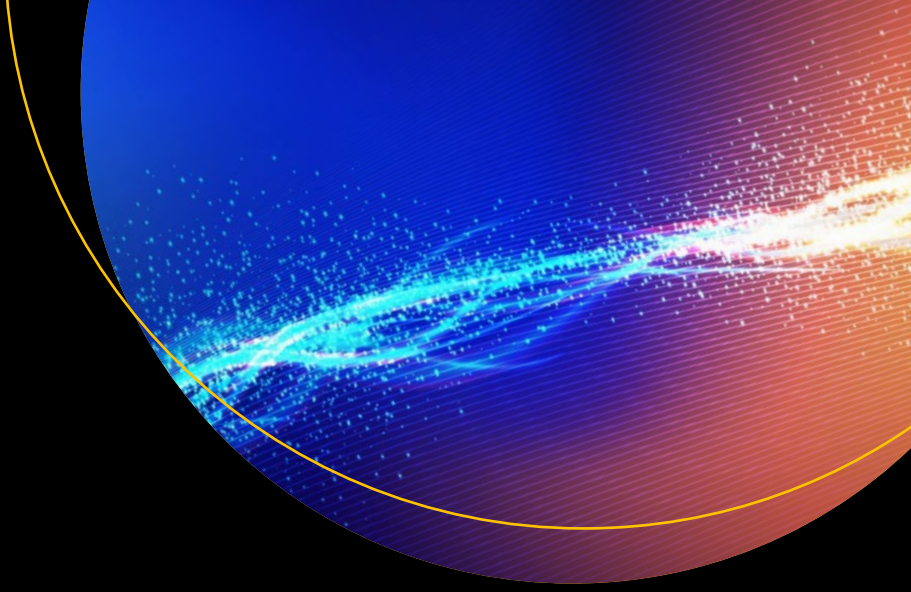

R3 Corda for Architects and Developers

With Case Studies in Finance, Insurance, Healthcare, Travel, Telecom, and Agriculture

Debajani Mohanty

Apress®

R3 Corda for Architects and Developers

With Case Studies in Finance, Insurance, Healthcare, Travel, Telecom, and Agriculture

Debajani Mohanty

Apress®

R3 Corda for Architects and Developers

Debajani Mohanty
Noida, Uttar Pradesh, India

ISBN-13 (pbk): 978-1-4842-4531-6 ISBN-13 (electronic): 978-1-4842-4529-3
https://doi.org/10.1007/978-1-4842-4529-3

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Celestin Suresh John
Development Editor: Siddhi Chavan
Coordinating Editor: Aditee Mirashi

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-4531-6. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Author

Debajani Mohanty, author of the Amazon bestsellers *BlockChain: From Concept to Execution* (BPB Publications, 2018), *Ethereum for Architects and Developers* (Apress, 2019), and now *R3 Corda for Architects and Developers*, is a Solution Architect with close to 18 years of experience in the industry. Her books have been translated into German and Chinese. Debajani is a keynote speaker at Philadelphia PACT, NASSCOM, IIM, WomenWhoCode, Unicom, Amity, India International Centre, and many similar national and international tech events. She is Honorary Faculty with Amity University, consultant, and an advisor and mentor to numerous reputed organizations in India and abroad. Debajani is also a woman activist and writer felicitated by Nobel laureate Kailash Satyarthi for her outstanding contributions to woman empowerment in India.

Follow her on Twitter: https://twitter.com/debimr75

Follow her on LinkedIn: https://www.linkedin.com/in/debajanimohantypmp/

About the Technical Reviewer

Prem Naraindas is a hands-on and highly experienced technology executive with over 17 years of successful, enterprise-level accomplishments with a passion to drive customer engagements to successful outcomes from start to finish. Through the course of his career, Prem has led transformational initiatives for clients in areas such as application development and maintenance, business process outsourcing, engineering services, R&D, innovation, and infrastructure. Prem has over three years of experience with Enterprise Blockchain, has been responsible for delivering over 20 Proofs of Concept, and has successfully envisaged and led production implementation of one of the world's first Enterprise Blockchain applications. In his current role, Prem is Global Blockchain Offering Director at DXC technology. This role is part of the DXC Global Blockchain Practice, in which Prem is responsible for understanding the Enterprise Blockchain market demands and trends and for working with clients, sales teams, delivery, and consultants to make the strategy relevant to DXC's client base and to create Blockchain offerings and solutions with value superior to that offered by the competition. He is also responsible for understating the market dynamics to drive DXC's Blockchain product, platform development, and go-to-market strategies.

