



Table of Contents

1	Introduction to Blockchain	1
1.1	What is Blockchain and Why it is Important for Us	1
1.2	Applications based on Blockchain Technology	3
1.2.1	Industry and Enterprise	4
1.2.2	Financial Services	5
1.2.3	Government Services	7
1.3	Blockchain Functionality	7
1.3.1	Blockchain as Data Storage	8
1.3.2	Blockchain as a Computational Infrastructure	10
1.4	Blockchain and its Non-functional Properties	10
1.4.1	Non-functional Properties and Requirements of the Blockchain	10
1.4.2	Non-functional Properties of the Blockchain	11

1.5	Blockchain Architecture Design	12
1.5.1	Software Architecture: Design and Analysis	12
1.5.2	Designing Blockchain-based Application	12
1.6	Summary	14
1.7	References	14
2	Existing Blockchain Platforms	16
2.1	Bitcoin	16
2.1.1	Bitcoin Transactions	18
2.1.2	Script	19
2.1.3	Mining	19
2.1.4	Accounts and States	20
2.1.5	Nakamoto Consensus	21
2.1.6	Deflationary Cryptocurrency	21
2.1.7	Wallets	22
2.1.8	Exchanges	22
2.2	Ethereum	22
2.2.1	Ethereum Protocol	23
2.2.2	Ethereum Transactions	23
2.2.3	Smart Contract	24
2.2.4	Paying Fees in 'Gas'	24
2.2.5	Decentralized Applications (dapp)	25
2.3	Hyperledger Fabric	25
2.3.1	Permissioned Blockchain	26
2.3.2	Chaincode as the Smart Contract	27
2.3.3	Nodes	27
2.3.4	Transactions	27
2.3.5	Consensus	28
2.4	Other Representative Blockchain Platforms	28
2.5	References	29
3	Varieties of Blockchains	30
3.1	Blockchain Fundamental Properties	30
3.2	Configuration of Block	37
3.3	Auxiliary Blockchains	39
3.4	References	42

4	Agricultural Supply Chain	44
4.1	Introduction	44
4.2	Conventional Technology	45
4.2.1	The Methodology of Supply Chain	45
4.2.2	The Blockchain Solution	46
4.2.3	Discussion of Requirements and Properties Which are Non-functional	47
4.3	Open Data Registry	47
4.3.1	Conventional Technology	48
4.3.2	The blockchain Solution	49
4.3.3	Discussion of Requirements and Properties Which are Non-functional	49
4.4	International Money Transfers	50
4.4.1	Conventional Methods	51
4.4.2	Blockchain Method	52
4.4.3	Discussion of Requirements and Properties Which are Non-functional	53
4.5	Continuous Reporting and Electricity Contract Selection	54
4.5.1	Non-functional Requirements of the Key	54
4.5.2	Conventional Technologies	55
4.5.3	Blockchain Solution and Design	55
4.5.4	Non-functional Properties	56
4.6	References	56
5	Blockchain in Software Architecture	58
5.1	Introduction	58
5.2	Blockchain as an Architectural Element	59
5.3	Blockchain as a Storage Element	60
5.3.1	Comparing with Centralized Databases	61
5.3.2	Comparing with Peer-to-Peer Data Storage	62
5.3.3	Comparing with Cloud Services	62
5.3.4	Comparing with Replicated State Machines	63
5.4	Blockchain as a Computational Element	63
5.5	Blockchain as a Communication Mechanism	64
5.5.1	Data Communication	65
5.5.2	Computation Communication	66
5.6	Blockchain as an Asset Management and Control Mechanism	67

5.7	Integration of Blockchain into a System as a Component	68
5.8	Summary	70
5.9	References	70
6	Designing Process for Application on Blockchain	72
6.1	Introduction	72
6.2	Suitability Evaluation	73
6.2.1	Multi-party	73
6.2.2	Trustworthy Authority	74
6.2.3	Immutability of Data and Non-repudiation	75
6.2.4	Operation	76
6.2.5	High-level Performance	76
6.2.6	Transparency	77
6.3	Examples for Suitability Evaluation	77
6.3.1	Example 1: Electronic Health Records (EHR)	78
6.3.2	Example 2: Chain of Supply	78
6.3.3	Example 3: Stock Market	79
6.3.4	Example 4: Identity Management	80
6.4	Design Process for Blockchain Systems	80
6.4.1	Trade-off Analysis	81
6.4.2	Decentralization	82
6.4.3	Off-chain Vs. On-chain Transactions	83
6.5	Summary	84
6.6	References	84
7	Patterns of Blockchain	86
7.1	Introduction	86
7.2	Patterns on Interaction with the External World	87
7.2.1	Oracle	87
7.2.2	Reverse Oracle	89
7.2.3	Legal and Smart Contract	90
7.3	Data Management Patterns	91
7.3.1	On-chain Data Encryption	91
7.3.2	Tokenization	93
7.3.3	Off-chain Data Storage	94
7.3.4	State Channel	95
7.4	Security Patterns	96
7.5	Multiple Authorization	96

7.5.1	Off-chain Secret Dynamic Authorization	97
7.6	Contract Structural Pattern	98
7.6.1	Registration of Contract	98
7.6.2	Data Contract	99
7.6.3	Embedded Permission	99
7.6.4	Execution of Incentive	99
7.7	References	100
8	Model Driven Engineering for Blockchain Applications	101
8.1	Introduction	101
8.2	Model Driven Generation of Smart Contract Code for Collaborative Business Processes	103
8.3	Model Driven Registry Generation for Blockchain	109
8.4	Summary	114
8.5	References	115
9	Cost	116
9.1	Introduction	116
9.2	On-chain Data Cost	117
9.3	Smart Contract Cost	119
9.4	Cost Models	120
9.5	Using and Evaluating the Cost Model	126
9.6	Discussion	130
9.7	Summary	131
9.8	References	131
10	Performance	133
10.1	Introduction	133
10.2	Performance Characteristics of Blockchain	133
10.3	Architectural Process Modeling	136
10.4	Prediction of the Latency of Blockchain-Based Systems	136
10.5	Architectural Decision Making	143
10.6	Summary	147
10.7	References	148
11	Blockchain Applications and its Security and Dependability	151
11.1	Confidentiality	151

11.2	Integrity	153
11.3	Reliability and Availability	154
11.4	Safety	156
11.5	Maintainability	157
11.6	Blockchain Transaction Inclusion and its Variation	159
11.7	Retrying and Aborting Transactions of Blockchain	161
11.8	Summary	162
11.9	References	163

12 AgriDigital Case Study 164

12.1	Supply Chains for Agriculture and its Blockchain Solution	164
12.1.1	Agricultural Supply Chains Worldwide	165
12.1.2	Agriculture and Blockchain	166
12.2	Vision for AgriDigital Sector	167
12.3	AgriDigital Vision's Pillars of Digital Trust	169
12.3.1	Blockchain Solution for AgriDigital Industry	169
12.4	Business Use Case Designs	170
12.5	Case Study: Pilot Components	172
12.5.1	Scenarios for Pilot	172
12.5.2	Decisions for Design	173
12.6	Summary	176
12.7	References	177

13 Blockchain Voting 178

13.1	Introduction	178
13.2	The Minimum Viable Product (MVP) Prototype	180
13.3	Construction of Tokenvote	183
13.4	Details of the Secure Vote system	186
13.5	Summary	189
13.6	References	190

14 Blockchain Traceability 192

14.1	Introduction	192
14.2	OriginChain Architecture	194
14.3	Analysis	199
14.4	Discussion	202
14.5	Summary	204
14.6	References	204

Index 206