Crypto Basics

A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors

—

Slava Gomzin

Foreword by Ken Westin

Apress®

Crypto Basics

A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors

Slava Gomzin

Foreword by Ken Westin

Apress®

Crypto Basics: A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors

Slava Gomzin
Frisco, TX, USA

ISBN-13 (pbk): 978-1-4842-8320-2 ISBN-13 (electronic): 978-1-4842-8321-9
https://doi.org/10.1007/978-1-4842-8321-9

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Gryffin Winkler

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 booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

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.

Printed on acid-free paper

To Svetlana
and our daughters Alona, Aliza, and Arina.

Table of Contents

About the Author

Slava Gomzin is a cybersecurity and crypto enthusiast, full-stack technologist, and entrepreneur. He is the author of multiple publications on information security and technology, including the books *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions* (Wiley, 2014) and *Bitcoin for Nonmathematicians: Exploring the Foundations of Crypto Payments* (Universal Publishers, 2016). *Hacking Point of Sale* became a handbook and the primary reference for many professionals in the payment, retail, and cybersecurity industries. Slava has designed and co-created two cryptocurrencies. GRAFT (GRFT), a CryptoNote blockchain-based two-layer payment network, was launched in 2018 and allowed secure, private crypto transactions with less than two-second confirmations. Lyra (LYR), a new generation blockchain for secure private closed-loop payment solutions, was launched in 2020 and was designed and coded from scratch using recent advances in crypto technologies. Lyra is based on DPoS and block lattice technologies and allows instant (less than one second) on-chain transaction confirmations. Slava is currently the director of software development at Toshiba Global Commerce Solutions, focused on payments R&D, product security, and cloud technologies.

About the Technical Reviewer

From Switzerland and currently working for AWS in New York, **Norbert Funke** has more than 20 years of industry experience with demonstrated success in all aspects of software engineering and information architecture. He has leading expertise in crypto, emerging data technologies, big data, and natural language processing (NLP), combined with deep industry experience in financial services and health care. He has worked in Europe, the United States, Australia, and China.

About the Foreword Author

Ken Westin is a security researcher who has been helping organizations with security analytics, threat hunting, and insider threat programs for the past 15 years and has aided law enforcement in investigations, unveiling organized crime groups in the process. His work has been featured in *Wired*, *Forbes*, *New York Times*, *Good Morning America*, and others, and he is regularly reached out to as an expert on topics including cybersecurity, insider threat, privacy, and surveillance.

Acknowledgments

Writing a book is not easy and one cannot succeed without help from other people. First of all, I would like to thank Susan McDermott for bringing this project to reality. Thanks to the entire Apress team, especially to Gryffin Winkler, for flexibility and support during this project. Thanks to my colleagues at Toshiba for establishing and maintaining a creative work environment. Also, I would like to thank my past and current colleagues in the crypto industry, especially Dan Itkis and Wuzhou Yang – without their dedicated work, I would have nothing to write about.

I would like to thank Val Abelhouse, whose questions helped inspire me to write this book. Thanks to Norbert Funke for his enthusiastic support and contribution. Special thanks to Ken Westin for his brilliant and genuine foreword. And finally, I want to thank my wife, Svetlana, for her continuous support and understanding.

Any opinions, findings, conclusions, or recommendations expressed in this book are those of the author and do not necessarily reflect the views of his respective employer.

Foreword

I met Slava Gomzin a decade ago; at the time, criminal hackers were successfully targeting major retailers' point-of-sale systems, harvesting credit cards en masse with customized malware specifically designed for these systems. The industry was in a panic and looking for help. At the time, I was working for a security vendor who specialized in monitoring the security configurations of these systems and wanted to learn more about how they are compromised. That is when I learned of Slava Gomzin's first book, *Hacking Point of Sale*, and I reached out to him with some questions, and he responded. Slava and I even did a joint webinar on the topic of point-of-sale malware, and we have been friends since. Slava is a great teacher and knows the ins and outs of payment systems unlike anyone else I know, from how transactions are made to how they're secured, and has a clear understanding of both the history and future of payment systems.

