Preface

About the Book

In the US, the services sector provides employment to about 100 million, while the manufacturing sector provides employment to about 20 million. In the services sector, retail (15 million employees), professional and business services (16 million employees), health care (14 million), hospitality (12 million), federal and local governments (20 million), educational services (2 million), and financial services (8 million) form the main business sectors. All these sectors are highly automated, and driven by sophisticated business processes forming an integral part of the digital economy. While the applications themselves may be distributed over the Internet in time and space, the core business, regulatory, and financial aspects of the digital economy are still centralized, with the need for centralized agencies (such as banks, customs authorities, and tax agencies) to authenticate and settle payments and transactions. These centralized services often are manual, difficult to automate, and represent a bottleneck to facilitating a frictionless digital economy. The next revolutionary step in the services and manufacturing economy of the future is the development of automated distributed applications that do not depend on these traditional centralized agencies for controlling, facilitating and settling multi-party transactions that may themselves be subject to complex contractual constraints. The blockchain technology is an integral part of these next steps that promises a smart new world of automation of complex services and manufacturing processes.

Blockchain is a distributed and public ledger which maintains records of all the transactions on a blockchain network comprising suppliers of products and services and consumers. A blockchain network is a peer-to-peer network and does not require a central authority or trusted intermediaries to authenticate or to settle the transactions or control the underlying infrastructure. Bitcoin was an early generation blockchain network that was introduced in 2008 where the primary application of the blockchain network was the use of electronic cash or cryptocurrency called Bitcoin. A second generation blockchain network called Ethereum was introduced in 2013. Ethereum allows a single programmable blockchain network to be used for developing different types of applications where each application takes the form

of a smart contract which is implemented in a high-level language and deployed on the blockchain network.

With the blockchain's ability to establish trust in a peer-to-peer network through a distributed consensus mechanism rather than relying on a powerful centralized authority, the technology is being seen by the industry experts as one of the greatest innovations since the invention of the Internet. The blockchain technology has the potential to disrupt FinTech, manufacturing, supply chain, logistics, and healthcare industries by making transactions faster, cheaper, more secure and transparent without the need for a central authority or a trusted intermediary. Recognizing the potential of the blockchain, several financial and technology firms have invested billions of dollars to bring blockchain technology to capital markets. Industry surveys predict that blockchain technologies could reduce the infrastructural costs for financial institutions by $15-20 billion a year by 2022.

There are very few books that can serve as a foundational textbook for colleges looking to create new educational programs in these areas of blockchain, smart contracts, and decentralized applications. Existing books are primarily focused on the business side of blockchain, or describing vendor-specific offerings for blockchain platforms. Recent studies from PwC and CapGemini have determined that only ten percent of the financial industry is comfortable with the technical aspects of blockchain, and FinTech and RegTech industries are struggling to identify its impact on their business and how they should react to it.

We have written this textbook, as part of our expanding "A Hands-On Approach"™ series, to meet this need at colleges and universities. This book is also written for use within industries in the FinTech and RegTech space that may be interested in rolling out products and services that utilize this new area of technology. The book can serve as a textbook for senior-level and graduate-level courses on financial and regulation technologies, business analytics, Internet of Things, and cryptocurrency, offered in Computer Science, Mathematics and Business Schools.

The typical reader is expected to have completed a couple of courses in programming using traditional high-level languages at the college-level, and is either a senior or a beginning graduate student in one of the science, technology, engineering or mathematics (STEM) fields. The reader is provided the necessary guidance and knowledge to develop working code for real-world blockchain applications. Concurrent development of practical applications that accompanies traditional instructional material within the book further enhances the learning process, in our opinion. Furthermore, an accompanying website for this book contains additional support for instruction and learning (www.blockchain-book.com).

The book is organized into three main parts, comprising a total of ten chapters. Part I provides an introduction to blockchain, applications of blockchain, design patterns, and architectures for blockchain applications. A blockchain stack comprising a decentralized computation platform, a decentralized messaging platform, and a decentralized storage platform is described. While in this book we describe a specific realization of the blockchain stack based on the Ethereum blockchain platform, the same blockchain concepts can be applied to other blockchain platforms as well, such as Eris and Multichain. We describe a blockchain application design methodology that includes analysis, design and implementation stages. Templates for blockchain applications are provided. The blockchain stack and application design methodology form the pedagogical foundation of this book.

Part II introduces the readers to various tools and platforms for blockchain, and the

architectural and programming aspects of these platforms. We chose the Ethereum blockchain platform for this book. For smart contract implementations, we chose the Solidity programming language. Other blockchain platforms and programming languages, may also be easily used within the blockchain stack described in this book. The reader is introduced to Ethereum tools such as Geth, PyEthApp, TestRPC, Mist Ethereum Wallet, MetaMask, Web3 JavaScript API, and the Truffle Dapp framework. The types of Ethereum accounts are described along with examples of setting up and working with the accounts. In the smart contracts chapter, we describe the structure of smart contracts and how to implement, compile, deploy and interact with smart contracts. Implementation examples of various smart contracts and the commonly used patterns are provided. In the chapter on decentralized applications (Dapps), we describe with the help of examples and case studies the steps involved in implementing Dapps using the Truffle Dapp framework. The chapter on mining provides an in-depth study of the consensus mechanism in a blockchain network, the steps involved in mining, the structure of a block, mining proof of work algorithm, mining rewards and state storage in Ethereum. The chapter on Whisper decentralized messaging platform introduces the reader to the structure of whisper envelope and message, whisper communication patterns, whisper wire protocol and routing approaches. The chapter on Swarm decentralized storage platform introduces the reader to the swarm architecture and concepts and the incentive mechanisms in swarm.

Part III focuses on advanced topics such as the security and scalability related challenges for the blockchain platforms.

Through generous use of hundreds of figures and tested code samples, we have attempted to provide a rigorous "no hype" guide to blockchain. It is expected that diligent readers of this book can use the canonical realizations of blockchain application templates and patterns described in this book to develop their own blockchain applications. We adopted an informal approach to describing well-known concepts primarily because these topics are covered well in existing textbooks, and our focus instead is on getting the reader firmly on track to developing robust blockchain applications as opposed to more theory.

While we frequently refer to offerings from commercial vendors, this book is not an endorsement of their products or services, nor is any portion of our work supported financially (or otherwise) by these vendors. All trademarks and products belong to their respective owners and the underlying principles and approaches, we believe, are applicable to other vendors as well. The opinions in this book are those of the authors alone.

Please also refer to our books "Big Data Science & Analytics: A Hands-On Approach[TM]", "Internet of Things: A Hands-On Approach[TM]" and "Cloud Computing: A Hands-On Approach[TM]" that provide additional and complementary information on these topics. We are grateful to the Association of Computing Surveys (ACM) for recognizing our book on cloud computing as a "Notable Book of 2014" as part of their annual literature survey. We are also grateful to the universities worldwide that have adopted these textbooks as part of their program offerings for providing us feedback that has helped us in improving our offerings.

Book Website

For more information on the book, copyrighted source code of all examples in the book, lab exercises, and instructor material visit the book website: www.blockchain-book.com