

Сегодня мы наблюдаем рост внимания к технологии блокчейн и распределенного реестра (*Distributed Ledger Technology, DLT*), которая является одной из ключевых сквозных технологий Цифровой экономики Российской Федерации. Однако большинство криптопримитивов, применяемых в блокчейне, в том числе хеш-функции (ГОСТ Р 34.11-2018, SHA-2, SHA-3, SHA256, Ethash, SCrypt, X11, Equihash, RIPEMD160 и др.), электронные подписи (ГОСТ 34.10-2018, ECDSA, EdDSA, Ring, One-Time, Borromean, Multi-signature и др.), асимметричные криптографические алгоритмы (RSA, Диффи-Хеллмана и др.) и соответствующие протоколы уже не являются квантово-устойчивыми, то есть устойчивыми к атакам с использованием так называемого релевантного или значимого квантового компьютера (англ. *Cryptographically Relevant Quantum Computer, CRQC*). Сегодня уже известны эффективные квантовые алгоритмы, в частности, алгоритм Шора для факторизации и дискретного логарифмирования, которые могут быть успешно применены для взлома перечисленных криптопримитивов.

Предложена новая постановка задачи обеспечения киберустойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации в условиях квантовых кибератак злоумышленников на основе авторских моделей и методов. Настоящий материал является первой работой по упомянутой проблеме и содержит результаты не только качественного, но и количественного изучения квантовой устойчивости блокчейн-экосистем и платформ государства и бизнеса. По этой причине пособие представляет несомненный теоретический и практический интерес для специалистов в области компьютерных наук и информационных технологий.

Введение

Глава 1. Актуальность создания квантово-устойчивых блокчейн-экосистем и платформ Цифровой экономики Российской Федерации

1.1. Общие сведения о технологии блокчейн

- 1.1.1. Что понимается под блокчейном
- 1.1.2. Как развивался блокчейн
- 1.1.3. Какие типы блокчейна существуют
- 1.1.4. Каковы перспективы блокчейна

1.2. Структура и поведение типового блокчейн

- 1.2.1. Связный список
- 1.2.2. Цепочка хешей
- 1.2.3. Дерево Меркла
- 1.2.4. Электронная подпись
- 1.2.5. Как работает блокчейн
- 1.2.6. Запись транзакций в блокчейн
- 1.2.7. Проверка подписанного блока

1.3. Проблема обеспечения киберустойчивости блокчейна

- 1.3.1. Сопроблемы обеспечения киберустойчивости блокчейна
- 1.3.2. Замысел разрешения проблемы

1.4. Возможные представления киберустойчивого блокчейна

- 1.4.1. Первичные понятия
- 1.4.2. Возмущенные вычисления
- 1.4.3. Характерные особенности возмущений
- 1.4.4. Модель гипервизора киберустойчивости блокчейн
- 1.4.5. Управление киберустойчивостью блокчейн
- 1.4.6. Моделирование поведения блокчейн в условиях возмущений
- 1.4.7. Системный облик системы обеспечения киберустойчивости блокчейн
- 1.4.8. Краткие итоги

Глава 2. Модели угроз безопасности блокчейн-экосистемам и платформам Цифровой экономики Российской Федерации

- 2.1. Модель угроз безопасности Цифровой экономики Российской Федерации на основе аналитики зарубежных национальных квантовых программ**
 - 2.1.1. Квантовая инициатива США
 - 2.1.2. Квантовые программы стран мира
 - 2.1.3. Общая модель квантовых угроз безопасности
- 2.2. Модель квантовых угроз безопасности блокчейн-экосистемам и платформам Цифровой экономики Российской Федерации**
 - 2.2.1. Криптопримитивы биткоина
 - 2.2.2. Уязвимости Биткоина
 - 2.2.3. Сценарии комбинированных атак
 - 2.2.4. Возможные квантово-устойчивые решения
 - 2.2.5. Промежуточные итоги
- 2.3. Общая модель угроз безопасности блокчейн-экосистем и платформ Цифровой экономики Российской Федерации**
 - 2.3.1. Криптопримитивы блокчейн
 - 2.3.2. Алгоритмы консенсуса
 - 2.3.3. Смарт-контракты
 - 2.3.4. Оракулы
 - 2.3.5. Узлы сети
 - 2.3.6. Клиентские приложения
 - 2.3.7. Как обеспечить требуемую безопасность блокчейна
- 2.4. Оценка последствий кибератак злоумышленников на блокчейн-экосистемы и платформы Цифровой экономики ведущих стран мира**
 - 2.4.1. 2020 год
 - 2.4.2. 2021 год
 - 2.4.3. 2022 год

Заключение

Литература

Приложение. Перечень известных национальных квантовых программ (НИОКР)

Сведения об авторе