Bitcoin for Nonmathematicians

Exploring the Foundations of Crypto Payments

Slava Gomzin

Universal-Publishers
Boca Raton

Copyright © 2016 Slava Gomzin
All rights reserved.
No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher

Universal-Publishers
Boca Raton, Florida • USA
2016

ISBN-10: 1-62734-071-8
ISBN-13: 978-1-62734-071-7

www.universal-publishers.com

Publisher's Cataloging-in-Publication Data

Names: Gomzin, Slava.
Title: Bitcoin for nonmathematicians : exploring the foundations of crypto payments / Slava Gomzin.
Description: Boca Raton, FL : Universal Publishers, 2016. | Includes bibliographical references and index.
Identifiers: LCCN 2016930001 | ISBN 978-1-62734-071-7 (pbk.)
Subjects: LCSH: Bitcoin. | Money. | Electronic commerce. | Mobile commerce. | Cryptography--Data processing. | Data encryption (Computer science) | BISAC: BUSINESS & ECONOMICS / Money & Monetary Policy. | BUSINESS & ECONOMICS / E-Commerce / General. | COMPUTERS / Electronic Commerce. | COMPUTERS / Security / Cryptography.
Classification: LCC HF5548.32 .G659 2016 (print) | DDC: 332.4--dc23.

To Svetlana
and our daughters Alona, Aliza, and Arina

About the Author

Slava Gomzin is Director of Information Security at PCCI (Parkland Center for Clinical Innovation), a nonprofit research and development corporation delivering real time predictive analytics solutions. Slava is also the author of *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions* (Wiley, 2014), and has written many articles on payment security and technology. Prior to joining PCCI, Slava was a security and payments technologist at Hewlett-Packard, where he helped create products that are integrated into modern payment processing ecosystems. Before HP, he worked as a security architect, corporate product security officer, and R&D and application security manager at Retalix, a division of NCR Retail. As PCI ISA, he focused on security and PA-DSS, PCI DSS, and PCI P2PE compliance of POS systems, payment applications, and gateways. Slava currently holds CISSP, PCIP, ECSP, and Security+ certifications. He blogs about information security and technology at www.gomzin.com.

Credits

Technical Editor
Ken Westin

Copy Editor
Adaobi Obi Tutton

Foreword
Doug McClellan

Publisher & CEO
Jeff Young

Photo
Svetlana Gomzin

Production Editor
Christie Mayer

Cover Design
Ivan Popov

Acknowledgments

Writing a book is not easy and cannot succeed without help from other people. First of all, I would like to thank Carol Long for convincing me to start writing another book right after the previous one was published. And thanks to Jeff Young for bringing this project to reality. Also, I would like to thank my ex-coworkers from HP, especially David White for his support and interest in such a controversial topic. Thanks to Ken Westin for his enthusiastic support and contribution. Thanks also go to VentureBeat editor, Morwenna Marshall, for the opportunity to share my ideas with a wider audience. Thanks to Adaobi Obi Tulton for another great editorial effort. Special thanks to Doug McClellan for his bright and sincere foreword. And finally, I want to thank my wife, Svetlana, for her continuous support and understanding.

Contents at a Glance

Foreword by Doug McClellan		**17**
Introduction		**21**
Part I	**From Coins to Crypto**	**25**
Chapter 1	**Traditional Money**	**27**
Chapter 2	**Digital Gold**	**35**
Chapter 3	**Centralized Digital Payments**	**43**
Chapter 4	**Cryptocurrencies**	**55**
Part II	**Bitcoin Cryptography**	**67**
Chapter 5	**Types of Encryption**	**69**
Chapter 6	**RSA Step by Step**	**81**
Chapter 7	**How Elliptic Curves Work**	**89**
Bonus Chapter	**Experimenting with the Code**	**115**
References		**127**
Index		**133**

