в наиболее подготовленной для инновация сфере. Они позволяют осуществлять анонимные транзакции без раскрытия их деталей или личности участников. Так работает, например, блокчейн Zcash, а сеть Ethereum использует ZK-Rollups для создания сжатых доказательств о состоянии целой группы транзакций, что позволяет значительно увеличить производительность блокчейна.

ZK-доказательства могут использоваться в полях аутентификации и контроля доступа, чтобы продемонстрировать знание пароля или криптографического ключа, не раскрывая сам пароль или ключ.

ZK-доказательства также используются в системах электронного голосования, где они позволяют избирателям продемонстрировать легитимность своего волеизъявления, не раскрывая подробностей голосования, защищая целостность избирательного процесса.

Доказательства с нулевым разглашением могут улучшить конфиденциальность транзакций в цифровых валютах центрального банка (CBDC), облегчая частные транзакции и поддерживая анонимность пользователей. Балансируя между конфиденциальностью и прозрачностью транзакций CBDC, ZKP обеспечивает возможность аудита без раскрытия специфики транзакции. Например, в технологии цифрового рубля ZKP можно использовать для повышения конфиденциальности, а также для сохранения анонимности при трансграничных переводах между разрабатываемым белорусским цифровым рублем и перспективной единой цифровой валютой БРИКС.

В качестве еще одного приложения можно привести Filecoin, децентрализованное хранилище данных, которое использует ZK-SNARK для обеспечения безопасной и эффективной проверки целостности данных, хранящихся на сети.

Недостатки

Доказательства с нулевым разглашением могут подвергаться различным видам атак:

1. Атака на приватность. Злоумышленник может попытаться извлечь конфиденциальную информацию, которая должна оставаться скрытой в процессе проведения ZKP. Это может произойти, если протокол ZKP не обеспечивает адекватную конфиденциальность.

2. Подделка доказательства. Злоумышленник может попытаться создать ложное доказательство и представить его как действительное. Протокол ZKP должен быть устойчив к подобным атакам.

3. Атаки на параметры. Злоумышленник может выбирать параметры так, чтобы они облегчили взлом системы: выбор ненадежных хеш-функций, кривых эллиптической криптографии и т.д.

4. Уязвимости в коде. Недостаточно безопасные или уязвимые реализации ZKP-протоколов могут стать точкой входа для атак.

5. Атаки на хеширование или криптографические алгоритмы.

6. Атаки на передачу данных. При передаче ZKP через сеть может существовать риск перехвата или модификации данных, что может повлиять на их целостность и конфиденциальность.

Есть и другие недостатки ZKP, не связанные с информационной безопасностью.

Разработка и проверка ZK-доказательств может быть трудоемкой с точки зрения ресурсов и вычислений, особенно для сложных вариантов реализации технологии. Увеличение времени обработки транзакций и объема вычислительной работы может затруднить масштабирование блокчейн-систем.

Кроме того, ZK-доказательства добавляют новый уровень сложности к исходной информационной системе, затрудняя ее аудит и проверку протокола. В свою очередь, это создает риск в части информационной безопасности и эксплуатации незамеченных багов.

Заключение

Уже сегодня технологию доказательства с нулевым разглашением в совокупности с блокчейнами и распределенными реестрами можно эффективно использовать в сфере защиты данных, в том числе и ПДн. При этом сами данные могут вообще не передаваться по внешней сети, а пользователь сможет в режиме онлайн отслеживать согласия на обработку.

В настоящее время у технического комитета ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection находятся в разработке рекомендации по сохранению конфиденциальности, основанные на доказательствах с нулевым разглашением (ISO/IEC WD 27565.3)[1].

Этот документ будет содержать рекомендации по использованию доказательств с нулевым разглашением для улучшения конфиденциальности путем снижения рисков, связанных с совместным использованием или передачей персональных данных между организациями и пользователями, путем сведения к минимуму объема передаваемой информации. В нем будут приведены несколько функциональных требований ZKP, относящихся к целому ряду различных вариантов бизнес-использования, а затем описано, как можно использовать различные модели ZKP для надежного удовлетворения этих функциональных требований. ●

В технологии цифрового рубля ZKP можно использовать для повышения конфиденциальности, а также для сохранения анонимности при трансграничных переводах между разрабатываемым белорусским цифровым рублем и перспективной единой цифровой валютой БРИКС.

Разработка и проверка ZK-доказательств может быть трудоемкой с точки зрения ресурсов и вычислений, особенно для сложных вариантов реализации технологии.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

1 https://www.iso.org/standard/80398.html