

Ишукова Е. А., Панасенко С. П., Романенко К. С., Салманов В. Д.

Криптографические ОСНОВЫ

блокчейн- технологий



Оглавление

Предисловие.....	6
Введение	7
Глава 1. Алгоритмы хеширования.....	9
1.1 Основные понятия и определения	10
1.1.1 Структура алгоритмов хеширования	10
1.1.2 Надстройки над алгоритмами хеширования.....	14
1.2 Методы криптоанализа и атаки на алгоритмы хеширования.....	18
1.2.1 Цели атак на алгоритмы хеширования	19
1.2.2 Атаки методом «грубой силы»	21
1.2.3 Словарные атаки и цепочки хеш-кодов	22
1.2.4 Радужные таблицы.....	26
1.2.5 Парадокс «дней рождения» и поиск коллизий	27
1.2.6 Дифференциальный криптоанализ	30
1.2.7 Алгебраический криптоанализ.....	34
1.2.8 Атаки, использующие утечки данных по побочным каналам.....	35
1.2.9 Другие виды атак	35
1.3 Наиболее известные алгоритмы хеширования	38
1.3.1 Алгоритмы семейства MD	38
1.3.2 Алгоритмы семейства RIPEMD	59
1.3.3 Алгоритмы семейства SHA.....	69
1.3.4 Отечественные стандарты хеширования.....	84
Глава 2. Алгоритмы электронной подписи на эллиптических кривых	91
2.1 Математические основы	91
2.2 Эллиптические кривые.....	95
2.2.1 Определение эллиптической кривой	95
2.2.2 Основные операции над точками эллиптической кривой	96
2.2.3 Основные характеристики эллиптической кривой.....	99
2.2.4 Примеры эллиптических кривых	101
2.2.5 Задача дискретного логарифмирования в группе точек эллиптической кривой.....	105
2.2.6 Альтернативные формы представления эллиптических кривых ...	107
2.3 Основные алгоритмы электронной подписи	111
2.3.1 Алгоритм ECDSA	111
2.3.2 ГОСТ Р 34.10–2012	112

2.3.3 Некоторые особенности алгоритмов ECDSA и ГОСТ Р 34.10–2012	114
2.3.4 Алгоритм EdDSA.....	116
2.3.5 Алгоритм BLS	118

Глава 3. Основные принципы работы блокчейн-технологий... 122

3.1 Базовые механизмы блокчейн-систем.....	123
3.1.1 Транзакции.....	123
3.1.2 Упаковка транзакций в блоки	127
3.1.3 Применение деревьев Меркля при формировании блоков.....	130
3.2 Механизмы консенсуса	131
3.2.1 Консенсус доказательства работы Proof of Work	131
3.2.2 Консенсус доказательства владения долей Proof of Stake.....	135
3.2.3 Консенсус на основе решения задачи византийских генералов	136
3.2.4 Другие механизмы достижения консенсуса	137
3.3 Выстраивание цепочки блоков	139
3.3.1 Принципы формирования цепочки	139
3.3.2 Ветвления цепочки блоков.....	142
3.4 Смарт-контракт.....	145
3.5 Основные виды блокчейн-систем	148
3.5.1 Публичный блокчейн.....	148
3.5.2 Приватный блокчейн.....	149
3.6 Криптовалютные кошельки	150
3.6.1 Программы-кошельки.....	150
3.6.2 Аппаратные кошельки.....	152

Глава 4. Основные блокчейн-платформы..... 153

4.1 Биткойн	153
4.1.1 Введение в устройство блокчейн-системы Биткойн.....	154
4.1.2 Особенности механизма консенсуса в системе Биткойн.....	156
4.1.3 Форки в системе Биткойн	156
4.1.4 Транзакции.....	159
4.1.5 Кошельки в системе Биткойн.....	203
4.1.6 Создание и использование иерархических детерминированных ключей.....	206
4.2 Эфириум	209
4.2.1 Глобальное состояние	209
4.2.2 Консенсус.....	210
4.2.3 Газ.....	211
4.2.4 Адреса и кошельки.....	212
4.2.5 Транзакции.....	213
4.2.6 Структура блока	213
4.2.7 Эволюция системы Эфириум.....	214
4.2.8 Основная и тестовые сети платформы Эфириум.....	218
4.2.9 Запуск сети Эфириум.....	219
4.2.10 Смарт-контракты в системе Эфириум	234
4.3 Hyperledger	245

4.3.1 Основные особенности системы	245
4.3.2 Проекты экосистемы Hyperledger	246
4.3.3 Архитектура Hyperledger Fabric	247
4.3.4 Пример смарт-контракта для Hyperledger	248
4.4 Обзор других платформ	253
4.4.1 EOSIO	253
4.4.2 Краткий обзор прочих блокчейн-платформ	255
4.4.3 Обзор отечественных решений	257
Приложение 1. Таблицы констант алгоритмов хеширования	261
П1.1 Таблица замен алгоритма MD2	261
П1.2 Индексы используемых в итерациях слов блока сообщения алгоритма MD4	262
П1.3 Константы алгоритма MD5	263
П1.4 Константы алгоритма MD6	267
П1.5 Константы алгоритмов семейства SHA-2	268
П1.6 Раундовые константы алгоритмов семейства SHA-3	270
П1.7 Константы алгоритма ГОСТ Р 34.11–2012	271
Список сокращений	275
Перечень рисунков	281
Перечень таблиц	286
Перечень источников	289