Contents

Foreword by Doug McClellan		**17**
Introduction		**21**
Part I	**From Coins to Crypto**	**25**
Chapter 1	**Traditional Money**	**27**
	Commodities versus Gold	27
	Payment Cards	29
	Mobile Payments	31
	From Coins to Crypto	32
Chapter 2	**Digital Gold**	**35**
	Gold Standard	36
	E-gold	36
	e-Bullion	40
Chapter 3	**Centralized Digital Payments**	**43**
	DigiCash and ecash	44
	Online Currencies: Flooz and Beenz	47
	Liberty Reserve	48
	Online Payment Processors	52
Chapter 4	**Cryptocurrencies**	**55**
	Satoshi Nakamoto White Paper	55
	Double-Spending Problem	56
	Decentralization	58
	Privacy: Anonymity or Pseudonymity	58
	Blockchain	61
	Byzantine Generals' Problem	62

	Mining	62
	Part I Summary	**65**
Part II	**Bitcoin Cryptography**	**67**
Chapter 5	**Types of Encryption**	**69**
	Symmetric Encryption	70
	One-Way Hash Functions	71
	One-Way Function and Message Digest	73
	Collision	74
	SHA-256	75
	RIPEMD-160	76
	Public-Key (Asymmetric) Cryptography	76
	Digital Signatures	78
Chapter 6	**RSA Step by Step**	**81**
	One-Way Functions	81
	Let's Start	83
	Public Key: Just a Random Number	83
	Modulus: It's Like a Clock Dial	83
	Encryption: Plaintext to the Power of Public Key	85
	Private Key: Phi Function + Modular Inversion	86
	Decryption: Ciphertext to the Power of Private Key	87
Chapter 7	**How Elliptic Curves Work**	**89**
	The Graph	89
	Horizontal Symmetry and Points of of Intersection	93

	Point Operations	96
	Point Addition	97
	Point Doubling	98
	Point Multiplication	99
	One-Way Function	102
	Limiting the Curve for the Sake of Cryptography	105
	Generating the Keys	
	Encryption	107
	Decryption	108
	Just a Little Bit of Math	108
	Point Addition: C = A + B	108
	Point Doubling: C = A + A = 2A	
	Now Let's Play with the Numbers	109
	Encryption	113
	Decryption	113
Bonus Chapter	**Experimenting with the Code**	**115**
	Modulus	115
	Modular Inversion	116
	Representing the Points	118
	Point Doubling	119
	Point Multiplication	121
	Calculating the Public Key	122
	Encryption	123
	Decryption	124
	Part II Summary	125
References		**127**
Index		**133**

Foreword

by Doug McClellan

I'm a numismatist, which is a fancy word for a coin collector. I'm also a software developer for electronic funds transfer (EFT) systems by profession and, like most readers here, also an investor.

So when Slava told me he was writing a book about bitcoins, I knew I wanted to read it because it was an area I've always had an interest in from the three perspectives I've just mentioned. Bitcoins mainly tie into the future of electronic payments, but also have been used as an investment vehicle and could very well have an impact on the future of numismatics.

I've been collecting coins ever since I was a kid, and started building my collection over 45 years ago with a Lincoln Cent album. For the last 25 years I've developed software for the retail merchant industry, and specialized in EFT systems for the convenience store market segment for the last 17 years. When you buy a soda at the convenience store or swipe your card at the pump, there is software needed to process your transaction electronically.

I will expand more on that in a bit, but first I want to introduce you to the author, Slava Gomzin. For those of you who are not familiar with his work from his blog at www.gomzin.com or from the other books he has published in the area of cybersecurity, such as *Hacking Point of Sale*, along with his *Application Security* and *Cyber Privacy* book series titles for electronic data security, I think you will join me in appreciating his insight in this area.

I met Slava in 1999 when we worked together to create an EFT software system through our mutual employer. Slava had emigrated from Russia to Israel when President Reagan had challenged the Russian government to allow its citizens to have more freedom in their lives. Slava was one of those people who saw the opportunity and had the courage to build a new life in a foreign country. He moved his family to Israel, where he found employment using his computer programming skills. Later he again utilized his pioneer spirit when he moved with his wife and children to America, the true land of opportunity.

Slava has proven that hard work and dedication, along with natural talent and abilities, will flourish in a free society. Slava was our team leader in the EFT development group during a time when our company was rapidly expanding here in the United States. While managing multiple development projects with different EFT networks, he had taken an interest in cyber security, which was in its infancy at the time. He read, studied, and attended courses in cybersecurity, and has earned many certifications over the years. Slava also served on the PCI standards committee when the early standards were being developed. So, as you can see, Slava knows cybersecurity. In fact, I would say he is an expert in the field.

