The Science of the Blockchain

Roger Wattenhofer

Contents

1 Introduction **1**
1.1 What are Distributed Systems? 1
1.2 Book Overview 2

2 Fault-Tolerance & Paxos **5**
2.1 Client/Server 5
2.2 Paxos 10

3 Consensus **17**
3.1 Two Friends 17
3.2 Consensus 18
3.3 Impossibility of Consensus 18
3.4 Randomized Consensus 25
3.5 Shared Coin 29

4 Byzantine Agreement **33**
4.1 Validity 34
4.2 How Many Byzantine Nodes? 35
4.3 The King Algorithm 38
4.4 Lower Bound on Number of Rounds 40
4.5 Asynchronous Byzantine Agreement 40

5 Authenticated Agreement **45**
5.1 Agreement with Authentication 45
5.2 Zyzzyva 47

6 Quorum Systems **61**
6.1 Load and Work 62
6.2 Grid Quorum Systems 64
6.3 Fault Tolerance 66
6.4 Byzantine Quorum Systems 70

7 Eventual Consistency & Bitcoin 77

7.1 Consistency, Availability and Partitions 78

7.2 Bitcoin 79

7.3 Smart Contracts 87

7.4 Weak Consistency 91

8 Distributed Storage 95

8.1 Consistent Hashing 95

8.2 Hypercubic Networks 97

8.3 DHT & Churn 105