Like my interest in point-of-sale systems, my interest in cryptocurrencies was piqued when I saw it was being used in underground forums and by criminal syndicates who were taking advantage of the pseudo-anonymous nature of Bitcoin to evade detection by regulators and law enforcement. It has been disturbing to see how cryptocurrency and the underlying blockchain technology quickly became overhyped in mainstream media as a "get-rich-quick" scheme fueling a craze of speculative investment, often by individuals who did not understand the underlying technology or risks associated with such a venture.

This hype reminds me of another hype cycle in cybersecurity when every cybersecurity vendor claimed to have "Artificial Intelligence" solutions that would replace the security analysts, mostly in attempts

to land large rounds of funding from VCs. The promise of AI replacing security analysts not only turned out to not be true but also took attention away from the real and practical research that has been done utilizing machine learning which is a tool of AI to aid security analysts in their work, versus replacing them.

Similarly, the speculative investment hype around cryptocurrencies fueled by countless initial coin offerings and exchanges has taken attention away from the practical use of cryptocurrencies as actual currency, facilitating the decentralized exchange of goods and services. Instead, cryptocurrencies became centralized through exchanges and further diminished by associating with overpriced NFTs and Web3, all of which have made the crypto space appear to be more of a Ponzi scheme from the outside than a revolutionary egalitarian technology for the masses to circumvent existing centralized currency and controls. The unfortunate result of this speculative investment and hype is that the original intention of cryptocurrency, as laid out by Satoshi Nakamoto in the original "Bitcoin: A Peer-to-Peer Electronic Cash System" paper which gave rise to Bitcoin, is lost. Nowhere in the Satoshi Nakamoto paper is there a mention of investment in cryptocurrencies, mechanisms to exchange for fiat currency, or even tying Bitcoin's value to fiat currency; this all came later and was driven by greed and speculation.

It is important for businesses to understand how cryptocurrencies work to better understand where they can be used not as a speculative investment but how and where they can be used as a legitimate payment method. Many companies now accept cryptocurrencies such as Bitcoin, including AT&T, Microsoft, and Tesla, to name a few. Security professionals should be familiar with how cryptocurrencies work, as they are the de facto currency of cybercrime, whether it's used by cybercriminals to pay for services and tools or ransomware gangs demanding payment in cryptocurrency, taking advantage of their pseudo-anonymous nature. Financial professionals also need to know how cryptocurrencies operate as

there are increasing regulations related to the use of cryptocurrency due to its capability for financial crimes such as money laundering, as well as tax implications of trading cryptocurrencies.

In this book, Slava walks through how cryptocurrencies work, from how cryptocurrency is created and traded to how it is secured. He provides a history of currencies so the reader understands how cryptocurrency fits within a historical context and highlights how some of the popular cryptocurrencies, such as Bitcoin and Monero, work and how they are different from each other. This book isn't a get-rich-quick scheme like you may find with some other books that hype cryptocurrencies as an investment vehicle, but more a guide to explain how cryptocurrencies operate and function to demystify them so that you, the reader, can make educated decisions on how and why to make use of them.

—Ken Westin

Preface

I was exposed to the idea of Bitcoin for the first time relatively late, back in 2014, after I finished writing my first "full size" book, *Hacking Point of Sale* (Wiley, 2014), and right before I joined HP as security and payment technologist. I remember it very well because writing a big book for a big publisher for the first time is a disaster you never forget. So, after I finished the book and it was published, I felt like a free man once again and decided to leverage the short break between my jobs and learn something completely new. Bitcoin, fortunately, was the best candidate at the time.

