Blockchain Platforms

A Look at the Underbelly of Distributed Platforms

Synthesis Lectures on Computer Science

The Synthesis Lectures on Computer Science publishes 75–150 page publications on general computer science topics that may appeal to researchers and practitioners in a variety of areas within computer science.

Blockchain Platforms: A Look at the Underbelly of Distributed Platforms
Stijn Van Hijfte
July 2020

Analytical Performance Modeling for Computer Systems, Third Edition
Y.C. Tay
July 2018

Creating Autonomous Vehicle Systems
Shaoshan Liu, Liyun Li, Jie Tang, Shuang Wu, and Jean-Luc Gaudiot
October 2017

Introduction to Logic, Third Edition
Michael Genesereth and Eric J. Kao
November 2016

Analytical Performance Modeling for Computer Systems, Second Edition
Y.C. Tay
October 2013

Introduction to Logic, Second Editio
Michael Genesereth and Eric Kao
August 2013

Introduction to Logic
Michael Genesereth and Eric Kao
January 2013

Science Fiction Prototyping: Designing the Future with Science Fiction
Brian David Johnson
April 2011

Storing Clocked Programs Inside DNA: A Simplifying Framework for Nanocomputing
Jessica P. Chang, Dennis E. Shasha
April 2011

Analytical Performance Modeling for Computer Systems
Y.C. Tay
April 2010

The Theory of Timed I/O Automata
Dilsun K. Kaynar, Nancy Lynch, Roberto Segala, and Frits Vaandrager
2006

© Springer Nature Switzerland AG 2022
Reprint of original edition © Morgan & Claypool 2020

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations in printed reviews, without the prior permission of the publisher.

Blockchain Platforms: A Look at the Underbelly of Distributed Platforms
Stijn Van Hijfte

ISBN: 978-3-031-00676-0 paperback
ISBN: 978-3-031-01804-6 ebook
ISBN: 978-3-031-00072-0 hardcover

DOI 10.1007/978-3-031-01804-6

A Publication in the Springer series
SYNTHESIS LECTURES ON COMPUTER SCIENCE
Lecture #11

Series ISSN 1932-1228 Print 1932-1686 Electronic

Blockchain Platforms

A Look at the Underbelly of Distributed Platforms

Stijn Van Hijfte, Howest Applied University College

SYNTHESIS LECTURES ON COMPUTER SCIENCE #11

ABSTRACT

This book introduces all the technical features that make up blockchain technology today. It starts with a thorough explanation of all technological concepts necessary to understand any discussions related to distributed ledgers and a short history of earlier implementations. It then discusses in detail how the Bitcoin network looks and what changes are coming in the near future, together with a range of altcoins that were created on the same base code. To get an even better idea, the book shortly explores how Bitcoin might be forked before going into detail on the Ethereum network and cryptocurrencies running on top of the network, smart contracts, and more. The book introduces the Hyperledger foundation and the tools offered to create private blockchain solutions. For those willing, it investigates directed acyclic graphs (DAGs) and several of its implementations, which could solve several of the problems other blockchain networks are still dealing with to this day. In Chapter 4, readers can find an overview of blockchain networks that can be used to build solutions of their own and the tools that can help them in the process.

