Новосибирский национальный исследовательский
государственный университет
Факультет информационный технологий
Кафедра компьютерных систем

Методы сокрытия приватных данных в открытых распределенных реестрах

Выполнил:
Аспирант группы 19232
Кондырев Д. О.

Руководитель ВКР:
Токарева Наталья Николаевна,
к.ф.-м.н., доцент кафедры компьютерных систем ФИТ, с.н.с. лаборатории дискретного анализа Института математики им. С.Л.Соболева

2019 г.

Проблема сокрытия информации в открытых распределенных реестрах

- Нет возможности скрыть часть полей транзакции.
- Существует возможность отслеживать действия пользователя путем анализа транзакций.

Цель

Разработать методы сокрытия приватных данных в открытых распределенных реестрах, что позволит расширить область применения технологии в промышленных программных комплексах.

Задачи

- Провести анализ проблемы сокрытия информации в открытых распределенных реестрах.
- Изучить существующие решения проблемы сокрытия информации.

Изученные системы

- **ZCash** – блокчейн-система с возможностью проведения анонимных финансовых транзакций.
- **zkLedger** – распределенный реестр с возможностью сокрытия информации о финансовых транзакциях, поддерживающий аудит сторонними организациями.
- **Identuty Mixer** - криптографический алгоритм для аутентификации пользователей, обеспечивающий конфиденциальность и безопасности.
- **FabZK** – протокол для сохранения приватности и обеспечения возможности аудита информации в смарт-контрактах Hyperledger Fabric.
- **PrivIdEx** – протокол сохранения приватности пользователей и обмена цифровыми идентификаторами пользователей в распределенном реестре.

Доказательство с нулевым разглашением

Цель доказательства с нулевым разглашением заключается в том, чтобы верификатор мог убедиться, что доказывающая сторона обладает знанием секретного параметра. При этом сам секретный параметр не должен раскрываться верификатору или кому-либо еще.

Требования к алгоритмам доказательства с нулевым разглашением в распределенных реестрах

- Неинтерактивность
- Небольшой размер доказательства
- Вычислительная эффективность

NIZK

NIZK (Non-Iterative Zero-Knowledge proof) – это криптографический протокол неинтерактивного доказательства с нулевым разглашением, представляющий из себя тройку алгоритмов:

- Алгоритм генерации параметров: $K(1^k) \rightarrow \sigma$
- Алгоритм доказательства: $P(\sigma, x, \omega) \rightarrow \pi$
- Алгоритм верификации: $V(\sigma, x, \pi) \rightarrow \{0,1\}$

NIZK

+ Не требует доверенной инициализации параметров

– Время проверки и генерации доказательства зависят от сложности проверяемых свойств
– Размер доказательства зависит от проверяемых свойств

zk-SNARK

zk-SNARK – это криптографический протокол неинтерактивного доказательства знания с нулевым разглашением, который представляет собой тройку алгоритмов (*Gen*, *P*, *V*):

- $Gen\ (\lambda, C) \rightarrow (pk, vk)$
  - pk – ключ доказательства
  - vk – ключ верификации
- $P\ (pk, x, a) \rightarrow \pi$
  - π –доказательство
- $V\ (vk, x, \pi) \rightarrow \{true, false\}$

zk-SNARK

+ Длина доказательства не зависит от сложности проверяемых свойств
+ Время проверки доказательства не зависит от размера схемы и секретного параметра.

– Требует доверенной инициализации параметров

Выявленные проблемы

- Решения работают для узкого круга задач
- Эффективность
- Реализации только на стадии прототипов

Результаты

- Исследованы последние разработки в области сокрытия приватности информации и анонимизации транзакций в распределенных реестрах.
- Изучены научные статьи и программные реализации алгоритмов.
- Подготовлен доклад на научный семинар «Криптография и криптоанализ».
- Написана научная статья на тему «Разработка метода сокрытия приватных данных для системы тендеров на основе технологии блокчейн».