Acknowledgments

This book is possible because of the combined effort of many; my work is so small it causes only ripples in a massive ocean. I take this opportunity to offer my gratitude to the following people for always being there with me when I was in need: my grandmother Mrs. Renuka Das, mother Mrs. Nirupama Mohanty, father Dr. N. K. Mohanty, husband Dr. Rajul Rastogi, and uncle Dr. N. R. Das. I am also grateful to Prem Naraindas, DXC Technology for taking his valuable time to review this book on time.

Last but not least, thanks to Coordinating Editor Aditee Mirashi, Acquisitions Editor Celestin Suresh John at Apress; for all the help while working on the book.

Introduction

R3 Corda for Architects and Developers is intended to be the standard book on R3 Corda, the industry-leading distributed ledger technology (DLT). The book explores the entire Corda ecosystem step by step with adequate theory, labs, and live use cases.

Today, R3 Corda has emerged as the DLT platform of choice for the insurance domain as well as many banks and regtech organizations. The main issue learning R3 Corda is the lack of trainers and the scarcity of sample codes in a well-accepted language such as Java, since most of its existing examples are written in Kotlin. *R3 Corda for Architects and Developers* will fill that vacuum by providing contents suitable to all stakeholders consolidated in one place. In this reading journey, the reader will be introduced chapter by chapter to Blockchain concepts, DLT, R3 Corda architecture, and smart contract programming in Java with ample examples, guiding the reader through testing and deployment of the entire ecosystem. In later chapters, readers will be introduced to various business problems in healthcare, agriculture, and a few other domains and how Corda can solve these issues through its unique and efficient DLT offering. The book also provides sample codes of some useful Proof of Concepts (PoCs) that will be most beneficial to business leaders and architects in their Corda journey from concept to execution. The business scenarios and solutions are provided with flowcharts, diagrams, and sample codes that stakeholders can refer to, further enhance as per their respective business needs, and deploy in live projects.

The book will be very useful for readers of every background, whether they are eager to develop decentralized applications in R3 Corda, or wish to learn its architecture, or even are interested in exploring different use

cases that can be implemented using this technology across business verticals. By the end of the book, readers will have enough information about how the correct usage of R3 Corda can create value for their business processes by eliminating middleman costs and bringing in transparency for creation of deduplicated, fraud-proof data storage for smoother execution of business. The best and most unique part of the book is that all the examples are written in Java.

Readership (who's the target audience?):

The book will appeal to the novice who wishes to learn R3 Corda from scratch and continue the journey until he or she knows the whole ecosystem and is able to deploy code in production. At the same time, it will be of interest to an existing Blockchain developer or architect, to know the R3 Corda best practices and live use cases where R3 Corda can do its wonders by bringing transparency to processes, cutting middleman costs, reducing time of operation, and finally eliminating fraud and duplication of data.

CHAPTER 1

Barter to Blockchain

In childhood, I heard many stories from my legendary grandfather about how certain people created immense amount of wealth in a short time, of course in an honest way, and then more importantly how they kept it all safe. While most little girls of my age were fascinated by fairytale stories, I found wealth creation ideas much more alluring and a means to be a powerful someone someday later in life. With time I came to know I was not the only one in this game. People in all ages and all times have ceaselessly thought over this puzzle of "creating wealth," "securing it," and "trading or investing for larger returns." Be it gold, spices, cattle, slaves, land, or oil, wealth has many different forms and there are inherent flaws when it comes to trading in wealth. In this chapter, let's discuss some of the different forms of money and figure out how this journey finally culminated in Bitcoin and Blockchain, one of the biggest technical inventions of the 21st century.