KEYWORDS

Blockchain, distributed ledger, DAG, Bitcoin, Ethereum, Iota, Hyperledger

Contents

Introduction .... **xvii**

1 Underlying Concepts and Technologies **1**

1.1 Hash functions 1

1.2 eCash 3

1.3 Hashcash 3

1.3.1 The Hashcash Cost Function 3

1.4 B-money 6

1.5 Peer-to-Peer 6

1.6 Distributed Hash Table 10

1.7 Decentralized vs. Distributed 10

1.7.1 SHA-256 11

1.8 Merkle Tree 16

1.8.1 Merkle Patricia Tree 17

1.8.2 Bloom Filters 17

1.9 State Machine 19

1.9.1 Turing Machine 19

1.10 Elliptical Curve Cryptography 20

1.11 Byzantine Generals Problem 24

1.11.1 Double Spend Problem 26

1.11.2 CAP Theorem 27

1.11.3 SPECTRE and the Condorcet Paradox 27

1.11.4 Fermat's Little Theorem 28

1.11.5 Pedersen Commitments 28

1.11.6 Fungibility and Liveness 28

1.11.7 Transaction and Settlement Finality 30

1.11.8 Censorship Resistance 31

1.11.9 Winternitz One-Time Signatures 32

1.12 What Is Blockchain? 32

1.12.1 Foundations 32

1.12.2 Building "Blocks" 33

1.12.3 Blockchain or Distributed Ledger? 36

1.12.4 Blockchain Address . . . 37
1.12.5 Blockchain Wallet . . . 39
1.12.6 Node . . . 40
1.12.7 Mining . . . 41
1.12.8 Merge Mining . . . 42
1.13 Block Time . . . 43
1.14 The Consensus Protocol . . . 44
1.15 Round Robin . . . 44
1.16 Proof of Work . . . 45
1.17 Nakamoto Consensus . . . 45
1.18 Proof of Stake . . . 46
1.19 Delegated Proof of Stake . . . 46
1.20 Proof of Authority . . . 46
1.21 PBFT . . . 47
1.22 The Cuckoo Cycle . . . 48
1.23 DECOR+HOP . . . 48
1.24 GHOST—SPECTRE—PHANTOM . . . 49
1.25 Ethash Algorithm and Dagger Hashimoto . . . 51
1.26 Keccak256 / SHA3 . . . 52
1.27 Other Protocols Used in Blockchain Platforms . . . 53
1.28 Nonce . . . 54
1.29 Blockchain Forks . . . 55
1.30 Sidechains . . . 56
1.31 Blockchain Execution Engine . . . 59
1.32 Serialization . . . 60
1.33 The Blockchain Technology Stack . . . 60
1.34 DAG—Directed Acyclic Graph . . . 61
1.34.1 MerkleDAG . . . 62
1.34.2 BlockDAG . . . 62
1.35 Blockchain-Specific Attacks . . . 63
1.35.1 Virtual Machines . . . 68
1.35.2 Smart Contracts . . . 68
1.35.3 Wallets . . . 68
1.35.4 Other Attacks . . . 69

2 Bitcoin . . . 71

2.1 How Does Bitcoin Work? . . . 71

2.2 The Bitcoin Blockchain: The Network 72

2.3 Bitcoin Blocks 75

2.4 Bitcoin Transactions 79

2.5 Bitcoin Signing and Verification 83

2.6 UTXO 84

2.6.1 Timelocks 86

2.7 Bitcoin Serialization 87

2.8 Bitcoin Script 89

2.8.1 Ivy for Bitcoin 90

2.9 Bitcoin Miniscript 92

2.10 Bitcoin Addresses 94

2.10.1 Encrypted Private Keys (BIP-38) 96

2.11 Bitcoin Wallet 96

2.12 Simplified Payment Verification 98

2.12.1 SPV Wallet Client 99

2.13 Segregated Witness 99

2.14 Bitcoin Improvement Proposals 101

2.15 Schnorr Signatures 101

2.16 Taproot, G'root, and Graftroot 102

2.17 Bitcoin Mining 104

2.18 Bitcoin Relay Networks 105

2.19 Bitcoin: The Cryptocurrency 105

2.20 Payment Channels on Bitcoin 106

2.20.1 Nakamoto High-Frequency Transactions 106

2.20.2 Spillman-Style Payment Channels 107

2.20.3 CLTV-Style Payments 107

2.20.4 Poon-Dryja Payment Channels 107

2.20.5 Decker-Wattenhofer Duplex Payment Channels 107

2.20.6 Decker-Russell-Osuntokun Eltoo Channels 108

2.20.7 Hashed Time-Locked Contracts or HTLCs 108

2.20.8 Transaction Malleability 108

2.21 Wasabi Wallet and Zerolink 109

2.22 Meta-Coin Platforms on Top of Bitcoin: Colored Coins 110

2.23 OpenAssets Protocol 110

2.24 Bitcoin 2.0 112

2.25 Bitcoin Hivemind 112

2.26 The Mimblewimble Protocol 114

2.27 The Elements Project 116
2.28 Siacoin 117
2.29 The Counterparty Protocol 118
2.30 Drop Zone 118
2.31 Omni Protocol 119
2.32 Lightning Network 120
2.33 Liquid Network 122
2.34 Rootstock 122
2.35 Zcash 124
2.35.1 Zk-SNARKs 125
2.35.2 Zk-STARKs 130
2.36 Zcash and HAWK 131
2.37 Hard Forks 131
2.38 Bitcoin XT 132
2.39 Bitcoin Classic 132
2.40 Bitcoin Unlimited 132
2.41 Bitcoin Cash 133
2.42 Bitcoin SV 134
2.43 Bitcoin Gold . . . . .
134
2.44 Bitcoin Diamond 134
2.45 Bitcoin Interest 135
2.46 Bitcoin Private 135
2.47 How to Fork Bitcoin 135
2.48 Altcoins Based on Bitcoin 141
2.49 Litecoin 141
2.50 Dash 142
2.51 Namecoin 143
2.52 Dogecoin 144
2.53 Ravencoin 144
2.54 Peercoin 145
2.55 Gridcoin 145
2.56 Primecoin 146