In this book, Slava brings the reader along on a journey from the origins of money and electronic payments and into the implementation of bitcoins as a cybercurrency.

I find the term bitcoin to be rather clever as a name. It is not, of course, a coin in the physical sense, but an electronic implementation of money represented by bits, the electronic 1s and 0s that computers use to store data. The origin of bitcoin is rather mysterious, as you will learn in the book.

Using the standard economic concepts that the value of anything is what a willing buyer will pay a willing seller in an arm's length transaction, cost is what you give up to get something else, and money is a standardization of trade units that allow for marketplace transactions to occur, bitcoins are an attempt to create a new type of currency that is separate from a central system (such as government-issued currency) and that can also be deployed as an electronic payment system.

Throughout history, money has always been physical. The earliest coinage originated in Asia Minor about 2,500 years ago from an alloy known as electrum or "elektron" to the Greeks. It is composed of silver and gold, along with other trace metals, occurs naturally in nugget form, and is found in riverbeds. It worked well for its purpose prior to the development of technology needed to separate elements. Merchants allowed trusted customers to carry a tab (the first use of credit) and pay with electrum coins when the bill was sufficiently high. The nuggets varied in size and weight and were treated as bullion. The first designs on coins were simple striation lines, which mimicked the lines formed on the nuggets from the water flow in rivers. It was Aristotle that championed the importance of having an image on the obverse, which really transitioned bullion into true coinage.

In early colonial America, daily commerce was conducted using coins produced by the official mints of other established nations, along with a hodgepodge of tokens and medals issued by private individuals and mints from inside and outside of America. The first coins issued by the authority of the United States were the Fugio pieces in 1787, and they are some of my personal favorite coins. The design had 13 interlocking circles and a small circle in the middle with the words "United States" around it and the words "We Are One" in the center. On the other side there was a sundial with a meridian Sun above it, the word "Fugio" (the intended meaning is time flies) on the left, and the year 1787 to the right of the sundial. Under the sundial are the words "Mind Your Business," a saying credited to Benjamin Franklin. To me, this coin encompasses a lot of pride, solidarity, and hope for the young United States of America.

An important characteristic of a sovereign nation is the right to issue its own coins, and America began exercising that right in 1792 by issuing pattern coins, followed by copper coins in 1793, silver coins in 1794, and gold coins in 1795. Before the denominations we have circulating today, there have been some more unusual ones, starting with the half cent in 1793, two-cent pieces (1864–1873) in which the motto "In God We Trust" first appeared, along with three-cent pieces (1851–1889). There have also been half dimes (1794–1873) and twenty-cent pieces (1875–1878). Gold coins have been minted in denominations of $1, $2.50, $3, $4, $5, $10, and $20. Gold $50 and platinum $100 coins are issued today by the US Mint, but these are considered bullion. There have been various reasons for the different denominations, but bitcoin transactions can occur in fractions of a bitcoin, making them very versatile.

As our society moves to a cashless environment, I wonder how that will impact future coin collectors. Bitcoins will never become a collectable, since they lack the characteristics of physical coins. Blockchains are free to anyone and have no varying condition state from circulating. At some future point in time, there won't be a need for physical coinage and the billions of coins the US Mint currently produces each year will become obsolete. Will there still be an interest in collecting something that future generations would have never used for their intended purpose in their daily lives? Only time will tell.

The future of bitcoins is also unknown. Early investors had a wild ride with large gains followed by large declines as they sought to find bitcoins' true value in relation to other currencies. They had

started to obtain a reputation as taboo due to their use in criminal activities based on the notion that they can be held anonymously. But as Slava explains, bitcoins are not entirely anonymous and can be traced and tracked back to a unique IP address.

One thing is certain: bitcoins are becoming mainstream, and with their lower cost as a payment system, many merchants not only accept bitcoins as tender, some actually prefer them as a cost-saving method for processing electronic payments.

