

# Contents

<b>I</b>	<b>BLOCKCHAIN TECHNOLOGY</b>	<b>17</b>
<b>1</b>	<b>Blockchain Concepts</b>	<b>19</b>
<b>1.1</b>	<b>Blockchain</b>	<b>20</b>
1.1.1	Blockchain Evolution	21
1.1.2	Blockchain Structure	22
1.1.3	Blockchain Characteristics	22
<b>1.2</b>	<b>Blockchain Application Example: Escrow</b>	<b>23</b>
<b>1.3</b>	<b>Blockchain Stack</b>	<b>35</b>
1.3.1	Decentralized Computation Platform - Ethereum	37
1.3.2	Decentralized Storage Platform - Swarm	39
1.3.3	Decentralized Messaging Platform - Whisper	39
1.3.4	Smart Contracts	39
1.3.5	Decentralized Applications (Dapps)	40
1.3.6	Tools & Interfaces	41
<b>1.4</b>	<b>From Web 2.0 to the Next Generation Decentralized Web</b>	<b>42</b>
<b>1.5</b>	<b>Domain Specific Blockchain Applications</b>	<b>44</b>
1.5.1	FinTech	44
1.5.2	Internet of Things	46
1.5.3	Industrial & Manufacturing	48
1.5.4	Registry of Assets & Inventory	52
1.5.5	Energy	52
1.5.6	Supply Chain & Logistics	52

1.5.7	Records & Identities .....	53
1.5.8	Healthcare .....	55
<b>1.6</b>	<b>Blockchain Benefits &amp; Challenges</b>	<b>57</b>
<b>1.7</b>	<b>Summary</b>	<b>59</b>
<b>2</b>	<b>Blockchain Application Templates .....</b>	<b>61</b>
<b>2.1</b>	<b>Blockchain Application Components</b>	<b>62</b>
<b>2.2</b>	<b>Design Methodology for Blockchain Applications</b>	<b>63</b>
<b>2.3</b>	<b>Blockchain Application Templates</b>	<b>67</b>
2.3.1	Many-to-One .....	67
2.3.2	Many-to-One for IoT Applications .....	68
2.3.3	Many-to-Many or Peer-to-Peer .....	68
2.3.4	One-to-One for Financial Applications .....	68
<b>II</b>	<b>BLOCKCHAIN COMPONENTS &amp; APPLICATIONS</b>	<b>71</b>
<b>3</b>	<b>Setting up Ethereum Development Tools .....</b>	<b>73</b>
<b>3.1</b>	<b>Ethereum Clients</b>	<b>74</b>
3.1.1	Go-Ethereum Client (geth) .....	74
3.1.2	Python Ethereum Client (pyethapp) .....	79
<b>3.2</b>	<b>Ethereum Languages</b>	<b>81</b>
3.2.1	Solidity .....	81
<b>3.3</b>	<b>TestRPC</b>	<b>82</b>
<b>3.4</b>	<b>Mist Ethereum Wallet</b>	<b>83</b>
<b>3.5</b>	<b>MetaMask</b>	<b>85</b>
<b>3.6</b>	<b>Web3 JavaScript API</b>	<b>88</b>
<b>3.7</b>	<b>Truffle</b>	<b>92</b>
<b>4</b>	<b>Ethereum Accounts .....</b>	<b>97</b>
<b>4.1</b>	<b>Ethereum Accounts</b>	<b>98</b>
4.1.1	Externally Owned Account (EOAs) .....	98
4.1.2	Contract Account .....	98
<b>4.2</b>	<b>Keypairs</b>	<b>98</b>
<b>4.3</b>	<b>Working with EOA Accounts</b>	<b>100</b>
4.3.1	Creating Account .....	100
4.3.2	Listing Accounts .....	101
4.3.3	Updating Accounts .....	102
4.3.4	Checking Balance .....	103

