



BUILDING BLOCKCHAIN APPS

MICHAEL JUNTAO YUAN

Foreword by MARC FLEURY, founder of JBoss and Two Prime



Building Blockchain Apps

Building Blockchain Apps

Table of Contents

Cover

Title Page

Copyright Page

Contents

Foreword

Acknowledgments

About the Author

Part I: Introduction

1 An Introduction to Blockchain

The Blockchain

The Collaborative Ledger

Cryptocurrency

Smart Contracts

A Trustless Network

New Ways of Collaborating

The Fat Protocol

In Code We Trust

Conclusion

2 Reaching Consensus

What Is Blockchain Consensus?

Proof of Work (PoW)

Proof of Stake (PoS)

Delegated Proof of Stake (DPoS)

Table of Contents

Conclusion

3 Your First Blockchain App

Smart Contract

Front-End HTML

JavaScript and web3.js

In Action

Share Your Dapp

Conclusion

Part II: An Introduction to Ethereum

4 Getting Started

The BUIDL Way

Ethereum Mainnet

Ethereum Classic Mainnet

CyberMiles Mainnet

The Hard Way

Metamask Wallet

Remix

Web3

Conclusion

5 Concepts and Tools

Ethereum Wallet and Basic Concepts

Etherscan

The TestRPC

Interacting with Ethereum via GETH

Interacting with Ethereum via web3

Running an Ethereum Node

Running a Private Ethereum Network

Conclusion

6 Smart Contracts

Hello, World! Again

Table of Contents

Learning Smart Contract Programming

- Consensus vs. Nonconsensus Code
- Data Structures
- Function Parameters and Return Values
- Payable Functions
- Calling Other Contracts

Building and Deploying the Smart Contract

- Solidity Tools
- The BUIDL Integrated Development Environment (IDE)
- The Remix IDE
- Truffle Framework

Calling Smart Contract Functions

- The BUIDL IDE
- The Remix IDE
- GETH Console

A New Language

- More Smart Contract Languages

Conclusion

7 Decentralized Applications (Dapps)

Dapp Stack

- The web3 Library
- External Services

Dapp Showcases

- Uniswap
- CryptoKitties
- Gambling Games
- Interactive Dapps

Conclusion

8 Alternatives to Dapps

JavaScript

- The Full-Node Wallet
- Raw Transactions

Table of Contents

Python and Others

Conclusion

Part III: Ethereum in Depth

9 Inside Ethereum

What Is Blockchain State?

Ethereum State

Data Structure

Trie (or Tree)

Standard Trie

Patricia Trie

Similarities between the Trie and Patricia Trie

Main Difference between the Trie and Patricia Trie

Modified Merkle Patricia Trie

Trie Structure in Ethereum

State Trie : The One and Only

Storage Trie : Where the Contract Data Lives

Transaction Trie : One per Block

Concrete Examples of Tries in Ethereum

Analyzing the Ethereum Database

Get the Data

Decoding the Data

Read and Write the State LevelDB

Conclusion

10 Blockchain Data Services

Blockchain Explorers

Harvesting Data

Transactions and Accounts

Awards

Off-Chain Identities

Inside Smart Contracts

Query Interface

Table of Contents

SQL Query

JSON Query

GraphQL

Google BigQuery

Whats Next?

Conclusion

11 Smart Contract Search Engine

Introduction to the Smart Contract Search Engine

Getting Started with a Smart Contract Search Engine

The FairPlay Dapp Example

A Modular Architecture

Using the Smart Contract Search Engine

Use Cases

Crypto Assets

DeFi

Gaming

Conclusion

12 Smart Contract Security and Best Practices

Major Ethereum Smart Contract Hacks and Vulnerabilities

Decentralized Autonomous Organization Hack

BEC Token Hack

The Parity Wallet Hack

FOMO3D and LastWinner Dapp Hack

Unknowns and Beyond

Best Practices for Securing Smart Contracts

Expert Manual Auditing

Formal Verification

Sandbox

Tools

Conclusion

13 The Future of Ethereum

Table of Contents

Ethereum 1.0

- Privacy

- Consensus

- Scalability

- Token Improvements

Beyond Ethereum 1.0

- Sharding

- Zero-Knowledge Proofs

Ethereum 2.0

- The Beacon Chain

- eWASM

Delivery Phases of Ethereum 2.0

- Phase 0

- Phase 1

- Phase 2

PostEthereum 2.0 Innovation

- Conclusion

Part IV: Building Application Protocols

14 Extending the Ethereum Protocol

- Fully Compatible, Yet Faster

- Smart Enhancements to the EVM

 - Trusted Oracles

 - Secure Random Numbers

 - Alternative Gas Fees

- Safety First

- Conclusion

15 Extending Ethereum Tools

- Smart Contract Tools

 - Venus Wallet

 - Europa IDE

 - The lityc Compiler and Analysis Tool

Table of Contents

Dapp Tools

- web3-cmt

- CyberMiles App

Conclusion

16 Example Dapps

Case Study 1: Valentines

- The Valentines Smart Contract

- The JavaScript Dapp

Case Study 2: WeBet

- WeBet Smart Contract

- WeBet JavaScript Application

- Dapp Off-Chain Operations

Conclusion

17 Business Rules and Contracts

An Example

Rules Language

- Rete Algorithm

- Rule Attribute

- Rule Filters

- Rule Actions

- Rule Inheritance

- Working Memory

More Business Examples

- Insurance Claim

- Taxes

- Product Combos

Conclusion

18 Building an Application-Specific EVM

Using libENI Functions

- The String Reversing Example

- The RSA Example

Table of Contents

The Script Example

Writing a libENI Function

Parsing Arguments

Estimating Gas

Executing the Function

Mapping to libENI Function Name

Deploying the libENI Function

CyberMiles Governance

Conclusion

Part V: Building Your Own Blockchain

19 Getting Started with Tendermint

How It Works

It Works as Follows

Set Up a Node

Set Up a Network

Conclusion

20 The Business Logic

The Protocol

Consensus on the Block

Consensus on the Transactions

Getting Information

A Sample Application

Java Implementation

GO Implementation

The Cosmos SDK

Conclusion

21 Creating a Blockchain Client

Overview of the Approach

The Sample Application

PHP

Table of Contents

Java

Conclusion

Part VI: Cryptoeconomics

22 The Cryptoeconomics of Token Design

Network Utility Tokens

Bitcoin (BTC)

Ethereum (ETH)

ZCash (ZEC)

Application Utility Tokens

Security Tokens

The DAO

Token Funds

Token Valuation

Utility Tokens

Design Considerations

An Alternative Approach

Advanced Topics

Nonmonetary Pricing

Stable Coins

Conclusion

23 Initial Coin Offerings

A Brief History

Utility of an ICO

Facilitation of the Blockchain Project

Fundraising

ICO vs. Traditional Equity Financing

Entry Barrier to Investment

Entry Barrier to Fundraising

Regulation/Paperwork

Liquidity after Fundraiser

Community Participation

Table of Contents

Risk

Market Size

Evaluating an ICO Project

Project

Team

Fundraising Structure

Token Distribution Table

Community

Legal Framework

ICO Participation Risk

Hacking Risk

Project Development Risk

Team Risk

Conclusion

24 Cryptocurrency Exchanges

Exchange Types

Fiat Currency Exchanges

Tokens-Only Exchanges

Security Token Exchanges

Decentralization

Products and Services

Conclusion

A: Getting Started with CyberMiles

Index

