Table of Contents

Blockchain: a Janus Bifrons Looking at the Past and the Future XI

Introduction 1

1 What is the Blockchain? 5
1. Blockchain: the background history 5
   1982: Ecash (David Chaum) 6
   1997: Hashcash (Adam Back) 6
   1998: B-money (Wei Dai) 7
   1998: Bit Gold (Nick Szabo) 7
   1999: Auditable, anonymous Ecash (Tomas Sander, Amnon Ta-Shma) 7
   2008: Bitcoin (Satoshi Nakamoto) 8
2. The Blockchain: definition and technical pillars 8
   Distributed network 9
   Advanced cryptography 11
   Data architecture 14
   Decentralized consensus 15
3. The blockchain tools 17
   Digital tokens 17
   Smart contracts 18

2 Blockchain Dimension Analysis 21
1. Approach 21
2. Governance aspects: types of blockchain from the ownership perspective 23
3. Technical aspects: protocol independence 24
4. Technical aspects: decentralized consensus 26
   Practical Byzantine Fault Tolerance (PBFT) 27

Proof-of-Work algorithm (PoW) 29
Proof-of-Stake algorithm (PoS) 31
Federated Byzantine Agreement (FBA) 33
Proof of Elapsed Time (PoET) 35
An analytical comparison of the main consensus algorithms 36
5. Blockchain – applications 38

3 Blockchain Applications 41
1 Cryptocurrency 42
2. Data certification 44
3. Digital advertisement 48
4. Digital identity 49
5. Digital voting and governance 50
6. Energy management and distribution 51
7. Financial payments platform 52
8. Gaming 55
9. IoT platform 57
10. P2P content distribution 59
11. P2P resource distribution 61
12. Prediction markets 63
13. Smart contract platform 64

4 Market Overview 67
1. Background 67
2. Cryptocurrency – permissionless use cases 69
Focus: bitcoin protocol 69
Other permissionless use cases 73
3. Data certification – permissionless use cases 75
4. Digital advertisement – permissionless use cases 78
5. Digital identity – permissionless use cases 80
6. Digital voting & governance – permissionless use cases 82
7. Energy management & distribution – permissionless use cases 84
8. Financial payments platform – permissionless use cases 86
9. Gaming – permissionless use cases 89
10. IoT platform – permissionless use cases 92
11. P2P content distribution – permissionless use cases 95
12. P2P resource distribution – permissionless use cases 98
13. Prediction markets – permissionless use cases 101
14. Smart contract platform – permissionless use cases 104

Focus: the Ethereum protocol 104
Other permissionless use cases 107

5. Blockchain Business Implications 109
1. Blockchain as a new IT architecture: description and business implications 109
Blockchain business model continuum 114
2. Decision making framework 117

6. Conclusions 119

Acknowledgments 123

Bibliography 125