DOI: 10.58168/CISMP2024_408-413
УДК 681.5

ИНФРАСТРУКТУРА КЛЮЧЕЙ И ПРИНЦИПЫ ЕЁ РАБОТЫ В СИСТЕМАХ РАСПРЕДЕЛЁННЫХ РЕЕСТРОВ

А.С. Плоткин[1], К.В. Стародубов[2], Ю.Ю. Громов[3]

[1]ФГАОУ ВО «Московский политехнический университет»
[2] ФГБОУ ВО «МИРЭА - Российский технологический университет»
[3]ФГБОУ ВО «Тамбовский государственный технический университет»

Аннотация. В статье приводятся результаты анализа принципов работы инфраструктуры ключей в «классических» системах и их сравнение с системами распределенных реестров, оценена применимость систем управления ключами в распределенных реестров. Сделан вывод о необходимости разработки специализированной математической модели, позволяющей провести оценку устойчивости инфраструктуры ключей в системах распределенных реестров.

Ключевые слова: технология распределённых реестров, инфраструктура ключей, системы управления ключами, устойчивость к деструктивным воздействиям.

KEY INFRASTRUCTURE AND PRINCIPLES OF ITS OPERATION IN DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS

A.S. Plotkin[1], K.V. Starodubov[2], Yu.Yu. Gromov[3]

[1]FGAOU VO Moscow Polytechnic University
[2]Federal State Budgetary Educational Institution Tambov State Technical University
[3]Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University

Abstract. The paper presents the results of analysing the principles of key infrastructure operation in ‘classical’ systems and their comparison with distributed registry systems, assesses the applicability of key management systems in distributed registries. It is concluded that it is necessary to develop a specialised mathematical model to assess the stability of key infrastructure in distributed registry systems.

Keywords: distributed ledger technology, key infrastructure, key management systems, resistance to destructive influences.

Технология распределённых реестров (ТРР) является одним из неотъемлемых элементов современных информационных систем и активно используется в критически важных секторах, таких как финансовые услуги, государственное управление, здравоохранение, энергетика и управление цепочками поставок [1].

С учетом строения систем ТРР, основанных на децентрализованной архитектуре, у которой отсутствует единая точка отказа, особое внимание уделяется обеспечению устойчивости к внешним и внутренним деструктивным воздействиям [2].

Важнейшей составляющей безопасности и устойчивости к таким деструктивным воздействиям является инфраструктура ключей (ИК), которая управляет криптографическими ключами, используемыми для аутентификации, шифрования данных и цифровой подписи. Именно от её устойчивости зависит защита данных, сохранение конфиденциальности и целостности информации, а также противодействие злоумышленникам, которые могут пытаться скомпрометировать ИК.

ИК представляет собой совокупность аппаратных, программных и организационных средств, обеспечивающих управление криптографическими ключами и сертификатами в информационных системах.

При определении факторов, приводящих к деструктивным воздействиям на ИК, необходимо учитывать особенности подходов, используемых для реализации ИК [3].

Классический подход в процессе работы задействует такие структуры, как Центр сертификации (ЦС) и Центр регистрации (ЦР).

Пример работы возможно изложить в последовательности шагов:

Шаг 1. Генерация ключей и выдача сертификата

1. Участник А генерирует пару ключей (открытый и закрытый).
2. Участник А отправляет открытый ключ в ЦР.
3. ЦР проверяет идентификационную информацию участника А.
4. ЦР пересылает запрос в ЦС.
5. ЦС подписывает открытый ключ участника А и создает цифровой сертификат.
6. Сертификат публикуется в репозитории.

Шаг 2. Подпись и верификация транзакции

1. Участник А создает транзакцию и подписывает ее своим закрытым ключом.
2. Транзакция передается участнику В.
3. Участник В извлекает сертификат участника А из репозитория.
4. Участник В использует открытый ключ из сертификата для верификации подписи.
5. Если подпись действительна, транзакция считается аутентичной.

Шаг 3. Шифрование и передача данных

1. Участник А шифрует данные с использованием открытого ключа участника В.
2. Данные передаются участнику В.
3. Участник В расшифровывает данные с использованием своего закрытого ключа.

Шаг 4. Отзыв сертификата

1. В случае компрометации закрытого ключа участника А, ЦА отзывает сертификат.