I was fascinated by the genius of a person or a group behind Bitcoin. It's too bad we still don't know their real identity. Given my extensive background in electronic payments and cybersecurity, which are still my two passions in addition to crypto, I immediately started thinking about adapting Bitcoin and other cryptos to the real world of retail business so that they could break into the mainstream. Unsurprisingly, my research resulted in another book, this time about crypto. *Bitcoin for Nonmathematicians* (Universal Publishers, 2016) was my first attempt to reveal the dangerous gap between traditional payment systems and cryptocurrencies. But the book started identifying some issues and did not offer any solutions.

Fast forward one year, and I was fascinated for the second time by the power and beauty of cryptography behind another breakthrough in the crypto world. Monero (XMR), a privacy coin based on the CryptoNote protocol, in a "bitcoin style," was also designed by an anonymous person or group. Unlike Bitcoin, Monero hides all the details of payment transactions from the public view while keeping intact the main advantage of crypto – decentralization.

The cryptography behind Monero is a perfect fit for what Arthur Clarke meant when he said that "any sufficiently advanced technology is indistinguishable from magic." Despite remaining issues with scalability (ability to process multiple payments simultaneously) and transaction processing time (the time it takes to validate and approve a single payment), I felt crypto is ready to go primetime for the first time. So, my friend Dan Itkis and I came up with the idea of a new cryptocurrency called GRAFT (GRFT), aiming to elevate the crypto payment processing to the level acceptable for the big retail but without defeating the very foundation of the crypto – decentralization. I was so thrilled by the opportunity to disturb the industry and consumed by the project that I left my day job in a prestigious predictive analytics startup and interrupted my promising career path as a cybersecurity executive.

The first version of the GRAFT network was successfully launched on January 16, 2018, and GRFT, at some point, was among the top 25% of cryptocurrencies by market capitalization. However, the initial success was shadowed by the complexity of development, weak market demand, and crypto winter 2018–2019.[1] In addition, over the course of the development process, I realized that GRAFT would not resolve all the issues associated with the long-term goal of entering the mainstream payment processing. Scalability was one of them, but another was the lack of flexibility as GRAFT was a "solo" blockchain that could not carry other tokens. That's how the idea of new crypto, which we later called Lyra (LYR), was born.

I wrote the Lyra white paper, created a design, and wrote the initial proof of concept code by myself, from scratch, while Dan helped to form the idea. But the actual, working version of Lyra (we call it *mainnet* in crypto) wouldn't happen without Wuzhou Yang, super-programmer and Lyra co-creator.

[1] Max Yakubowski. What's Next for the Industry as 'Crypto Winter' Thaws? https://cointelegraph.com/news/whats-next-for-the-industry-as-crypto-winter-thaws

Lyra's design has been based on a combination of more advanced technologies, very different from Bitcoin or Monero: *block lattice* and *delegated proof of stake* (DPoS). This completely new tech stack allowed us to resolve all the preceding issues while enabling even more features. Thousands of transactions with various coins, tokens, and NFTs (non-fungible tokens) can be processed within milliseconds, with the wallet software's footprint so small that it can even be placed on a smartcard chip.

Lyra mainnet was successfully launched on September 30, 2020, and it is still in development. I believe Lyra has its unique niche in the crypto specter, and one day, once all the proposed features are implemented, it will demonstrate its full power. I also believe that my good and bad experiences, which I sincerely share with the readers of this book, will help them succeed in their own crypto journey.

Introduction

I am not in the business. I am the business.

—*Blade Runner: The Final Cut*. Director: Ridley Scott

For many centuries, creating money was a king's privilege. Money was (and still is) associated with the higher power, and so monarchs were marking their reign by minting new coins with their portraits, like a golden *Louis d'or* coin first created by King of France Louis XIII in 1640 (Figure 1).

