

Contents

Preface

Who this book is for

What this book covers

To get the most out of this book

Get in touch

1. Blockchain 101

The growth of blockchain technology.

Progress towards maturity.

Rising interest

Distributed systems

CAP theorem

PACELC theorem

The history of blockchain

Bitcoin

Electronic cash

Introducing blockchain

Blockchain architecture

Blockchain by layers

Blockchain in business

Generic elements of a blockchain

Blockchain functionality.

Benefits and features of blockchain

Limitations of blockchain technology.

Types of blockchain

Distributed ledgers

Shared ledger

Public blockchains

Private blockchains

Semi-private blockchains

Permissioned ledger

Fully private and proprietary blockchains

Tokenized blockchains

Tokenless blockchains

Layer 1 blockchains

Monolithic and polyolithic blockchains

Layer 2 blockchains

Sidechains

Summary

2. Decentralization

Introducing decentralization

Methods of decentralization

Disintermediation

Contest-driven decentralization

Quantifying decentralization

Benefits of decentralization

Evaluating requirements

Full-ecosystem decentralization

Storage

Communication

Computing power

Decentralization in practice

Smart contracts

Autonomous agents

Decentralized organizations

Decentralized autonomous organizations

Decentralized autonomous corporations

Decentralized autonomous societies

Decentralized applications

Criteria for a DApp

Operations of a DApp

Design of a DApp

Innovative trends

Decentralized web

Web 1

Web 2

Web 3

Summary

3. Symmetric Cryptography

Introducing cryptography

Services provided by cryptography

Cryptographic primitives

Keyless primitives

Random numbers

Hash functions

Symmetric key primitives

Message authentication codes

Secret key ciphers

Advanced Encryption Standard

Data Encryption Standard

How AES works

Encrypting and decrypting using AES

Summary

4. Asymmetric Cryptography

Foundational mathematics

Asymmetric cryptography

Public and private keys

Asymmetric cryptography algorithms

Integer factorization

Discrete logarithm

Elliptic curves

Integrated encryption scheme

Introducing RSA

Encrypting and decrypting with RSA

Introducing ECC

Mathematics behind ECC

Point addition

Point doubling

Point multiplication

The discrete logarithm problem

Generating keys with ECC

Digital signatures

RSA digital signature algorithms

Generating RSA digital signatures

The elliptic curve digital signature algorithm

Generating ECDSA digital signatures

Different types of digital signatures

Blind signatures

Multisignatures

Threshold signatures

Aggregate signatures

Ring signatures

Cryptographic constructs and blockchain technology

Homomorphic encryption

Secret sharing

Commitment schemes

Zero-knowledge proofs

zk-SNARKs

zk-STARKs

Zero-knowledge range proofs

Encoding schemes

Base64

base58

Verifiable random functions

Summary

5. Consensus Algorithms

Introducing consensus

Fault tolerance

FLP impossibility

Analysis and design

Model

Processes

Timing assumptions

Classification

Algorithms

CFT algorithms

Paxos

Raft

BFT algorithms

Practical Byzantine Fault Tolerance

Istanbul Byzantine Fault Tolerance

Tendermint

Nakamoto consensus

Variants of PoW

HotStuff

Choosing an algorithm

Finality

Speed, performance, and scalability

Summary

6. Bitcoin Architecture

Introducing Bitcoin

Cryptographic keys

Private keys in Bitcoin

Public keys in Bitcoin

Addresses

Typical Bitcoin addresses

Advanced Bitcoin addresses

Transactions

Coinbase transactions

The transaction lifecycle

Transaction validation

Transaction fees

The transaction data structure

Metadata

Inputs

Outputs

Verification

The Script language

Opcodes

Standard transaction scripts

Contracts

Transaction bugs

Blockchain

Structure

The genesis block

Stale and orphan blocks

Forks

Properties

Miners

Proof of Work (PoW)