2. Информация об отзыве публикуется в реестре отозванных сертификатов.

3. Участники сети проверяют статус сертификатов перед выполнением транзакций.

Данный подход не применим в системах ТРР, так как нарушает основной принцип их работы (децентрализацию).

В системах ТРР вместо классической централизованной модели управления используется децентрализованный подход к управлению криптографическими ключами и аутентификации [4]. Основные принципы децентрализованной работы ИК в системах ТРР заключаются в следующем [5]:

– каждый участник системы генерирует свою пару ключей (открытый и закрытый). Закрытый ключ хранится в безопасном месте, обычно на локальном устройстве узла сети, и никогда не передается по сети. Открытый ключ распространяется в сети и может быть доступен всем узлам сети;

– в распределенных реестрах нет единого центра сертификации, который бы подтверждал подлинность участников. Вместо этого используется принцип децентрализованного доверия. Аутентификация и проверка узлов сети происходят с помощью криптографических методов, таких как цифровые подписи и хеш-функции;

– при создании транзакции узел сети подписывает её своим закрытым ключом. Эта подпись обеспечивает подлинность и целостность транзакции. Другие узлы сети могут проверить подпись с помощью открытого ключа отправителя;

– для верификации транзакции другие узлы сети используют открытый ключ отправителя. Если цифровая подпись транзакции действительна, и транзакция соответствует правилам консенсуса, она включается в блок и добавляется в распределенный реестр.

Пример работы ИК при децентрализованном подходе можно изобразить следующими шагами.

Шаг 1. Генерация ключевой пары

– Узел А генерирует пару ключей: закрытый ключ хранится локально, открытый ключ публикуется в распределенном реестре.

Шаг 2. Подпись транзакции

– Узел А создает транзакцию и подписывает её своим закрытым ключом. Подпись включает хеш транзакции, зашифрованный закрытым ключом узла А.

Шаг 3. Верификация транзакции

– Узел В получает транзакцию, извлекает открытый ключ узла А из РР и проверяет подпись, расшифровывая хеш. Если хеш совпадает с хешем транзакции, подпись действительна.

Шаг 4. Добавление блока в распределенный реестр

– Проверенные транзакции включаются в блок, который подписывается майнерами или валидаторами в зависимости от используемого алгоритма консенсуса. Подпись блока также проверяется остальными узлами сети.

Исходя из описанных шагов можно сделать вывод, что основными элементами, участвующими в работе ИК являются криптографические ключи, криптографические методы (цифровые подписи и хэш функции), которые используются для обеспечения доверия и устойчивости систем ТРР к деструктивным воздействиям.

Управление ИК оказывает значительное влияние на эффективность использования криптографии при обеспечении устойчивости к деструктивным воздействиям. Ненадлежащее управление ИК может поставить под угрозу любую систему, в том числе системы ТРР.

Для «классических» систем, в которых используется ИК существуют вспомогательные системы, которые берут на себя функции по управлению ключами, обеспечивая устойчивость ИК (системы управления ключами).

Системы управления ключами – это системы, предназначенные для генерации, распределения, хранения, защиты и управления криптографическими ключами в информационных системах. Они обеспечивают безопасность и целостность данных, поддерживая шифрование, цифровые подписи и аутентификацию [6].

Основные функции систем управления ключами:

- **генерация ключей**: Создание криптографических ключей.
- **распределение ключей**: Безопасное распространение ключей между пользователями или системами.
- **хранение ключей**: Надежное и защищенное хранение ключей.
- **замена ключей**: Обновление или замена устаревших или скомпрометированных ключей.
- **уничтожение ключей**: Безопасное удаление ключей по истечении их срока действия.
- **управление политиками**: Настройка и соблюдение политик безопасности в отношении ключей.

Применение систем управления ключами в системах ТРР возможно, они могут быть интегрированы, но чаще всего возникает ряд сложностей.

1. **Децентрализация и управление ключами:**

– системы ТРР, такие как блокчейн, по своей природе децентрализованы. Это усложняет централизованное управление ключами, которое предлагают традиционные системы управления ключами.

– в децентрализованных системах каждый узел или участник должен управлять своими ключами самостоятельно, что требует дополнительных механизмов для обеспечения безопасности и координации.

2. **Масштабируемость:**

– распределённые реестры могут включать тысячи или миллионы участников, что ставит высокие требования к масштабируемости и производительности систем управления ключами.