Figure 1. *Half Louis d'or coin minted in 1662*

Later on, state governments took over the right to mint and print new money. But things still change, faster and faster these days, thanks to industrial and technological revolutions. The invention of cryptocurrencies pushed the borders of possibilities even further: it

allowed virtually any group of people, or even individuals not associated with any government or corporation, to create their own money. They typically don't call it money and put various explanations around their "tokens" utility. But in reality, it is what it is: money. Crypto tokens can be counted, divided, transferred, exchanged, and even minted, so they have all the necessary attributes of money.

With recent developments in crypto – an introduction of NFT (non-fungible token) – you can even put your face on your coin if you wish, similar to kings' coins. But I leave open the discussion about the nature of crypto and where it belongs and let other people decide whether crypto is, in fact, money or not. I would instead focus in this book on how to use it and, yes, how to create it – just in case you'd like to create your own… crypto.

I learned at least three things while speaking about crypto on multiple occasions.

First, most people are fascinated by the whole idea of crypto, but at the same time, they are typically interested in different aspects of it. The two major areas are technical and financial, which are also fragmented. For example, the technical side includes massive subdivisions such as cryptography, decentralized networking, and distributed consensus. But there are other aspects: economic, political, humanitarian, and psychological.

Second, it is impossible to explain the crypto phenomena in only technical or economic terms. The genius of the bitcoin creator (or creators?) is that she/he/they compiled multiple mandates for ultimate digital money in a single outstanding invention, which includes a decentralized payment network and economic policy on top of blockchain and distributed consensus with all the math around them.

And finally, the third thing I realized is that most people don't fully understand what crypto really is and how it works. Some of them get the basics of crypto financials but don't understand – and, as a result, underestimate and don't trust – the power of cryptography, distributed

consensus, and, most importantly, the decentralized nature of crypto. This is, by the way, one of the main reasons for crypto to remain outside of mainstream payment and banking industries.

But I am still optimistic – after all, it's been less than 15 years since the Bitcoin white paper was published. It took us centuries to switch from metal to paper to electronic money, so 15 or 20 years would be a reasonable time to move from plastic to crypto. It's worth mentioning that this transition is not just about going from plastic cards to digital wallets. There is much more to that – moving from a centralized banking system controlled by national governments and corporations to decentralized financial networks, which are open across borders and do not belong to anyone!

Why Do We Need Crypto?

To get a definitive answer to this question, let's first look at the Bitcoin white paper – the document that proposed the first crypto. This is the first (but not the last) time I am going to cite the original Bitcoin white paper, which defines the very first crypto as an "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[1] The two key declarations here are *payment system* and *without the need for a trusted third party*. In other words, crypto is a decentralized financial system that any national government or corporation does not control. Thus, the two prominent use cases for crypto are *peer-to-peer payments* and *frictionless funds transfer* (which is a superset of payment, but there is a vast difference which will be described in Chapter 7). Let's review some examples for these two use cases.

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf

Imagine you own some real estate in Russia or Argentina, and you want to sell it and transfer proceeds to your US bank account. Many real estate deals in these countries are still done using cash. So, you need to open a local bank account, deposit the cash, exchange it for US dollars, and then transfer it to the US bank. While technically, it is a relatively simple operation, which can be done using SWIFT (an international banking funds transfer system) or Western Union (another system for international money transfers), it's not an obvious task given the relatively large amounts of real estate transactions, the current state of the political and economic relationships between some countries, and local financial regulations and cultural differences.

With crypto, however, money transfer is simple: buy Bitcoin (for example) in one country and sell it in another country (or just spend it without even exchanging it for the local fiat[2] currency). Most countries today have legal and unofficial exchanges, both online and physical, where local fiat currency can be exchanged for crypto, and then crypto can be converted to different fiat currency in another country. Crypto does not recognize national borders and exists everywhere as long as there is access to the Internet.

Typical payment use cases differ from funds transfers, but payments can also be made using crypto, especially when traditional payment methods are unavailable. Here is, perhaps, not the best example, but at least very well known: ransom payment to ransomware attackers. One of the significant ransomware attacks on the oil pipeline resulted in a 75 BTC (bitcoins) payment, equivalent to $4.4 million.[3] Given the amount and nature of such payment, it would be impossible for the attackers to process

[2] Fiat currency is the money issued by a national government and is not backed by any commodity such as gold. Examples: US dollar, Euro, the British pound.