Mining systems

CPU

GPU

FPGAs

ASICs

Mining pools

Network

Types of messages

Client software

Bloom filters

Wallets

Summary

7. Bitcoin in Practice

Bitcoin in the real world

Bitcoin payments

Innovation in Bitcoin

Bitcoin improvement proposals

Advanced protocols

Segregated Witness

Bitcoin Cash

Bitcoin Unlimited

Bitcoin Gold

Taproot

Extended protocols on top of Bitcoin

Colored coins

Counterparty

Altcoins from Bitcoin

Bitcoin client installation

Types of clients and tools

Setting up a Bitcoin node

Setting up the source code

Setting up bitcoin.conf

Starting up a node in the testnet

Starting up a node in regtest

Experimenting further with bitcoin-cli

Using the Bitcoin command-line tool

Using the JSON-RPC interface

Using the HTTP REST interface

Bitcoin programming

Summary

8. Smart Contracts

Introducing smart contracts

Definitions

Properties

Real-world application

Ricardian contracts

Smart contract templates

Oracles

Software-and network-assisted proofs

TLSNotary

TLS-N-based mechanism

Hardware device-assisted proofs

Android proof

Ledger proof

Trusted hardware-assisted proofs

Types of blockchain oracles

Inbound oracles

Outbound oracles

Cryptoeconomic oracles

Blockchain oracle services

Deploying smart contracts

The DAO

Advances in smart contract technology

Solana Sealevel

Digital Asset Modeling Language

Summary

9. Ethereum Architecture

Introducing Ethereum

Cryptocurrency

Keys and addresses

Accounts

Transactions and messages

MPTs

Transaction components

Recursive Length Prefix

Gas

Transaction types

Simple transactions

Contract creation transactions

Message call transactions

Messages

Transaction validation and execution

State and storage in the Ethereum blockchain

The world state

The account state

Transaction receipts

Ethereum virtual machine

Execution environment

The machine state

Blocks and blockchain

The genesis block

Block validation, finalization, and processing

Block difficulty mechanism

Nodes and miners

The consensus mechanism

Forks in the blockchain

The Ethereum network

Main net

Test nets

Private nets

Precompiled smart contracts

Programming languages

Solidity

Runtime bytecode

Opcodes

Wallets and client software

Wallets

Geth

Light clients

Supporting protocols

Whisper

Swarm

Summary

10. Ethereum in Practice

Ethereum payments

Innovations in Ethereum

Difficulty time bomb

EIP-1559

The merge and upcoming upgrades

Programming with Geth

Installing and configuring the Geth client

Creating a Geth new account

Querying the blockchain using Geth

Geth console

Geth attach

Geth JSON RPC API

Setting up a development environment

Connecting to test networks

Creating a private network

Starting up the private network

Experimenting with the Geth JavaScript console

Mining and sending transactions

Introducing Remix IDE

Interacting with the Ethereum Blockchain with MetaMask

Installing MetaMask

Creating and funding an account with MetaMask

Using MetaMask and Remix IDE to deploy a smart contract

Adding a custom network to MetaMask and connecting it with Remix IDE

Importing accounts into MetaMask using keystore files

Deploying a contract with MetaMask

Interacting with a contract through MetaMask using Remix IDE

Summary

11. Tools, Languages, and Frameworks for Ethereum Developers

Languages

The Solidity compiler

Installing solc

Experimenting with solc

Tools, libraries, and frameworks

Node.js

Ganache

ganache-cli

Ganache UI

Truffle

Drizzle

Other tools

Contract development and deployment

Writing smart contracts

Testing smart contracts

Deploying smart contracts

The Solidity language

Functions

Variables

Local variables

Global variables

State variables

Data types

Value types

Reference types

Control structures

Events

Inheritance

Libraries

Error handling

Summary

12. Web3 Development Using Ethereum

Interacting with contracts using Web3 and Geth

Deploying contracts

Using solc to generate ABI and code

Querying contracts with Geth

Interacting with Geth using POST requests

Interacting with contracts via frontends

Installing the web3.js JavaScript library

Creating a web3 object

Creating an app.js JavaScript file

Creating a frontend webpage

Calling contract functions

Creating a frontend webpage

Deploying and interacting with contracts using Truffle

Installing and initializing Truffle

Compiling, testing, and migrating using Truffle

Interacting with the contract

Using Truffle to test and deploy smart contracts

Deployment on decentralized storage using IPFS

Summary

13. The Merge and Beyond

Introduction

Ethereum after The Merge

The Beacon Chain

Beacon nodes

Consensus client

Execution client

Validator client

Proof-of-stake

P2P interface (networking)

The Merge

Sharding

The future roadmap of Ethereum

Summary

14. Hyperledger

Projects under Hyperledger

Distributed ledgers

Fabric

Sawtooth

Iroha

Indy

Besu

Libraries

Aries

Transact

Ursa

AnonCreds

Tools

Cello

Caliper

Domain-specific

Grid

Hyperledger reference architecture

Hyperledger design principles

Hyperledger Fabric

Key concepts

Membership service

Blockchain services

Smart contract services

APIs and CLIs

Components

Peers/nodes

Clients

Channels

World state database

Private data collections

Transactions

Membership Service Provider

Smart contracts

Crypto service provider

Applications

Chaincode implementation

The application model

Consensus mechanism

Transaction lifecycle

Fabric 2.0

New chaincode lifecycle management

New chaincode application patterns

Summary

15. Tokenization

Tokenization on a blockchain

Advantages of tokenization

Disadvantages of tokenization

Types of tokens

Fungible tokens

Non-fungible tokens

Stable tokens

Security tokens

Process of tokenization

Token offerings

Initial coin offerings

Security token offerings

Initial exchange offerings

Equity token offerings

Decentralized autonomous initial coin offering

Other token offerings

Token standards

ERC-20

ERC-223

ERC-777

ERC-721

ERC-884

ERC-1400

ERC-1404

ERC-1155

ERC-4626

Building an ERC-20 token

Building the Solidity contract

Deploying the contract on the Remix JavaScript virtual machine

Adding tokens in MetaMask

Emerging concepts

Tokenomics/token economics

Token engineering

Token taxonomy

Summary

16. Enterprise Blockchain

Enterprise solutions and blockchain

Success factors

Limiting factors

Requirements

Privacy

Performance

Access governance

Further requirements

Compliance

Interoperability

Integration

Ease of use

Monitoring

Secure off-chain computation

Better tools

Enterprise blockchain versus public blockchain

Enterprise blockchain architecture

Designing enterprise blockchain solutions

TOGAF

Architecture development method (ADM)

