



# **БЛОКЧЕЙН**

**И ДЕЦЕНТРАЛИЗОВАННЫЕ  
СИСТЕМЫ**

**ЧАСТЬ 3**

Distributed Lab

УДК 004.738.5:336]:007-057.21](07)

К78

Авторы:

*П. Кравченко, Б. Скрябин, А. Курбатов, О. Дубинина*

**Кравченко П.**

К78 Блокчейн и децентрализованные системы : учеб. пособие для студ. заведений высш. образования : в 3 частях. Ч. 3 / П. Кравченко, Б. Скрябин, А. Курбатов, О. Дубинина. – Харьков : ПРОМАРТ, 2020. – 306 с. : ил. 178; табл. 7; библиогр.: 145 назв.

ISBN 978-617-7634-25-5

ISBN 978-617-7634-78-1 (ч. 3)

Предлагаемое учебное пособие посвящено децентрализованным технологиям, которые стали популярны благодаря распространению криптовалют. Вначале авторы акцентируют внимание на технических и фундаментальных аспектах криптовалют, технологии блокчейн и уровне приложений, предоставляя читателю возможность глубоко разобраться в основах. Особенность книги состоит в том, что материал изложен на стыке принципов работы, преимуществ и рисков инновационных информационных технологий.

Издание рассчитано на широкую аудиторию: научных работников, преподавателей, аспирантов, студентов, имеющих базовые знания в области криптографии и информационных технологий, – всех, кого интересуют вопросы децентрализованных технологий.

УДК 004.738.5:336]:007-057.21](07)

ISBN 978-617-7634-78-1 (ч. 3)

ISBN 978-617-7634-25-5

© Кравченко П., Скрябин Б.,

Курбатов А., Дубинина О., 2020

784 712

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	9
О DISTRIBUTED LAB.....	11
1. ПРИМЕНЕНИЕ ДЕЦЕНТРАЛИЗОВАННЫХ ПОДХОДОВ ДЛЯ ОРГАНИЗАЦИИ РАЗЛИЧНЫХ СИСТЕМ.....	13
1.1 Принципы функционирования и развитие mesh networks .....	13
Глобальная цель mesh-сетей.....	15
Популярные протоколы для организации mesh-сетей.....	17
Применение mesh-сетей на практике.....	19
Недостатки mesh-сетей.....	21
1.2 Децентрализованные системы цифровой идентификации.....	23
Устройство и принципы функционирования протокола OAuth.....	28
Протоколы OpenID и OpenID Connect.....	31
Ограничения описанных протоколов .....	34
Принципы построения глобальной системы идентификации.....	36
Расширение возможностей глобальной системы идентификации с помощью технологии blockchain.....	41
Цифровой identity для IoT.....	45
1.3 Децентрализованные платформы электронного голосования.....	47
Проблемы традиционных подходов к проведению голосования.....	47
Электронное голосование в Эстонии.....	50
Электронное голосование в Швейцарии.....	54
Децентрализованный подход к проведению электронного голосования.....	56
Пример схемы голосования без центрального органа.....	56
Использование технологии blockchain для системы электронного голосования.....	63
1.4 Технологии децентрализованных бирж.....	65

Принципы функционирования децентрализованных бирж.....	67
Escrow.....	68
Atomic Swap.....	69
0x Protocol.....	70
Internal exchanges.....	72
1.5 Децентрализованный аукцион.....	74
Принцип работы онлайн-аукциона.....	75
Принцип работы децентрализованного онлайн-аукциона.....	77
2 ПОДПИСИ ШНОРРА И СВЯЗАННЫЕ С НИМИ ОБНОВЛЕНИЯ.....	81
2.1 Особенности подписей Шнорра и возможность их имплементации в учетных системах.....	81
Преимущества подписей Шнорра.....	82
Устройство подписей Шнорра.....	85
Мультиподпись при помощи алгоритма Шнорра.....	86
Принцип проведения Rouge Key Attack.....	87
Схема Bellare-Neven.....	92
Схема MuSig.....	92
Ограничения использования подписей Шнорра.....	93
Особенности имплементации подписей Шнорра.....	95
2.2 Концепция MAST в Bitcoin.....	96
Abstract Syntax Tree.....	98
Что же такое MAST?.....	101
Упрощенная схема MAST.....	102
Преимущества и особенности MAST при большом количестве альтернативных условий.....	105
Применение MAST на практике.....	108
Развитие концепции и текущее состояние.....	109
2.3 Принципы функционирования Taproot.....	110