History of Money

Have you ever wondered why we need to secure our valuables, and if so was there always a need to do so? Well, perhaps not. More than ten thousand years back, human beings lived in caves. They were hunters who lived on their daily earnings, whether animal or fruit or equivalent, and there was no need to store or keep such perishable items safe for a long time. That was the time when they started living in groups in caves to

D. Mohanty, *R3 Corda for Architects and Developers*,
https://doi.org/10.1007/978-1-4842-4529-3_1

stay protected from animal attacks and other natural calamities. Slowly, they gained different skills such as cooking, making weapons, and sewing clothes. Gradually they learned cultivation and domestication of certain animals. Soon people started a classification and division of labor on the basis of specialization of skills, so that a particular group of people good at a certain skill would work in that particular skill area only. However, that led to a problem: for example let's say a farmer who cultivated rice produced more rice than his family could consume and at the same time needed milk for his family. Where would this farmer be able to get it? So the need to trade took a concrete shape. Some 9,000 to 10,000 years back, people started trading, and the mechanism is called "the barter system." This is a very popular mechanism to exchange products and services and people even today do it in every country in the world.

Barter System

The barter system, the most primeval form of trading, was easy and simple. People used to gather in groups on a particular day and exchange items for something else that would be useful for them. Mostly it was an exchange of products and services, which happens even today in many communities and countries across the world. The barter system gained wide popularity because of its simple way of exchanging products and services. However, the double coincidence of wants was always a problem. For example, there might not be an exact requirement match of commodities between parties. Divisibility too was another concern. Let's consider an example; one cow is selling for ten chickens. However, what if someone wants to purchase only one chicken. Also commodities were mostly perishable items and could not be stored as permanent wealth. So there was a need for a universally approved token that could be used as an exchange item for payment and would address the original issues inherent in the "barter system" of that time: divisibility, perishability, exchangeability, storage, and so on.

Metal Currency

So some people who had understood the limitations of the barter system started thinking of an alternate payment medium and that is the time when metal currency was introduced. At different time periods, different types of currencies were in execution: for example, grains, seashells, leather money, and so on. Finally metal currencies were introduced between 700 BC and 600 BC. In order to make the currency universal, these metal currencies needed approval or stamp by kings and rulers. Initially, only those metals that were durable, divisible, portable, limited in supply, and nonperishable were selected. Also, it's very important that in terms of weight and value, the price of metal was the price of money so that even if someone used regular silver or gold to create fake currencies it would not affect the monetary valuation system. The issue with metal currencies was that they were heavy and difficult to transport in larger quantities. Also, the utility of metals was wasted by converting them to currency.

Paper Money

Time and need again prompted certain smart people to craft another currency which would be lighter and easier for storage and would have no intrinsic value so that metals and usable items can be saved for utility. Hence paper money was introduced somewhere around 800–900 AD. However, the issue with paper money was that it could be quickly reproduced in an illegal way, and also that it could be misused by black-marketers and money-hoarders. The most dangerous part, however, was that it carried no inherent value.

Banks

Over the last few thousand years, banks have evolved to a great extent; however modern banks mostly have the same operations as centuries back: credit and debit. Banks will take the money that users deposit, invest it elsewhere, get some profits, and return back the principal with interest to the users. Also, after paper money was introduced, banks played a central role in guaranteeing the value of money. The emblem that kings and rulers once enforced to convert a metal to a currency nowadays is done by the banks.

With time, banks mushroomed everywhere, and gradually every country appointed a central bank to regulate functions of banks and act as the centralized authority to carry out monetary policy, taxation, and economic development of the country. The following are some examples of central banks:

- Reserve Bank of India, India
- Federal Reserve System, USA
- Bank of England, UK

Issue with Centralized Authority in Banking

Since our school days, our textbooks have taught us about monetary policies and claimed that banks are the safest place to save our hard-earned money. Let's find out the extent to which that's true. If you peruse the history of banking, you can find a plethora of financial crises: credit crisis in 1772, the Great Depression beginning in 1929, and the banking crisis in 2008, among others. During such a crisis, there is a sudden panic in the market followed by a long list of investors who wish to withdraw their investments from banks almost immediately. But banks might not always have a reserve of cash as they have invested it elsewhere; hence they are not in a position to handle paying back all deposits quickly if there is a sudden hike in demand. Under such instances, they declare bankruptcy.