3 Ethereum 147
3.1 The Ethereum Virtual Machine 148
3.2 Network Communication in Ethereum 150

3.3 Blocks and Chains 151
3.4 GHOST Protocol 154
3.5 UTXOs? 155
3.6 Transactions 156
3.7 Serialization 157
3.8 Signing 158
3.9 Ether, Fees, Gas, and Fuel 158
3.10 The Milestones of Ethereum 160
3.11 The Stages of Ethereum Explained 160
3.12 Frontier 161
3.13 Ice Age 161
3.14 Homestead 162
3.15 DAO 162
3.16 The DAO Attack 163
3.17 Tangerine Whistle 163
3.18 Spurious Dragon 163
3.19 Metropolis Byzantium 164
3.20 Metropolis Constantinople 164
3.21 Serenity 165
3.21.1 Phase 0 165
3.21.2 Phase 1 166
3.21.3 Phase 2 167
3.21.4 Phase 3 167
3.21.5 Phases 4, 5, and 6 167
3.21.6 Ethereum 3.0 168
3.22 Scalability and the Casper Protocol 168
3.22.1 State Channels 168
3.22.2 Plasma 168
3.23 The Casper Protocol 169
3.23.1 Safety Oracles 170
3.24 Smart Contracts 170
3.25 Blockchain Oracles 172
3.26 DApps 172
3.27 Decentralized and Autonomous 173
3.28 Web 3.0 174
3.28.1 Ethereum Whisper 175
3.28.2 Ethereum Swarm 176

3.28.3 IPFS 177
3.28.4 Libp2p 179
3.28.5 IPLD 179
3.28.6 Multiformats 179
3.28.7 0x Protocol 180
3.28.8 Dat Protocol 180
3.28.9 Cryptocurrency Implementations on Ethereum 185
3.28.10 EIP 20: ERC-20 Token Standard 185
3.28.11 ERC-223 186
3.28.12 ERC-721 187
3.28.13 ERC-777 187
3.28.14 ERC-827 188
3.28.15 ERC-664 188
3.28.16 ERC-677 188
3.29 Ethereum Classic 188

4 Hyperledger and DAGs 191
4.1 Hyperledger 191
4.1.1 Hyperledger Besu 192
4.1.2 Hyperledger Burrow 192
4.1.3 Hyperledger Fabric 193
4.1.4 Hyperledger Grid 194
4.1.5 Hyperledger Indy 194
4.1.6 Hyperledger Iroha 194
4.1.7 Hyperledger Sawtooth 195
4.1.8 Hyperledger Aries 195
4.1.9 Hyperledger Avalon 195
4.1.10 Hyperledger Cactus 196
4.1.11 Hyperledger Caliper 196
4.1.12 Hyperledger Cello 196
4.1.13 Hyperledger Composer 196
4.1.14 Hyperledger Explorer 197
4.1.15 Hyperledger Quilt 197
4.1.16 Hyperledger Transact 197
4.1.17 Hyperledger Ursa 197
4.2 Digital Asset 198
4.3 Iota 198

4.4 Hedera Hashgraph 204
4.5 Fantom 204
4.6 Other Public and Private Platforms 205
4.7 Monero 205

5 Some Final Remarks 209

Bibliography 211

Author Biography 225

Introduction

Why another book on blockchain? I asked myself the same question when I started to write this very line. The reason is actually quite simple. By this point, everyone seems to have heard of blockchain in one way or another. But it is clear to me that, on average, not one person really understands the core concepts or really knows what it was all about. Others had deep knowledge but either only of the core concepts or of one specific platform. Theory and personal perception are the core of the information and many of the sources I scoured from all over the world all seemed to be limited. Not bad, just limited. They all brought only a small piece of the puzzle that I had to try to form myself.

This book attempts to give an extensive explanation of the core concepts and explain several platforms. Do I want to create a training manual that explains each platform in excruciating detail? No. However, this book should at least show you how these platforms generally work and, upon your choosing, allow you to investigate certain platforms in more detail on your own. All of the information is out there; it is up to you to go out and explore!