1. Record Nr. UNINA9910586579703321

Autore	Gramoli Vincent
Titolo	Blockchain scalability and its foundations in distributed systems / / Vincent Gramoli
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	9783031125782 9783031125775
Descrizione fisica	1 online resource (133 pages)
Disciplina	005.74
Soggetti	Blockchains (Databases)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- Chapter 1 Introduction -- Chapter 2 Consensus in Blockchain -- 2.1 A Brief History -- 2.2 What is Blockchain? -- 2.2.1 The blockchain abstraction as a directed acyclic graph -- 2.2.2 Signed transactions -- 2.2.3 Distributed implementation of the blockchain abstraction -- 2.3 Double spending -- 2.3.1 Forks as disagreements on the blocks at a given index -- 2.3.2 From forks to double spending -- 2.3.3 How to avoid forks? -- 2.4 Conclusion -- 2.5 Bibliographic notes -- 2.6 Exercises -- References -- Chapter 3 Blockchain Fundamentals -- 3.1 Introduction -- 3.2 Failures and communication -- 3.3 Properties of consensus -- 3.4 Impossibility to solve consensus in asynchronous networks -- 3.4.1 Failure detectors -- 3.4.2 Randomized consensus -- 3.4.3 Deterministic termination -- 3.4.4 Additional synchrony -- 3.4.5 Impossibility to solve consensus with too many failures -- 3.5 Proof of work and mining -- 3.5.1 Proposing to the consensus -- 3.5.2 Decided blocks and committed transactions -- 3.6 Resolving forks -- 3.7 The 51% Attack -- 3.8 The GHOST protocol -- 3.9 Conclusion -- 3.10 Bibliographic notes -- 3.11 Exercises -- References -- Chapter 4 Consensus Fundamentals -- 4.1 Introduction -- 4.2 Consensus without failures -- 4.2.1 Consensus algorithm without failures and with synchrony -- 4.2.2 Correctness of the consensus algorithm without failures -- 4.2.3 Complexities of the consensus algorithm without

failures -- 4.3 Consensus with crash failures -- 4.3.1 Correctness of the consensus algorithm with crash failures -- 4.3.2 Complexity of the consensus algorithm with crash failures -- 4.4 Consensus with Byzantine failures -- 4.4.1 The problem of consensus with Byzantine failures -- 4.4.2 The EIG algorithm -- 4.4.3 Example with n = 4 and f = 1 -- 4.4.4 Complexity of the EIG algorithm -- 4.5 Conclusion. 4.6 Bibliographic notes -- 4.7 Exercises -- References -- Chapter 5 Making Blockchains Secure -- 5.1 Introduction -- 5.2 Beyond synchrony -- 5.3 The Balance Attack -- 5.4 Double spending in Ethereum -- 5.4.1 Double spending is easy in case of route hijacking -- 5.4.2 Partitioning Ethereum mining pools turns out to be hard -- 5.5 Proof-of-Authority and permissioned sealers of Ethereum -- 5.5.1 The Aura algorithm -- 5.5.2 The Attack of the Clones -- 5.6 Accountability -- 5.7 Conclusion -- 5.8 Bibliographic notes -- 5.9 Exercises -- References -- Chapter 6 Making Blockchains Scale -- 6.1 Introduction -- 6.2 Consensus without synchrony -- 6.2.1 The seminal Practical Byzantine Fault Tolerance -- 6.2.2 Complexities -- 6.2.3 Changes required by the scale of the consensus network -- 6.3 Leveraging bandwidth -- 6.3.1 The time complexity of a leader-based propagation -- 6.3.2 The time complexity of a leaderless propagation -- 6.3.3 Bypassing the leader bottleneck with the superblock optimization -- 6.4 The Set Byzantine Consensus problem -- 6.5 Democratic Byzantine fault tolerance -- 6.5.1 The binary Byzantine consensus problem -- 6.5.2 The binary Byzantine consensus algorithm of DBFT -- 6.5.3 Safety proof of the binary Byzantine consensus -- 6.6 Red Belly Blockchain -- 6.6.1 Reducing the computation at small scale -- 6.6.2 Leveraging bandwidth at larger scales -- 6.6.3 Assigning roles to nodes -- 6.6.4 From DBFT to Red Belly Blockchain -- 6.6.5 Binary Byzantine consensus of RBBC -- 6.6.6 Proof of Correctness -- 6.7 Conclusion -- 6.8 Bibliographic notes -- 6.9 Exercises -- References -- Chapter 7 Concluding Remarks -- References -- Chapter 8 Glossary.