Hyperledger fabric

Большинство блокчейнов представляют из себя децентрализованную базу данных, функционирующую как распределенный цифровой реестр.

Основными преимуществами блокчейн технологии являются децентрализация и минимизация предположений о доверии, а также прозрачность исполняемых транзакций.

Обычно блокчейн рассматривается как единая технология, но существует два основных его вида: публичный и приватный.

Приватные блокчейны – это блокчейны, в которых создание блоков централизовано, и управление ими принадлежит одной организации. У участников такой сети должно быть разрешение на чтение, запись или проверку блокчейна. Также в частных блокчейнах существуют разные уровни доступа, и информация должна быть зашифрована, чтобы обеспечить конфиденциальность.

Публичные блокчейны – это общедоступные блокчейны, в которых каждый пользователь имеет право формировать транзакции, а операции защищены различными криптографическими протоколами (например proof-of-stake).

У приватных блокчейнов отсутствует важная особенность – децентрализация, однако такие сети эффективнее и экономичнее, чем публичные, которые требуют много ресурсов для проверки транзакций.

HLF – Это платформа с открытым исходным кодом для разработки и выполнения распределенных приложений (Distributed Ledger technology), основанных на технологии

ZKP и существующие варианты реализации

Доказательство с нулевым разглашением (ZKP ­– zero-knowledge-proof) – представляет из себя криптографические протоколы, позволяющие одной стороне (доказывающему) убедить другую сторону (проверяющего) в истинности какого-либо утверждения без раскрытия информации, подтверждающей это утверждение.

ZKP может быть интерактивным, когда доказывающий повторяет процесс доказательства для каждого проверяющего, а также неинтерактивным, когда доказывающий создаёт доказательство, которым может воспользоваться каждый человек, использующий то же доказательство.

Существует множество примеров реализации доказательства с нулевым разглашением, вот некоторые из них:

Протокол парольной аутентификации SRP (Secure Remote Password Protocol) – позволяет идентифицировать пользователя по знанию пароля, его особенность заключается в том, что пользователь подтверждает знание пароля, но не раскрывает его при подключении. SRP использует асимметричное шифрование, где используются два ключа: открытый и закрытый. Открытый ключ может быть распространен свободно, но закрытый ключ должен храниться в секрете, так как он используется для расшифровки данных. Алгоритм работы асимметричного шифрования заключается в генерации сервером пары ключей, передаче открытого ключа клиенту, шифровании клиентом данных с помощью открытого ключа и расшифровке сервером данных с помощью закрытого ключа.

zk-SNARKs (Zero Knowledge Succint Non-Interactive Argument of Knowledge) – неинтерактивный криптографический протоколом, позволяющий доказать знание о некоторых данных, не раскрывая сами данные. У протоколов zk-SNARK есть важная особенность: они требуют доверительной установки между проверяющим и проверяемым. Для построения доказательств нулевого знания с помощью zk-SNARK необходим набор открытых параметров, а также создание криптографических ключей. Эти параметры можно сравнить с «правилами» протокола, и они обычно кодируются. Между тем, ключи делают возможной конфиденциальность. Zcash – один из самых популярных протоколов, сохраняющих конфиденциальность, в котором используются zk-SNARK. Кроме того, некоторые популярные ZK-роллапы и блокчейны второго уровня используют технологию доказательства zk-SNARK для обеспечения масштабируемости традиционных блокчейн-сетей, таких как Ethereum.

Приложение для переводов с использованием алгоритмов ZKP на Hyperledger Fabric

Приложение обеспечивает безопасные и конфиденциальные переводы между электронными счетами, используя алгоритмы ZKP для гарантии приватности и интеграции данных. Основные функции приложения включают:

1. Безопасные и конфиденциальные переводы: Приложение использует алгоритмы ZKP для проверки транзакций без раскрытия деталей транзакции, обеспечивая таким образом конфиденциальность данных.

2. Лимиты на переводы: Приложение учитывает возможные лимиты на переводы между счетами в день, обеспечивая таким образом контроль над финансовыми операциями и соответствие требованиям регулирования.

3. Скрытие и доказывание информации о лимитах: Приложение использует доказательства с нулевым разглашением для скрытия информации о лимитах на переводы, гарантируя приватность пользовательских данных.

Hyperledger Fabric обеспечивает надежность и безопасность транзакций благодаря своей модулярной архитектуре и возможностям настройки прав доступа. Таким образом, пользователи могут осуществлять переводы средств, сохраняя конфиденциальность своих финансовых операций и обеспечивая безопасность передачи средств.

Для реализации этого приложения можно использовать криптографические протоколы, такие как Identity Mixer (Idemix), основанные на ZKP. Эти протоколы позволяют обеспечить приватную аутентификацию и передачу сертификатов или атрибутов с помощью доказательств знания, не раскрывая самих знания.