As you read this book, you will learn both the history and possible future of bitcoins. With Slava's in-depth analysis of the security aspect of bitcoin financial transactions, perhaps you will learn to prefer this cryptocurrency system as well.

Introduction

There are no conditions of life to which a man cannot get accustomed, especially if he sees them accepted by everyone about him.
—Leo Tolstoy

Several years ago I was fascinated by an experiment I did. I was trying to live cashless, paying only with plastic cards, either debit or credit. My attempt was pretty successful until I went on a business trip abroad. My first (but not last!) failure was in a restaurant, when I received a check without a placeholder for a tip amount. There were no problems paying with a credit card, but there was no way to add a tip to the bill. So I had to ask my friend (who was not participating in my experiment) to pay a cash tip. The payment system, even though it was "aware" of electronic payments, was not fully integrated into the world of plastic money. Such a situation is still common in many places, especially outside North America and Europe.

I would face similar challenges today if suddenly I decided to do the same experiment with bitcoin, but this time the limitations would be different. Instead of geographical borders that divide the world into cash and cashless zones, there is an invisible Rubicon between the offline and online worlds. In this new version of my experiment, I could live a sustainable life without cash (or plastic) if I didn't leave my house. I could shop online and even order food from local restaurants. Whenever I needed to make a transfer of traditional money, for example, to pay the commodity bills (still virtual but counted in dollars rather bitcoins), I could exchange my bitcoins online and convert them to dollar transfer. I could even earn a living by mining the cryptocurrencies at home. However, this pattern breaks very quickly when you go offline and enter traditional brick-and-mortar stores. Few retailers today accept bitcoin or any other cryptocurrency, despite the obvious benefits: convenience, security, lower transaction fees, and attracting new generation of customers.

One of the most important goals of this book is to help people who are not closely familiar with math and cryptography to understand crypto payments. In order to do it smoothly and wisely, we need to understand several things, the first being the place cryptocurrency has in the modern payment ecosystem.

Don't let the fact that this book is technical scare you if you are not a programmer. This book can still be read by anyone who wants to get paid or pay with cryptocurrency, and the first several chapters will prove it by answering very basic questions, such as what are the players in the existing electronic payments game, and whether it is possible to integrate bitcoin into it painlessly without breaking the major rules.

While I realize that the readers of this book might be in a sense obsessed with crypto payments, we should stay calm and remember that there were (and in fact still are!) other types of currencies and methods of payment. Although bitcoin enthusiasts often use the term "revolution," from many perspectives, especially from the merchants' point of view, creation of cryptocurrency is just an evolution of a payment system that was made possible by modern science and technology, namely cryptography and the Internet.

If you ask how to characterize bitcoin in a single word, many would answer "cryptography." Although I agree with this answer, it is too generic, so my answer would be more specific (but contain more words): "public-key encryption and hash function." Here is why.

If we analyze existing payment systems—predecessors of bitcoin—there are two main problems in their design: security and centralization. Security flaws in the design of payment cards resulted in the creation of PCI data security standards, which forced merchants, service providers, banks, and payment brands to invest billions of dollars into security controls, which eventually failed to protect them from data breaches. On the other hand, as you will see in part I of this book, centralized management of the first virtual currencies was the main reason for fiasco.

Bitcoin design provides solutions to both the security and centralization problems: *digital signature* and *proof of work*. A digital signature is based on public-key cryptography, while a cryptographic hash function is the essential part of both a digital signature and a proof-of-work implementation.

Before the invention of digital signatures, it was impossible to broadcast the message throughout a public channel such as the

Internet and verify through multiple recipients that this message was unchanged since its creation by the original sender. Along with public-key encryption, the cryptographic hash function made creation of a digital signature possible, which protects the *integrity of crypto transactions*—a solution for *security problems*.

At the same time, a cryptographic one-way hash function, besides its participation in digital signature design, made proof-of-work implementation possible, which is a solution for *centralization problems*.

So it's safe to say that if you understand the cryptography behind bitcoin, then you know how bitcoin and other cryptocurrencies work, so you can trust them.

PART I

From Coins to Crypto

In This Part

Chapter 1: Traditional Money
Chapter 2: Digital Gold
Chapter 3: Centralized Digital Payments
Chapter 4: Cryptocurrencies