---

Альтернативные условия нужны для решения разногласий между участниками контракта.....	111
Подписи Шнорра как базовый элемент Taproot.....	113
Каскады Taproot сценариев.....	117
2.4 Устройство Graftroot.....	119
Отдельная подпись каждого альтернативного условия.....	119
Возможность добавление новых условий.....	123
3 ИСПОЛЬЗОВАНИЕ КОНЦЕПЦИЙ SHARDING, OFF-CHAIN И DAG ДЛЯ МАСШТАБИРОВАНИЯ УЧЕТНЫХ СИСТЕМ.....	126
3.1 Использование off-chain протоколов.....	127
3.2 Концепция шардинга.....	130
Sharding в blockchain-based системах.....	134
Архитектура TON.....	137
Устройство цепочки блоков в TON.....	137
Разделение и объединение shardchains.....	140
Принятие решений относительно состояния системы.....	141
Обмен сообщениями между shardchains.....	142
3.3 Конструкция и применение DAG.....	145
Directed acyclic graph.....	145
Понятие направленных ациклических графов.....	147
Архитектура распределенных учетных систем на основе DAG.....	148
Достижение консенсуса и решение разногласий.....	150
IOTA.....	152
Транзакции в IOTA.....	152
Структура и назначение Bundle.....	156
4 МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ В ИНТЕРНЕТЕ.....	160
4.1 Принципы функционирования и применение Tor.....	160

Подходы анонимизации пользователя сети .....	161
Особенности применения Tor .....	163
Получение списка узлов Tor .....	165
Методики деанонимизации пользователей dark networks .....	166
4.2 Internet invisible project.....	169
Чесночная маршрутизация.....	170
Выбор промежуточных узлов и создание туннелей.....	172
Адресация и поиск узлов.....	173
4.3 Устройство Tox.....	175
Как устроены аккаунты Tox.....	175
Типы узлов и приложения.....	177
Принцип работы луковой маршрутизации.....	178
Соединение собеседников.....	180
TCP Relay узлы.....	183
Использование DHT для поиска контактов в сети.....	184
4.4 Стеганографические методы скрытия информации .....	186
Особенности работы и преимущества.....	187
Классическая стеганография.....	188
Компьютерная стеганография.....	189
Цифровая стеганография.....	190
Особенности применения и атаки.....	193
5 ОСОБЕННОСТИ И РОЛЬ КРИПТОГРАФИЧЕСКИХ ОБЯЗАТЕЛЬСТВ В УЧЕТНЫХ СИСТЕМАХ.....	195
5.1 Особенности и методы построения криптографических обязательств .....	196
Добавление случайности как компонента обязательств.....	197
Обязательства Педерсена.....	199
Подмена знаний и подходы Nothing Up My Sleeve.....	201

---

Одно обязательство для вектора значений .....	203
Схема ElGamal commitment .....	205
5.2 Протокол идентификации Шнора как схема интерактивного доказательства с нулевым разглашением .....	206
Схема идентификации Шнора .....	206
В каком случае доказывающая сторона может подделать доказательство .....	208
Превращение интерактивного протокола в неинтерактивный .....	210
5.3 Использование обязательств Педерсена для доказательств с нулевым разглашением .....	210
Использование обязательств Педерсена в Confidential Transaction .....	215
Использование обязательств Педерсена для range proofs .....	216
6 КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И ПОСТКВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ .....	218
6.1 Введение в quantum computing .....	218
Основные принципы квантовой механики .....	219
Возможности квантового компьютера .....	224
6.2 Что такое кубит и основные операции с кубитами .....	228
Оперирование с несколькими кубитами .....	233
6.3 Использование квантовых гейтов .....	236
Однокубитовые квантовые гейты .....	237
Мультикубитные квантовые гейты .....	239
Квантовые схемы .....	241
Схема создания состояний Белла .....	244
Схема квантовой телепортации .....	245
6.4 Математические основы постквантовых криптографических алгоритмов .....	248
Криптографические примитивы, уязвимые к атакам квантового компьютера .....	250

Насколько срочно необходимо переходить на алгоритмы, устойчивые к атакам квантового компьютера?.....	253
Возможные пути решения .....	254
Семейства постквантовых примитивов.....	256
Lattice-based cryptography (ЛВ-криптография).....	257
Code-based cryptography (СВ-криптография).....	259
Multivariate polynomial cryptography (MQ- криптография).....	260
Hash-based cryptography (НВ-криптография).....	261
Альтернативные группы .....	262
6.5 Алгоритмы подписи, которые строятся на использовании хэш-функций.....	263
Конструкция HORS.....	263
Схема подписи Меркла.....	268
Семейство алгоритмов Sphincs .....	272
СЛОВАРЬ ТЕРМИНОВ.....	282
БЛАГОДАРНОСТИ .....	295
ОБ АВТОРАХ.....	296
ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ И ССЫЛКИ.....	298