УДК 004.056

ПРИМЕНЕНИЕ БЛОКЧЕЙН ТЕХНОЛОГИИ В ОБЛАЧНЫХ ДАННЫХ

Артамонова А.В. (Университет ИТМО)
Научный руководитель – Чуваков В.А. (Университет ИТМО)

Введение. С быстрым развитием облачных вычислений стремительно развиваются сервисы облачного хранения данных. Одна из проблем, которая привлекла особое внимание в таких службах удаленного хранения, заключается в том, что серверов облачного хранилища недостаточно для надежного сохранения и обслуживания данных, что сильно влияет на уверенность пользователей в покупке и использовании услуг облачного хранения. Традиционные методы целостности данных для облачных хранилищ являются централизованными, что связано с огромными рисками безопасности из-за единой точки отказа и уязвимостей центральных серверов. Технология блокчейн предлагает новый подход к этой проблеме. Многие исследователи пытались использовать блокчейн для целостности данных. Основываясь на поиске соответствующих статей, было обнаружено, что в существующей литературе отсутствует тщательный обзор целостности облачных данных на основе блокчейна. В этой статье мы проводим углубленный обзор облачных данных на основе блокчейна. Во-первых, охватываются основные базовые знания по целостности облачных данных и методам блокчейна. Затем предлагается ряд требований для оценки существующих схем аудита целостности данных (САЦД) на основе блокчейна. Кроме того, предоставляется всесторонний обзор существующих схем САЦД и проводится оценка на основе предложенных критериев. Наконец, согласно завершенному обзору и анализу, исследуются некоторые нерешенные вопросы и предлагаются направления исследований, достойные дальнейших усилий в будущем [1].

Основная часть. В этом подразделе указываются некоторые потенциальные направления будущих исследований технологии аудита целостности облачных данных на основе блокчейна.

Во-первых, в схемах САЦД ожидается восстановление данных. Одним из прямых решений является то, что владельцы информации (ВИ) хранят несколько копий файла на нескольких провайдерах облачных сервисов (ПОС) в сети блокчейн. Таким образом, даже если копия файла повреждена в одном ПОС, ВИ может извлечь файл из другого ПОС. Однако это решение требует, чтобы ВИ генерировал несколько копий одного и того же файла, что может привести к дублированию хранилища и его потере. Таким образом, разработка экономичного решения САЦД, способного поддерживать восстановление данных с высокой эффективностью, является важной темой будущих исследований [2].

Во-вторых, свойство прослеживаемости имеет важное значение для исследований в схемах САЦД. Из-за ограниченной производительности распределенных узлов хранение больших объемов журналов операций блокчейна приводит к дополнительным накладным расходам на хранение и снижает скорость обработки транзакций. Одним из решений, которое можно было бы рассмотреть, является внедрение Межпланетной файловой системы (МФС). Такая децентрализованная файловая система эффективна и безопасна для хранения больших объемов журналов операций, поскольку она использует адресацию содержимого для уникальной идентификации каждого файла и в полной мере использует пространство для хранения каждого узла в сети. Таким образом, разработка облегченного метода хранения журналов операций является интересной темой исследования [3].

В-третьих, в схемах САЦД существенное значение имеет сокращение вычислительных затрат, связанных с операцией с динамическими данными. Для существующих схем оптимизация стратегии обновления является эффективным решением для снижения вычислительных затрат. Кроме того, лучше спроектировать эффективную структуру данных, которая поддерживает динамическую обработку данных. Для хранения информации о блоке

файла можно было бы использовать двухсвязный список. Такая структура данных может снизить вычислительные издержки, поскольку динамические операции с файловым блоком не приведут к изменениям в других файловых блоках, но страдают от высоких затрат на хранение. Поэтому вопрос о том, как спроектировать эффективную структуру данных, поддерживающую динамические операции с данными, является важной темой исследования.

В-четвертых, обнаружение атак и защита важны в схемах САЦД. Для обнаружения атак может быть полезно проанализировать стратегии обнаружения аналогичных атак в других сценариях (например, Peer to peer) и применить эти стратегии в схемах САЦД после улучшения. Для защиты от атак увеличение случайности в схеме САЦД может быть приемлемым методом предотвращения некоторых потенциальных внутренних атак. Кроме того, некоторые псевдослучайные функции могут быть использованы для маскировки местоположения объектов. Очевидно, что обнаружение и защита от потенциальных внутренних атак являются важными темами исследований, заслуживающими особых усилий.

Выводы. Схемы САЦД в основном предлагаются для противодействия злонамеренным аудиторам и решения отдельных проблем и ограничений производительности. В этой статье мы провели тщательный обзор схем САЦД. Сначала мы познакомили вас с базовыми знаниями САЦД. Затем мы предложили набор критериев для оценки существующих схем САЦД. После этого мы предложили систематику существующих схем в соответствии с различием в генерации метаданных.

Список использованных источников:

1. Зернов М.А. Блокчейн как распределенная система информационной безопасности предприятия // Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств. - 2018. - С. 67-75.
2. K.Yang,X.Jia Data storage auditing service in cloud computing: challenges, methods and opportunities World Wide Web, 15 (4) (2012), pp. 409-428
3. H. Tabrizchi, M. KuchakiRafsanjani A survey on security challenges in cloud computing: issues, threats, and solutions J. Supercomput., 76 (12) (2020), pp. 9493-9532