[3] Tom Robinson. Elliptic Follows the Bitcoin Ransoms Paid by Colonial Pipeline and Other DarkSide Ransomware Victims. May 14, 2021. www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims

it via regular bank wire transfer or credit card. But crypto payment can be made regardless of the physical location of the payer and payee, who can also stay anonymous. However, there is only a certain degree of anonymity that can be provided by "regular" crypto, such as Bitcoin – we will review this issue in detail in Chapter 5.

Finally, another use case was not even foreseen (or at least not described) by the genius Bitcoin creator(s) – trading and investment. The fact that crypto prices fluctuate attracts short-term traders, while the common trend of historically growing crypto prices attracts long-term investors. We will review crypto trading and investment in Chapter 11.

What This Book Is About

This book has been written for a broad audience. The title, ambiguous at a glance ("Creating Your Own Money"?), in fact, is double-barreled, which is also hinted at by this phrase: "For Investors and Inventors." Yes, you understood it correctly. I will show you both how to use crypto (buy, store, transfer, trade, and invest) as well as how to create your own one – depending on your goals, not to mention the fact that you need to know how to handle crypto before you can create a new one, don't you? Also, in both cases, you need to understand how crypto works, first, on a high level, and then even more in depth.

You own your crypto money no matter who you are – user or creator. Think about it. When you simply buy crypto, you get the money that does not belong to any government or corporation, and it only belongs to you. You own your money created by someone for you and other people. When you create new crypto (maybe it sounds like a very hypothetical case to you right now, but I will show you how relatively simple it is in reality), you own new money that others also can use. With that said, the title is not just double-barreled but also a little bit sarcastic because, let's face it, you cannot just create your own money entirely out of thin air.

Creating money is not just a technological act. While crypto is a pure product of technology, money results from the collective consciousness. Everyone can potentially create their own crypto. Then, it can or cannot become money. I will show you how to create your own crypto, and I will explain how some crypto might or might not become money, but I cannot guarantee that the crypto you have created will ever become money. If you are eager to create your own crypto project, I'm not going to demotivate you, but you should build the right expectations. There will be a comprehensive review of this process in Part III.

Another goal of this book is to explain crypto while reviewing its integral parts in detail. This book is focused on two top aspects of crypto: technical and financial, and their subdivisions such as cryptography, decentralization, distributed consensus, monetary policy, security, privacy, and payment processing capabilities.

When you finish reading this book, you will understand all these elements and how they work together. You will understand Bitcoin and any other cryptocurrency and be ready to start doing a business with crypto. To become savvy enough about crypto, you don't have to learn the math behind cryptography and distributed consensus. In addition to explaining the crypto basics in layman's terms, this book also offers different parts for various audiences.

While Part I gives an overview of the technologies around crypto, Part II provides practical knowledge necessary to dive into the crypto business, such as investment, trading, and even creating your own crypto project, which is covered in detail in Part III. Just check out the table of contents and select what you want to learn.

What This Book Is Not About

Before we dive into the depths of the crypto ocean, it's also important to mention what this book does not cover, just to help the readers build the right expectations.

First, this book is not a "how to get rich" guide. While it contains an analysis of financial and economic aspects of crypto, because it is almost impossible to conduct an intelligible conversation about crypto without mentioning money, it still puts a more significant emphasis on the technical side when it comes to crypto creation schemes. And, once again, as you will see, not every crypto ends up as money.

