

Евгений Хата Юрий Припачкин

БЛОКЧЕЙН ДЛЯ БАБУШКИ



ПАЛЪМИРА

Санкт-Петербург
2023

УДК 33
ББК 65
Х25

Хата Е. А., Припачкин Ю.И.

Х25 Блокчейн для бабушки за 60 минут / Евгений Хата, Юрий Припачкин — СПб. : ООО «Издательство «Пальмира» ; «Т8», 2023. — 84 с.
ISBN 978-5-519-60597-7

Что такое блокчейн? Что такое криптовалюта? Что такое приватный ключ и публичный адрес? Что такое майнинг? Что такое криптокошельки? Что такое форк? Можно ли убить блокчейн? Куда инвестировать?

Ответы на эти и другие вопросы вы найдете в данной книге. Чтение не займет много времени и заполнит необходимой информацией пробел в вашем криптообразовании.

Эта книга для того, кто хочет знать, как устроен блокчейн. Ведь она написана настолько просто и доступно, что понять ее сможет даже тот, кто раньше никогда не слышал о криптовалютах.

Узнайте о блокчейне за 60 минут!

УДК 33
ББК 65

© Е. А. Хата, Ю.И. Припачкин 2023
© Оформление.
ООО «Издательство «Пальмира»,
АО «Т8 Издательские Технологии», 2023

ISBN 978-5-519-60597-7

Очевидно, что с появлением компьютеров не могла не возникнуть мысль о том, чтобы перевести весь денежный учет и расчеты в электронный вид, создав электронные деньги - криптовалюту. Первым человеком, создавшим криптовалюту без централизованного управления и необходимости доверия третьим лицам стал в 2008 году Сатоши Накомото, разработавший протокол криптовалюты биткоин.

Но протокол сам по себе, на одном компьютере Сатоши, был почти бессмысленным явлением его личной фантазии. Нужна была технология фиксирования передачи точного кода с одного компьютера на другой и связи этих компьютеров в единую сеть, постоянно синхронно обновляющую события на разных компьютерах. Именно это взаимодействие компьютеров, сохраняющих единое представление об истории каждой записи, и есть блокчейн.

Блокчейн – это реестр цепочек информации, где каждая цепочка состоит из звеньев-блоков с данными о том, кому и когда принадлежало какое-либо право. Фактически, блокчейн – это «амбарная книга», защищенность которой обеспечивается тем, что она одновременно находится на очень многих компьютерах в одинаковом виде. Если попытаться изменить одно звено (блок) в общей истории, то посыплется вся структура реестра. То есть, по сути, блокчейн как технология

хранения и передачи информации может использоваться в очень разных областях. Криптовалюты – лишь одно из множества направлений, где может быть использована эта технология, фиксирующая право обладания и пользования определенной суммой ценности конкретным человеком. Расплачиваясь криптовалютой за товар или услугу, ее владелец вносит изменения в свою цепочку записей, тем самым фактически объявляя всему миру, что вот именно он передает столько-то монет другому лицу и этим заявлением передает этому другому лицу право распоряжаться переданными монетами.

Предлагаемая вашему вниманию книга ответит простым языком на сложные, как кажется многим, вопросы: что такое блокчейн и смарт-контракт, как создать криптовалюту, насколько выгодно быть сейчас майнером, появится ли в России крипторубль? Надеемся, что по итогам ее прочтения вы станете если не полноценным криптогуру, то точно сможете ориентироваться в новом цифровом пространстве.

*Юрий Припачкин,
президент Российской ассоциации криптоиндустрии
и блокчейна (РАКИБ)*

*Посвящается
всем бабушкам
Советского Союза*

СОДЕРЖАНИЕ

ПРОБЛЕМА ДЕНЕГ И ДОВЕРИЯ	10
Что такое деньги?	10
Децентрализованная денежная система	11
Золото как деньги.....	11
Что такое долговая расписка?.....	13
Централизованная денежная система	14
Что такое фиатные деньги?	14
Новая денежная система	17
БЛОКЧЕЙН И КРИПТОШИФРОВАНИЕ	19
Проблема двойного расхода	19
Что такое блокчейн?.....	20
Что такое криптовалюта?.....	21
Что такое приватный ключ и публичный адрес?	21
Что значит open source?	25
ЧТО ТАКОЕ МАЙНИНГ?	26
Что такое консенсус?	26
Роли в блокчейне	26
Шаги для достижения консенсуса	27
Что такое алгоритм консенсуса?	29
Proof of Work	29
Как подтверждаются транзакции?.....	30

Как найти nonce?	31
Структура блокчейна.....	32
Что такое хешрейт?	33
Проблема масштабирования блокчейна	34
Что такое SegWit?	35
Как можно решить вопрос	
о масштабировании?	35
Как появляется криптовалюта?	36
Можно ли заработать на майнинге?	37
Почему майнеры воруют блоки?	38
ЧТО ТАКОЕ ФОРК?	40
Форк	40
Что такое софт-форк?.....	41
Что такое хард-форк?.....	41
Что происходит с монетами	
в момент форка?	42
Пример Litecoin	43
Почему сложно создать форк?	45
Что такое блокчейн-атаки?	45
Атаки повторного воспроизведения.....	46
Атака Сивиллы.....	47
Атака 51%.....	47
Стоит ли опасаться атак?	47
ЧТО ТАКОЕ КРИПТОКОШЕЛЬКИ?.....	49
Холодные кошельки	49
Горячие кошельки	51
Что делать, если вы не знаете	
свой приватный ключ?	52

МОЖНО ЛИ УБИТЬ БЛОКЧЕЙН?	53
Что такое квантовые вычисления?	53
Государственное регулирование	
и запреты	54
Почему правительства	
не могут запретить криптовалюты?	56
Запретить Интернет	57
Где ахиллеса пята блокчейна?	58
Как быстро растет блокчейн?	59
ЧТО ТАКОЕ АНОНИМНОСТЬ	
В БЛОКЧЕЙНЕ?	61
Что такое анонимность?	61
Что такое приватность?	61
Что такое прозрачность?	62
Прозрачность + анонимность	62
КУДА СТОИТ ИНВЕСТИРОВАТЬ?	63
Bitcoin (BTC)	63
Кто такой Сатоши Накамото?	64
Прогноз стоимости биткойна	65
Что такое альткоины?	66
Ethereum-ETH	67
Что такое смарт-контракт?	67
Что такое EVM?	68
Прогноз стоимости Ethereum	68
Зачем нужен стандарт ERC20?	69
Litecoin-LTC	70
NEM, NEO, QTUM, Waves, Stratis	71