4.3.5	Account Transactions	103
<b>4.4</b>	<b>Working with Contract Accounts</b>	<b>106</b>
4.4.1	Compiling & Deploying Contract	106
4.4.2	Interacting with Contracts	113
4.4.3	Instantiating or Watching a Contract	114
<b>5</b>	<b>Smart Contracts</b>	<b>117</b>
<b>5.1</b>	<b>Smart Contract</b>	<b>118</b>
<b>5.2</b>	<b>Structure of a Contract</b>	<b>118</b>
<b>5.3</b>	<b>Setting up and Interacting with a Contract using Geth Client</b>	<b>118</b>
5.3.1	Compiling & Deploying a Contract	120
5.3.2	Transactions and Calls	127
5.3.3	Interacting with a Contract	129
5.3.4	Gas	130
5.3.5	Logs	131
5.3.6	Events	132
<b>5.4</b>	<b>Setting up and Interacting with a Contract using Mist Wallet</b>	<b>135</b>
5.4.1	Compiling & Deploying a Contract	137
5.4.2	Interacting with a Contract	138
<b>5.5</b>	<b>Smart Contract Examples</b>	<b>146</b>
5.5.1	Event Registration Contract	146
5.5.2	Voting Contract	151
5.5.3	Name Registry Contract	155
5.5.4	IoT Smart Switch Contract	159
<b>5.6</b>	<b>Smart Contract Patterns</b>	<b>164</b>
5.6.1	Conditions-Effects-Interaction	164
5.6.2	Withdrawal	166
5.6.3	Access Restriction	169
5.6.4	Mortal	170
5.6.5	Automatic Expiration	171
5.6.6	Rejector	173
5.6.7	Circuit Breaker	174
5.6.8	Allow Once per Account	177
<b>6</b>	<b>Decentralized Applications (Dapps)</b>	<b>179</b>
<b>6.1</b>	<b>Implementing Dapps</b>	<b>183</b>
<b>6.2</b>	<b>Case Studies</b>	<b>190</b>
6.2.1	Crowdfunding	190
6.2.2	Event Registration	197
6.2.3	Document Verification	204
6.2.4	Call Option	210
6.2.5	Interest Rate Swap	222

6.2.6	Industrial IoT - Machine Maintenance	239
6.2.7	Solar Charging Stations	248
<b>7</b>	<b>Mining</b>	<b>277</b>
<b>7.1</b>	<b>Consensus on Blockchain Network</b>	<b>278</b>
<b>7.2</b>	<b>Mining</b>	<b>278</b>
7.2.1	Stage-1: Determine Uncles	278
7.2.2	Stage-2: Determine and Process Transactions	278
7.2.3	Stage-3: Apply Mining Rewards	285
7.2.4	Stage-4: Compute Mining Proof-of-Work	286
<b>7.3</b>	<b>Block Validation</b>	<b>291</b>
<b>7.4</b>	<b>Setting up Mining Node</b>	<b>293</b>
<b>7.5</b>	<b>State Storage in Ethereum</b>	<b>294</b>
7.5.1	World State	294
7.5.2	Transactions List	294
7.5.3	Transaction Receipts	294
7.5.4	Modified Merkle Patricia Tree	294
<b>8</b>	<b>Whisper</b>	<b>299</b>
<b>8.1</b>	<b>Whisper Protocol</b>	<b>300</b>
8.1.1	Whisper Envelope and Message	300
8.1.2	Configurable Privacy and Efficiency	301
8.1.3	Whisper Communication Patterns	301
8.1.4	Whisper Wire Protocol	303
8.1.5	Posting a Message	303
8.1.6	Topics, Abridged Topics & Bloomed Topics	304
<b>8.2</b>	<b>Whisper Routing Approaches</b>	<b>306</b>
8.2.1	Passive Routing - Peer Steering	306
8.2.2	Active Routing - Topic Filtering	306
<b>8.3</b>	<b>Whisper API</b>	<b>307</b>
8.3.1	NewIdentity	307
8.3.2	HasIdentity	307
8.3.3	Post	307
8.3.4	Filter	308
8.3.5	Working with Whisper	308
<b>8.4</b>	<b>Case Study: Smart Switch Dapp</b>	<b>310</b>
<b>9</b>	<b>Swarm</b>	<b>323</b>
<b>9.1</b>	<b>Swarm Architecture and Concepts</b>	<b>324</b>
9.1.1	Swarm Nodes	324
9.1.2	Storage Layer	324

9.1.3	Network Layer .....	328
<b>9.2</b>	<b>Incentive Mechanisms in Swarm</b>	<b>330</b>
9.2.1	SWAP .....	330
9.2.2	SWEAR .....	332
9.2.3	SWINDLE .....	332
<b>9.3</b>	<b>Swarm Setup</b>	<b>332</b>
<b>9.4</b>	<b>Working with Swarm</b>	<b>333</b>
<b>9.5</b>	<b>Case Study: Stock Photos Dapp</b>	<b>337</b>
<b>III</b>	<b>ADVANCED TOPICS</b>	<b>349</b>
<b>10</b>	<b>Advanced Topics on Blockchain .....</b>	<b>351</b>
10.1	Double-Spending Problem	352
10.2	Byzantine Fault Tolerance	352
10.3	Proof-of-Work vs Proof-of-Stake	353
10.4	Consistency, Availability & Partition Tolerance (CAP)	354
10.5	Turing Completeness	354
10.6	Greedy Heaviest-Observed Sub-Tree (GHOST)	355
10.7	Sybil Attack	357
10.8	Mining Pools and Centralization	357
10.9	Smart Contracts Vulnerabilities	358
10.10	Blockchain Scalability	358
	 <b>Appendix-A - Solidity Language Tutorial .....</b>	 <b>371</b>
	 <b>Bibliography .....</b>	 <b>375</b>
	 <b>Index .....</b>	 <b>377</b>