Another important "not" is the use cases not associated with the payment or financial systems. The Bitcoin white paper defines Bitcoin as a payment system. But just as not all cryptos are based on the original blockchain technology proposed by Bitcoin creators, not all blockchains are payment systems. There is an army of inventors who fanatically try to apply blockchain database technology to all aspects of our life, no matter if it's appropriate or not. It often looks like an attempt to use a jet rocket engine in a car: it will drive (or fly?), perhaps faster than a traditional car, but no one would use it in real life because there are less expensive and safer gasoline or electric engines that are more suitable for cars. In the same way, there are traditional relational or NoSQL databases that are more suitable in most cases for solutions outside of FinTech. Even though some attempts to use a blockchain database and decentralized tech outside of their original intended area might be pretty successful, they will remain out of scope for this book which is focused solely on crypto.

And finally, I am not a professional investor or trader but rather living on the "opposite" side of the barricades. So, this book cannot be viewed as a professional crypto investment or trading guide but rather as a starter and helper. There are many books on trading and investment, and some books in this area explicitly target crypto. With that said, when you deal with crypto projects day to day, from the very beginning to coding to the actual listing of the trading pair on an exchange, you must understand the motivation and behavior of the "other side" – people who view the crypto as a purely financial instrument.

Besides being an amateur investor and trader by myself, I know some professionals in this area. They don't need anyone to teach them to do what they know to do well already. They are looking for a guide on getting started that answers some basic but essential questions: What is crypto? How does it work? And finally, what are the right things to begin with, and what is no go? They will find answers to those questions in this book. In addition to understanding what's under the hood, an insider's overview of crypto technology and economy should help investors and traders estimate the potential of a particular project and even try to predict its future.

Some Basic Terminology

Before we continue, let's agree on some basic industry jargon.

First, *crypto* is the same as *cryptocurrency*. We simply save some time, ink, storage space, power, and paper by using crypto instead of cryptocurrency. Cryptocurrency is also a shortcut for *cryptographic currency*, which is essentially a money and payment system combined together and based on cryptographic algorithms. Now try to count how much more ink and paper we just saved.

Next, *blockchain* is not the same as crypto. Most cryptos are based on blockchain, but other essential technologies are required for crypto to exist, and blockchain is just one of them. Blockchain is just a type of database where records, financial transaction records in the case of crypto, are stored in chained blocks. Another name for such a database is *distributed transaction ledger*. The blocks are linked one after another to form a chain. It's worth mentioning that all crypto use some kind of database to store transaction records. Still, it's not always the same blockchain technology invented by Bitcoin creator(s), and it's not even always called a blockchain. Read more about types of distributed transaction ledgers in Chapters 2 and 3.

A *network node* is another important term. It's often simply called a *node*. This is typically a computer, server, or a group of servers running crypto software. The nodes are linked to each other through the Internet and comprise a crypto network, often called the *mainnet*. Each node maintains its own copy of the transaction ledger (such as a blockchain). The nodes constantly sync with each other to make sure their copy of the blockchain is up to date.

Another exciting term associated with crypto is a *fork*. The fork is created when two parallel versions of blockchain are started from the same original blockchain, for example, when developers release a new version of crypto node software. The fork might create two temporary versions of the same blockchain or even a new cryptocurrency. In many cases, the fork is the standard way to upgrade the cryptosystem or maintain the distributed consensus. There are different types of forks: *soft fork*, *hard fork*, and *temporary fork*.

In simple words, a *soft fork* is a minor update, while a *hard fork* is a major network update that creates a new version of blockchain that is not compatible with the old one. Typically, the new version of the blockchain gradually replaces the old "forked" version as node operators update their nodes.

The hard fork is also the way to create new crypto from the existing one. For example, Bitcoin Cash is a hard fork of Bitcoin. New crypto based on another crypto code base is also called its fork. For example, Litecoin is a fork of Bitcoin because its code is forked from Bitcoin code. And finally, a *temporary fork* can be created during the *mining* process, which we will review in Chapter 2.

The crypto community creates much more industry jargon, but we will introduce it gradually in the following chapters as we move forward by describing different aspects of crypto.