Криптография и блокчейн, обзор решений и перспективы развития

Матвеев Сергей Васильевич,
ПФ ФГУП «НТЦ «Атлас», г.Пенза

Bitcoin – самый известный блокчейн

Использовались известные механизмы

- схема ЭЦП (ECDSA)
- хеш-цепочки и хеш-деревья (Merkle Tree)
- Схема доказательства работы (Proof of Work)

Уровни технологии блокчейн

- Пользовательский уровень или уровень приложений
- Уровень сетевого взаимодействия
- Уровень консенсуса

Пользовательский уровень Функционал

- Формирование данных для включения в реестр
- Запросы на чтение и запись к реестру
- Взаимодействие между пользователями
- Управление персональными конфиденциальными данными (ключами)
- Реализация мер по обеспечению безопасности персональных данных

Пользовательский уровень Криптография и безопасность

- функции хеширования (SHA256, RIPEMD160, SHA512 и т.п.)
- Схема ЭЦП
- Защищенные протоколы обмена данными между пользователями

- Алгоритмы шифрования
- Организационные и технические меры обеспечения безопасности на местах пользования

Уровень сетевого взаимодействия

- Алгоритмы и протоколы взаимодействия между узлами сети
  - Установления связи
  - Обмен сообщениями между узлами сети
  - Прием и рассылка сообщений

Уровень консенсуса

- Представление данных для хранения в реестре
- Верификация данных для включения в реестр
- Запись данных в реестре
- Чтение данных в реестре
- Модификация данных в реестре

Безопасность на уровне пользователя и сетевого взаимодействия

- Стандартные предположения о доступных нарушителю знаниях и методах реализации атак
- Традиционные задачи обеспечения безопасности (аутентификация сторон, аутентификация источника данных, целостность данных, и т.д.)
- Традиционные, в том числе стандартизированные, криптографические алгоритмы и протоколы

- Можем использовать известные подходы по теоретической и практической оценке стойкости, ранее разработанные методические документы

Пример 1. Оценка свойств безопасности протоколов согласно IETF

Код	Свойство	Bitcoin
G1	Аутентификация субъекта	+
G2	Аутентификация сообщения	+
G3	Защита от повтора	+
G5	Аутентификация источника	+
G6	Авторизация третьей стороной	-
G7	Аутентификация ключа	+
G8	Подтверждение правильности ключа	+
G9	Защищенность от чтения назад	-
G10	Формирование новых ключей	-
G11	Защищенная возможность договориться о параметрах безопасности	-
G12	Конфиденциальность	-

Пример 2. Атака на основе информации, полученной из технических каналов

- Атака:
  - Секретный ключ (СК) однозначно определяет адрес получателя/отправителя
  - Количество наблюдений СК (вероятность успеха атаки) пропорционально количеству транзакций и зависит от оставшихся средств
- Защита
  - После каждой транзакции выводить все оставшиеся средства на новый адрес связанный с новым СК
- Недостатки
  - Может быть накладно, если каждый перевод требует оплаты

Безопасность уровня консенсуса

- Модель угроз и нарушителя существенно отличается от традиционной
- Зависит от характеристик устройств верифицирующих данные для включения в реестр (для алгоритмов PoW)
- Зависит от характеристик сети связи
  - Синхронная или асинхронная
  - Скорость
  - Задержки
  - Связность
  - Потеря данных

Безопасность уровня консенсуса

Исходная работа

S. Nakamoto. «*Bitcoin: A Peer-to-Peer Electronic Cash System*»
не содержит строгого обоснования безопасности предлагаемых решений

Безопасность уровня консенсуса

Ряд последних результатов:

- *Р*азработана формальная модель ядра протокола Bitcoin
- Определены фундаментальные свойства протокола
- Для синхронной сети строго доказано, что задача о Византийских генералах решается в случае, если у нарушителя менее 0.5 хеширующей мощности
  - Работа J. A. Garay, A. Kiayias, N. Leonardos, *«The Bitcoin Backbone Protocol: Analysis and Applications». «The Bitcoin Backbone Protocol with Chains of Variable Difficulty», 2014-2016.*
- Формальная модель для случая асинхронной сети
  - R. Pass, L. Seeman, A. Shelat, *«Analysis of the Blockchain Protocol in Asynchronous Networks», 2016.*

Выводы

- для уровня пользователя и сетевого уровня можно использовать традиционные подходы
- ряд традиционных криптоатак применительно к технологии блокчейн до настоящего времени не рассматривались
- в настоящее время активно ведутся работы по теоретическому обоснованию стойкости существующих алгоритмов достижения консенсуса
- при внедрении технологии блокчейн на практике стоит отдавать предпочтение решениям, имеющим строгое теоретическое обоснование стойкости

Спасибо за внимание!

Вопросы?