Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

“Proiectarea sistemelor informatice”

Лабораторная работа 1

Эссе:“Системы с централизованным и децентрализованным хранением данных”

Проверил: Гладей Анатлоий

Выполнил: Чобану Артём

Кишинев 2021

**Централизованное хранение:**

Многие компании вынуждены полагаться на централизованные базы данных для хранения информации своих клиентов. Подобные решения могут стать идеальным и экономически оправданным выбором для малого бизнеса. Но по мере роста компании необходимо расширять инфраструктуру и добавлять дополнительные сервера для обеспечения бесперебойной работы. В результате, масштабирование системы может стать основной статьей расходов. Не следует также забывать о проблемах, которые возникают в результате высокого трафика.

 Основная идея централизованных баз данных заключается в том, что один все данные хранятся в одном месте определенной сети. Поскольку резервность данных часто не предусмотрено, при ее потере возобновление практически невозможно и его приходится делать вручную.

Централизованные базы данных подвержены риску взломов и утечки данных. Обычно конфигурация данных настолько слаба, что злоумышленники могут легко ее использовать в своих целях. Очень часто нет необходимости использовать сложные подходы к взлому из-за изначально небезопасной базы данных. Даже при наличии системы защиты можно использовать метод перебора возможных решений для взлома слабых или дефолтных имен пользователей и паролей, прибегнуть к уязвимостям базы данных, применить SQL-инъекцию или украсть резервную копию. Результатом неправомерных действий может быть идентификация личности по хранимых данных, что GDPR рассматривает как грубое нарушение закона.

Используя слабо защищенную базу данных, бизнес не может гарантировать безопасность пользовательских данных. GDPR очень строг в отношении защиты данных и вероятность нарушений ставит компанию под угрозу. Даже при соблюдении законов, одна успешная хакерская атака может обойтись в миллионные штрафы и поставить бизнес в опасность.

**Децентрализованное хранение с использованием block-chain:**

Децентрализованные решения – более надежный и безопасный способ взаимодействия с пользовательскими данными. Если централизованное хранилище использует единый сервер для хранения данных, в децентрализованном информация хранится на нескольких серверах, за счет чего данные можно легко восстановить. И когда мы добавляем блокчейн, мы получаем безопасное хранилище для любых данных, включая данные ваших пользователей и клиентов.

Анонимность пользователей и защита данных лежат в основе как GDPR, так и блокчейна. Последний призван быть безопасным и скрытым. Открытые и закрытые ключи позволяют участникам отправлять и получать данные почти с абсолютной анонимностью. Публичный ключ не привязан к конкретному человеку, а информация хэшируется, поэтому не может быть использована для идентификации его личности. В этом плане блокчейн соответствует требованиям GDPR.

Увеличение безопасности – еще одно преимущество, которое следует принимать во внимание. Само понятие блокчейна подразумевает отсутствие единой уязвимости. Данные хранятся на многих нодах по всему миру, поэтому мы получаем распределенную систему без единой точки отказа. Компании, которые используют информацию с блокчейна, не будут работать под угрозой утечки данных. Вероятность сводится к минимуму, а то и вовсе равна нулю.

Практически неограниченная масштабируемость является главным основанных на блокчейне систем. Если при использовании централизованной базы данных вам нужно докупать новые сервера, то используя блокчейн, вам не придется выделять средства на их покупку и обслуживание. В результате, стоимость сервиса для вашей компании значительно снижается.

Различные блокчейн-компании предоставляют инструменты для создания собственных решений на основе блокчейна. Необходимо только нанять квалифицированных специалистов и оплатить транзакции. Цена разработки подобного решения может быть ниже цены обеспечения работы централизованного хранилища. Более того, оно нивелирует риск взломов, которые могут привести к многомиллионным штрафам.

Emercoin также работает над решением, которое поможет компаниям соответствовать требованиям GDPR. Блокчейн предоставляет более надежные решения для сбора, хранения и безопасности данных, поскольку он соответствует принципам «privacy by design», представленным в Общем регламенте защиты данных.