It is interesting to note that such financial crises are mostly human created and might not have much to do with the inherent price of commodities. For example, if a seller wishes to sell a property in the market, then the cash amount that they would get would be different at different points of time depending upon the market conditions. However, if they want to exchange it with any commodity, for example a property owner in San Francisco wishes to exchange their house with another one in New York, the exchange rate might not vary unless there is again a mismatch between demand and supply. Hence, during many financial crises in history, it's observed that the age-old barter system has come back into the mainstream.

2008 Financial Crisis: A Pathbreaker

Among all these historical financial crises, the most recent one, which most of us have observed in our lifetimes, was in the year 2008. Who can forget its impact: so much unemployment, property meltdown and ill health? If one traces down what went wrong, it's pretty simple and it could have been completely avoided.

In the 2007–2008 time period, banks had started to give out risky loans to people even with bad credit history to attract new customers mostly out of greed for a possible higher interest rate. Ultimately, that money could not be paid back for obvious reasons. Many banks collapsed and filed for bankruptcy. The American government tried to save some financial institutions from crisis by bailing them out. However, money offered by the government to the banks was also the people's money, which had been paid in taxes. The actions of the American government led to customer dissatisfaction across the entire country. Since the global economy is interconnected and most banks work in brotherhood, the events that took place in the United States also affected the world, bringing the world's economy to a standstill.

Bitcoin Was Born

As in earlier phases in the evolution of money, after the 2008 financial crisis some intellectuals started doubting centralized systems as banks and financial organizations. Why?

- Banks might not be actually a trusted third party for securing all the money.
- Banks charge a huge fee for their services, especially for international remittances.
- They take considerable time for clearing transactions in interbank and intercountry transactions.

It's quite amusing that while in most countries in the world, democracy is prevalent in terms of choosing leadership, when it comes to money we still live in autocracy as the money is handled by banks, a centralized third party, rather than lying in the hands of the people.

In documented human history over the past thousand years, we have witnessed many demonetizations, where an existing currency is invalidated, followed by remonetization, in which a form of payment is restored as legal tender. Currencies were a mere representation of exchange media and yet carried no value without the backing of kings, emperors, or ruling governments.

Cryptocurrency is one such currency: its distribution and exchange though is entirely confined to the digital world. Contrary to the belief of many, Bitcoin is not the first cryptocurrency. DigiCash in 1992, CyberCash in 1994, E-Gold in 1996, WebMoney in 1998, Liberty Reserve in 2006, and Perfect Money in 2007 were all crypto or digital currencies, some of which are still in use by communities. However Bitcoin was revolutionary as it came up with a new, previously unseen concept: decentralization.

Note While all these currencies are referred to as cryptocurrency, the regular currencies such as USD, GBP, INR, and so on are still known as fiat currencies or fiat cash.

Bitcoin White Paper

It's hard to believe the legendary cryptocurrency Bitcoin is only a decade old and only a baby in the world of money and yet could bring in such high value to the monetary system. In October 2008, Satoshi Nakamoto's nine-page Bitcoin white paper appeared on the market, and not too many paid attention. However, in just under a decade's time, this technology proved to be the most disruptive since the invention of the Internet itself. This white paper specified

- Instructions on how to run the Bitcoin network.
- Why and how transactions are hashed and saved to Merkle root (should be explained later in this Chapter).
- How network handles anticipatory attacks.
- How to establish a Proof-of-Work (PoW) system to deter hackers (should be explained later in this Chapter).
- How it is practically impossible for hackers to change transactions.
- How to prohibit double spending in a decentralized way not involving a centralized third party such as banks (should be explained later in this Chapter).