Blockchain in the cloud

Currently available enterprise blockchains

Enterprise blockchain challenges

Interoperability

Lack of standardization

Compliance

Business challenges

VMware Blockchain

Components

Consensus protocol

Architecture

VMware Blockchain for Ethereum

Quorum

Architecture

Nodes

Privacy manager

Cryptography

Privacy

Enclave encryption

Transaction propagation to transaction managers

Enclave decryption

Access control with permissioning

Performance

Pluggable consensus

Setting up a Quorum network with IBFT

Installing and running Quorum Wizard

Running a private transaction

Attaching Geth to nodes

Viewing the transaction in Cakeshop

Further investigation with Geth

Other Quorum projects

Remix plugin

Pluggable architecture

Summary

17. Scalability

What is scalability?

Blockchain trilemma

Methods for improving scalability

Layer 0 – multichain solutions

Polkadot

Layer 1 – on-chain scaling solutions

Layer 2 – off-chain solutions

Layer 2

Rollups

Data validity

Data availability

How rollups work

Types of rollups

Optimistic rollups

ZK-rollups

Technologies used for building ZK-rollups

ZK-ZK-rollups

Optimistic rollups vs ZK-rollups

Fraud and validity proof-based classification of rollups

Example

Layer 3 and beyond

Summary

18. Blockchain Privacy

Privacy

Anonymity

Confidentiality

Techniques to achieve privacy

Layer 0

Tor

I2P

Indistinguishability obfuscation

Homomorphic encryption

Secure multiparty computation

Trusted hardware-assisted confidentiality

Mixing protocols

CoinSwap

TumbleBit

Dandelion

Confidential transactions

MimbleWimble

Zkledger

Attribute-based encryption

Anonymous signatures

Zether

Privacy using Layer 2 protocols

Privacy managers

Privacy using zero-knowledge

Cryptographic Commitments

Zero-knowledge proofs

Building ZK-SNARKs

Example

Summary

19. Blockchain Security

Security

Blockchain layers and attacks

Hardware layer

Network layer

Blockchain layer

Attacks on transactions

Transaction replay attacks

Attacks on consensus protocols

Double-spending

Selfish mining

Forking and chain reorganization

Blockchain application layer

Smart contract vulnerabilities

DeFi attacks

Interface layer

Oracle attacks/oracle manipulation attacks

Attacks on wallets

Attacks on layer 2 blockchains

Cryptography layer

Attacking public key cryptography

Attacking hash functions

Key management-related vulnerabilities and attacks

ZKP-related attacks

Security analysis tools and mechanism

Formal verification

Formal verification of smart contracts

Model checking

Smart contract security

Oyente

Solgraph

Threat modeling

Regulation and compliance

Summary

20. Decentralized Identity

Identity

Digital identity

Centralized identity model

Federated identity model

Decentralized identity model

Self-sovereign identity

Components of SSI

Identity in Ethereum

Identity in the world of Web3, DeFi, and Metaverse

SSI-specific blockchain projects

Hyperledger Indy, Aries, Ursa, and AnonCreds

Other projects

Some other initiatives

Challenges

Summary

21. Decentralized Finance

Introduction

Financial markets

Trading

Exchanges

Orders and order properties

Order management and routing systems

Components of a trade

Trade lifecycle

Applications of blockchain in finance

Insurance

Post-trade settlement

Financial crime prevention

Payments

Decentralized finance

Properties of DeFi

DeFi layers

DeFi primitives

DeFi services

Asset tokenization

Decentralized exchanges

Flash loans

Derivatives

Money streaming

Yield farming

Insurance

Decentralized lending – lending and borrowing

Benefits of DeFi

Uniswap

Swap the token

Uniswap liquidity pool

Summary

22. Blockchain Applications and What's Next

Use cases

IoT

IoT architecture

The physical object layer

The device layer

The network layer

The management layer

The application layer

Benefits of IoT and blockchain convergence

Implementing blockchain-based IoT in practice

Setting up Raspberry Pi

Setting up the first node

Setting up the Raspberry Pi node

Installing Node.js

Building the electronic circuit

Developing and running a Solidity contract

Government

Border control

Elections

Citizen identification

Health

Media

Blockchain and AI

Some emerging trends

Some challenges

Summary

Index

Landmarks

Cover

Index