– обеспечение безопасности ключей на таком масштабе может быть сложной задачей.

3. **Комплаенс и регуляторные требования:**

– системы ТРР могут работать в различных юрисдикциях с различными регуляторными требованиями. Системы управления ключами должны соответствовать этим требованиям, что может быть сложно при глобальном развертывании.

4. **Интеграция и совместимость:**

– интеграция систем управления ключами с существующими системами ТРР может требовать значительных усилий и адаптации.

– не все системы управления ключами могут поддерживать специфические потребности и протоколы конкретных систем ТРР.

5. **Устойчивость и уязвимости:**

– системы управления ключами должны быть высокозащищёнными, так как они становятся ключевой точкой отказа и потенциальной целью для атак.

– комплексные механизмы защиты, такие как аппаратные криптографическое модули, могут быть необходимы для обеспечения безопасности.

При использовании ТРР системы управления ключами слабо применимы и не эффективны.

Выводы

Таким образом существующее математическое и алгоритмическое обеспечение, разработанное для централизованных систем, не способно в полной мере обеспечить необходимый уровень устойчивости ИК в условиях распределённых реестров «из коробки».

Проблемы возникают на всех этапах жизненного цикла ключей: от их генерации и распределения до эксплуатации, хранения и уничтожения, а также усугубляются при наличии множества независимых узлов, что затрудняет мониторинг и обеспечение устойчивости ИК.

Разработка инструмента, позволяющего проводить оценку устойчивости, могла бы решить данную проблему, путем выявление слабых мест и доработки процессов обеспечения устойчивости [7]. Это возможно реализовать при помощи разработки специализированной математической модели, позволяющей провести оценку устойчивости ИК в системах ТРР, что позволит внедрять необходимые средства обеспечения устойчивости к деструктивным воздействиям.

Список литературы

1. Плоткин А.С. Анализ применения распределенных реестров при взаимодействии банковских систем разных стран // Теория и практика проектного образования. 2022. №20.

2. Pal O., Alam B., Thakur V., Singh S. Key management for blockchain technology. ICT Express (2019). DOI: 10.1016/j.icte.2019.08.002.

3. Плоткин А.С., Кесель С.А., Репин М.М., Федоров Н.В. Анализ уязвимостей систем управления ключами в распределенных реестрах на примере блокчейн IBM // Вопросы кибербезопасности. - 2021. - № 1 (41). - С. 58-68.

4. Управление ключами шифрования и безопасность сети. – URL: https://www.intuit.ru/studies/courses/553/409/info (дата обращения: 11.09.2024).

5. Key management. – URL: https://cloud.ibm.com/docs/blockchain?topic=blockchain-ibp-security (дата обращения: 24.09.2024);

6. CKMS – Система управления криптографическими ключами // https://www.cryptomathic.com. – URL: https://www.cryptomathic.com/hubfs/Documents/Product_Sheets/Cryptomathic_CKMS_-_Product_Sheet.pdf (дата обращения: 23.05.2022).

7. Еськов С.С. Специальное математическое и программное обеспечение взаимного информационного согласования в системах распределенного реестра, 2020.

References

1. Plotkin A.S. Analysis of the application of distributed registers in the interaction of banking systems of different countries // Theory and Practice of Project Education. 2022. № 20.

2. O. Pal, B. Alam, V. Thakur, S. Singh, Key management for blockchain technology. ICT Express (2019). DOI: 10.1016/j.icte.2019.08.002.

3. Plotkin A.S., Kesel S.A., Repin M.M., Fedorov N.V. Vulnerability analysis of key management systems in distributed registries on the example of IBM blockchain // Voprosy cybersecurity. - 2021. - №1(41). - C. 58-68.

4. Encryption key management and network security. URL: https://www.intuit.ru/studies/courses/553/409/info (date of reference: 11.09.2024).

5. Key management. URL: https://cloud.ibm.com/docs/blockchain?topic=blockchain-ibp-security (access date: 24.09.2024);

6. CKMS - Cryptographic Key Management System. – URL: https://www.cryptomathic.com/hubfs/Documents/Product_Sheets/Cryptomathic_CKMS_-_Product_Sheet.pdf (access date: 23.05.2022).

7. Yeskov S.S. Special mathematical and software of mutual information coordination in distributed registry systems, 2020.