

Blockchain

Tatiana Gayvoronskaya • Christoph Meinel

Blockchain

Hype or Innovation



Springer

Tatiana Gayvoronskaya
Hasso Plattner Institute for Digital
Engineering gGmbH
Potsdam, Germany

Christoph Meinel
Hasso Plattner Institute for Digital
Engineering gGmbH
Potsdam, Germany

ISBN 978-3-030-61558-1 ISBN 978-3-030-61559-8 (eBook)
<https://doi.org/10.1007/978-3-030-61559-8>

© Springer Nature Switzerland AG 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Is blockchain an “alien technology” or a new encryption algorithm to achieve the creation of digital currency that has been turned into hype for marketing reasons? Technically speaking, blockchain is presumably a highly complicated, non-transparent technology, something that only corporate giants with innovation labs can work with – at least that is what most people think. The confusion is understandable, as even today¹ the debate rages on as to the “correct” definition of blockchain technology.

In 2016 and 2017, when the hype surrounding blockchain had reached its peak, numerous companies began to take part in the “blockchain experiment.” Each had its own visualization of blockchain. This meant that the hype surrounding blockchain technology not only served to spur on development but, at the same time, was the most common cause of failure. The planning and development phases of numerous projects were shortened dramatically, so that the product could be brought to the market as quickly as possible and thereby profit from the extensive hype. At the same time, many technical concepts and projects that had already existed before the appearance of blockchain technology (and had little to do with its innovation) could be sold more successfully under the blockchain name. That the strongly hyped blockchain technology was met with disappointment should therefore come as no surprise. Looking at a new technology realistically is the cornerstone of its success. This can only happen when the innovation is used correctly.

In this book, we focus on the innovation of blockchain technology and the advantages this technology offers us when compared to existing solutions. Our goal is to provide a clear and comprehensive overview of blockchain technology and its possibilities, thereby helping you to form an opinion and draw your own conclusions.

Right from the start, we would like to sharpen our focus on the main objective of blockchain technology. To do this, we begin in the first chapter with the topic of decentralized networks, familiarizing ourselves with their challenges and using

¹At the time this book was written.

the example of an online trading platform. In succeeding chapters, we explain what blockchain technology is, where it comes from, and how it works. Before we take a closer look at technical questions, we will explore the necessary technical foundations. In this chapter, we examine individual approaches at the core of blockchain technology, and how they are composed. With the help of well-known examples, such as Bitcoin and Ethereum, we look at the architecture of blockchain technology and focus on the challenges facing it, such as those involving security and scalability. Subsequently, we discuss the options available when introducing blockchain technology. Among other things, we will target best-practice examples to get a better idea of what areas benefit from this technology.

Numerous examples and detailed explanations will accompany you throughout this book. It is our hope that by the time you have reached the end, you will be able to decide for yourself what is truly innovative about the blockchain technology and what is nothing more than hype.

This book builds on our Technical Report [25] and aims to provide a comprehensive overview of blockchain technology. In addition to the technical foundations, it aims to cover the big picture, from the idea of the Bitcoin system to the challenges facing blockchain technology and its alternatives.

We would like to thank Mr. Matthias Bauer for his linguistic support in the writing of this book. We also wish to thank Dr. Sharon Therese Nemeth for the translation of this book from the German language edition.

Potsdam, Germany
August 2020

Tatiana Gayvoronskaya
Christoph Meinel

Contents

1	Introduction	1
1.1	Trust	2
1.2	Resource Allocation and Administration	3
2	What Is Hidden Behind the Term “Blockchain”?	5
2.1	Understanding Blockchain: A Simple Example	6
2.2	Bitcoin	9
3	Technical Basics for a Better Understanding of Blockchain Technology	15
3.1	Cryptography	15
3.1.1	Digital Signatures and Hash Values	16
3.1.2	User Identification and Addresses	18
3.2	Exchange Among Equals	20
3.2.1	Obfuscation	25
3.2.2	Data Protection and Liability	27
3.3	Consensus Finding	28
4	Where Does the Hype End, and Where Does the Innovation of Blockchain Technology Begin?	35
4.1	Traceability, Forgery Protection, Reliability	36
4.1.1	The Smallest Component in a Blockchain	38
4.1.2	Block and Chain	42
4.1.3	Updating the Blockchain	46
4.1.4	New Blockchains and Alternatives	50
4.2	Challenges of Blockchain Technology	52
4.2.1	Possible Attacks	52
4.2.2	Scalability	56

5 The Right Use Leads to Success	69
5.1 The Application of an Existing Blockchain Solution	71
5.1.1 UTXO-Based Solution with Colored Coins	71
5.1.2 Account-Based Solution and Smart Contracts	73
5.1.3 Interoperable Blockchains	75
5.2 Implementation of a New, Unique Blockchain Solution	78
6 Projects and Application Areas of Blockchain Technology	79
6.1 Financial Sector	87
6.2 Identity Management	89
6.3 Internet of Things	91
6.4 Energy	93
6.5 Logistics	94
7 Summary	97
A Byzantine Agreement Algorithm	103
B Automatically Use TOR Hidden Services	105
C Verifying the Transaction in the Bitcoin System	107
D The Byzantine Generals Problem	109
E Atomic Cross-Chain Trading	111
F Ethereum Roadmap	113
References	115
Index	125