установки соединения),
- False Start (процедура возобновления сессии),

- Chain of trust (проверки каждого компонента аппаратного и программного обеспечения от конечного объекта до корневого сертификата).

На каждом этапе работы протокола используются различные криптографические алгоритмы, которые задаются криптонабором – совокупностью алгоритмов, определенной в стандартизирующих документах и включающей, алгоритм выработки симметричного ключа, алгоритм шифрования и алгоритм выработки имитовставки (хэш-суммы). [12] Используемый криптонабор согласуется сторонами в самом начале установления защищенного канала. В качестве криптонаборов целесообразно использовать алгоритмы российского стандарта шифрования ГОСТ 34.12-2018.

При работе по протоколу TLS с ГОСТ клиент может доверять сертификату, если его корневым сертификатом является либо сертификат головного удостоверяющего центра Минцифры России (сертификат ГУЦ), либо сертификат любого доверенного удостоверяющего центра (сертификат TLS-CA). Сертификаты, имеющие в качестве корневого сертификат ГУЦ, выдаются только аккредитованными удостоверяющими центрами в соответствии с ФЗ №63 «Об электронной подписи».

Основным техническим решением для управления операциями информационной безопасности являются системы управления событиями и инцидентами информационной безопасности SIEM (security information and event management). [13] Эти системы предназначены для сбора и анализа информации от различных подсистем информационной безопасности, таких как контроль доступа, антивирусы, межсетевые экраны, анализ безопасности, контроль целостности, обнаружение и предотвращение вторжений и др. Собранные данные могут быть использованы для обнаружения отклонений в состоянии информационной безопасности в соответствии, при этом в системе управления событиями создается инцидент или уведомление, и соответствующие стороны оповещаются. [14]

Обнаружение отклонений позволяет не только своевременно и автоматически выявлять угрозы информационной безопасности, но и обнаруживать предпосылки к их возникновению, события и данные, хранящиеся в репозитории системы SIEM, могут быть использованы для расследования инцидентов информационной безопасности. Очевидно, что данные, хранящиеся в системах управления инцидентами и событиями безопасности, должны надежно храниться в течение длительного периода времени, и крайне важно обеспечить их целостность. Использование технологии распределенного реестра в реализации модулей хранения упрощает решение подобных задач благодаря своим особенностям: данные, хранящиеся в децентрализованном реестре, практически невозможно изменить или удалить, в то же время децентрализация обеспечивает отказоустойчивость, распределяя нагрузку путем направления доступа к различным узлам системы и защищая от попыток вывести из строя хранилище или модифицировать хранимые данные.

Наряду с инцидентами безопасности SIEM-система должна хранить инструкции обнаружения компьютерных атак, настройки и конфигурации защищаемых узлов для отслеживания изменений и т.д. Целостность этих данных имеет решающее значение для корректной работы систем управления событиями и инцидентами информационной безопасности. Для решения этой задачи также актуально использование распределенного реестра.

Анализ готовых решений применения технологии распределенного реестра, предоставляющие функциональность для хранения данных в распределённых системах представлен в таблице 1.

Таблица 1. Анализ готовых решений применения технологии распределенного реестра

	Fluree	**Enigma**	**Guardtime MIDA**
Обеспечение целостности данных	Использование технологий блокчейн	Использование технологий блокчейн	Сопоставление данных с криптографическим контейнером
Обеспечение доступа пользователей	Открытый/закрытый ключ	Цифровые подписи	Открытый/закрытый ключ
Обнаружение нарушений в режиме реального времени	-	-	+
Возможность интеграции с SIEM-системами	+	-	-/+
Характерные недостатки	Излишний функционал снижает производительность	Излишний функционал снижает производительность	Требует высокого уровня ресурсных затрат

Исследования показали, что лишь немногие продукты, основанные на технологии распределенных реестров, могут быть интегрированы с системами SIEM. Решения с такой функциональностью основаны на узких типах распределенных реестров, таких как блокчейн, или имеют избыточную функциональность, стоимость которой не оправдана практической необходимостью. Можно сделать вывод о целесообразности разработки собственных решений для хранения информации об инцидентах информационной безопасности, основывающиеся на технологии распределённого реестра.

3. Заключение

Подводя итоги, можно выделить такие преимущества технологии распределенного реестра, как целостность и прозрачность данных, устойчивость и экономичность системы, а также высокий уровень безопасности данных и транзакций, что приводит повышению эффективности финансовых операций. Использование технологии распределенного реестра может привести к устранению основных недостатков безопасности хранения и передачи данных на финансовом рынке.

Литература

1. *Усков В. С.* К вопросу о цифровизации российской экономики //Проблемы развития территории. – 2020. – №. 6 (110). – С. 157-175.
2. *Дюдикова Е. И., Куницына Н. Н.* Распределенные реестры в цифровой экономике: база данных, технология или протокол? //Инновации. – 2019. – №. 9 (251). – С. 98-106.
3. *Башир И.* Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. – Litres, 2022.
4. *Горбунова М. В. и др.* Обзор проблем внедрения технологии распределенного реестра //Информационно-управляющие системы. – 2020. – №. 2 (105). – С. 10-19.
5. *Ivanyuk V.* Forecasting of digital financial crimes in Russia based on machine learning methods //Journal of Computer Virology and Hacking Techniques. – 2023. – С. 1-14.
6. *Andriyanov N. et al.* Intelligent system for estimation of the spatial position of apples based on YOLOv3 and real sense depth camera D415 //Symmetry. – 2022. – Т. 14. – №. 1. – С. 148.
7. *Gataullin T. M., Gataullin S. T.* Endpoint Functions: Mathematical Apparatus and Economic Applications //Mathematical Notes. – 2022. – Т. 112. – №. 5-6. – С. 656-663.
8. *Zhang J. et al.* A Secure and Lightweight Multi-Party Private Intersection-Sum Scheme over a Symmetric Cryptosystem //Symmetry. – 2023. – Т. 15. – №. 2. – С. 319.
9. *Timofeev I. et al.* Mathematical Models and Methods for Research and Optimization of Protein Extraction Processes from Chickpea and Curd Whey Solutions by Electroflotation Coagulation Method //Mathematics. – 2022. – Т. 10. – №. 8. – С. 1284.
10. *Yerznkyan B. H., Gataullin T. M., Gataullin S. T.* Mathematical Aspects of Synergy //Montenegrin Journal of Economics. – 2022. – Т. 18. – №. 3. – С. 197-207.
11. *Petrosov D. A. et al.* Modeling of resource allocation in industrial organizations //Procedia Computer Science. – 2022. – Т. 213. – С. 355-359.
12. *Petrosov D. A. et al.* Mathematical apparatus of artificial neural networks for genetic algorithm controlling under structural parametric synthesis of large discrete systems //Procedia Computer Science. – 2022. – Т. 213. – С. 346-354.
13. *Беларев И. А., Обаева А. С.* О распределенном реестре и возможности его применения //Финансы: теория и практика. – 2017. – Т. 21. – №. 2. – С. 94-99.
14. *Walport M. (ed.).* Distributed ledger technology: Beyond block chain. – Government Office for Science, 2016.