The Blockchain Developer

A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects

—

Elad Elrom

Apress®

The Blockchain Developer

A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects

Elad Elrom

Apress®

The Blockchain Developer

Elad Elrom
New York, NY, USA

ISBN-13 (pbk): 978-1-4842-4846-1 ISBN-13 (electronic): 978-1-4842-4847-8
https://doi.org/10.1007/978-1-4842-4847-8

Managing Director, Apress media LLC: Welmoed Spahr
Acquisitions Editor: Louise Corrigan
Development Editor: James Markham
Coordinating Editor: Nancy Chen

Cover designed by eStudioCalamar

Cover image designed by Chris Barbalis on Unsplash

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 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 www.apress.com/bulk-sales.

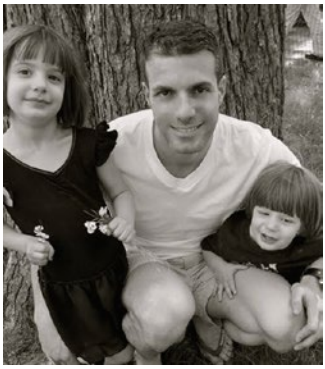
Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484248461. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

I would like to dedicate this book to my children, Romi Scarlett Elrom and Ariel Rocco Elrom. Have solid boundaries, and don't allow anyone to dictate what you cannot achieve or cannot do. I love you very much and will always be there for you.

Table of Contents

About the Author



Elad Elrom is a coder, technical lead, and technical writer. As a writer, he has co-authored four technical books. Elad has consulted for a variety of clients, from large corporations, such as HBO, Viacom, NBC Universal, and Weight Watchers, to smaller startups. Aside from coding, Elad is a certified PADI dive instructor and an accomplished certified pilot. You can contact him at `elad.ny@gmail.com`.

About the Technical Reviewer

Nishith Pathak is India's first Artificial Intelligence (AI) Most Valuable Professional (MVP), a Microsoft Regional Director (RD), a lead architect, a speaker, an AI thinker, an innovator, and a strategist. Nishith's expertise lies in helping Fortune 100 companies design and architect next-generation solutions that incorporate AI, machine learning, cognitive services, blockchain, and many more. He sits on several technical advisory boards across the globe and is the author of multiple books on AI and blockchain. Nishith has played a PAN account enterprise architect role where he was responsible for everything from the overall architecture to the design in multiple projects. He is an internationally acclaimed speaker on technologies such as AI and blockchain and regularly speaks at various technical conferences.

For his expertise on artificial intelligence, Microsoft awarded him the first Most Valuable Professional in the Artificial Intelligence category. Globally, he is among 19 MVPs on AI, recognized by Microsoft for their sheer expertise in AI. He has also been awarded the Microsoft Regional Director award, bestowed upon 150 of the world's top technology visionaries chosen specifically for their proven cross-platform expertise. Nishith is currently working on key areas such as artificial intelligence, machine learning, cognitive computing, blockchain, Internet of Things, and cloud computing; he helps companies architect solutions based on these technologies.

He can be contacted at NisPathak@GMail.com or found on LinkedIn (https://www.linkedin.com/in/nishithpathak/), Twitter (http://twitter.com/nispathak), or Microsoft (https://rd.microsoft.com/en-us/nishith-pathak).

CHAPTER 1

Blockchain Basics

This chapter will serve as your ground school before you "take off" toward development. It will introduce basic concepts that will help you to understand the blockchain technology. This chapter is split into four parts.

- Introduction to Cryptoeconomics
- Blockchain Explained
- Cryptocurrencies Overload
- Blockchain P2P Network

To understand cryptoeconomics, you first need to understand concepts such as encryption and decryption, private-public keys, cryptography, digital assets, cryptography, and cryptocurrency.

Once you understand these basic concepts, I will cover blockchain. I will cover the pieces that make up an individual blockchain, such as blocks, and how the blocks are linked together, as well as the problems with blockchain such as double spending. I will also explain cryptomining, cryptominers, and cryptocurrency wallets.

Then, I will cover the different types of cryptocurrencies: bitcoin, tokens, and alternative cryptocurrency coins (altcoins).

Last, I will cover the P2P network that is used with the blockchain technology and the different layers that make up the network: consensus layer, miner layer, propagation layer, semantic layer, and application layer.

E. Elrom, *The Blockchain Developer*, https://doi.org/10.1007/978-1-4842-4847-8_1

Introduction to Cryptoeconomics

The world of crypto is full of technical jargon that can confuse even the savviest technology ninja. Bitcoin introduced the concept of cryptoeconomics and paved the way for the creation of many blockchain platforms. Before we dive deep into how a blockchain works, let's understand what cryptoeconomics is and the underlying concepts behind a blockchain.

Verbal communication is based on selecting words to describe a message you want to convey. However, sometimes you want to communicate with only certain people while excluding others. A good example is during wartime; a commander communicates with soldiers stationed on the front line while ensuring the enemy is unable to listen. The commander could use encryption for this communication.

Electronically speaking, today all shopping sites offer their merchandise over an encryption protocol, called Secure Sockets Layer (SSL), that can protect your personal information from hackers. Video encryption and decryption are common to ensure the delivery of video to authorized members only, and on personal computers, people often use encryption to back up and protect files and passwords.

Moreover, as a developer, you likely sent encrypted messages and also decrypt incoming messages with the help of libraries as all programming languages offer string encryption and decryption functions.

So, let's look at some definitions:

- *Encryption*: Encryption is a process of converting your message into code so that only authorized parties can access it.
- *Decryption*: Decryption is reversing the encryption process so that the message can be converted to the original message.

- *Cryptography*: This is using the techniques of encryption and decryption to send and receive messages.
- *Cryptocurrency*: This is using cryptography the same way as the earlier SSL or video example but specifically to fit the needs of a digital asset.

Note A *digital asset* can be anything of value, such as the combination to your home safe, a secret password, a list, a message, electronic cash, a document, a photo, and so on.

- *Cryptoeconomics*: This is the combination of cryptography and economics to provide a platform to pass digital assets.

For further clarification, let's look at these terms in more detail and apply them to the topics I will be covering in this book.

Ig-pay Atin-lay

To begin, let's go back in time. Have you ever spoken as a child in Pig Latin? The secret Pig Latin language is simple. You take off the first letter of the word you want to say and then move the letter to the end of the word, as well as add the sound "ay."

For example:

- "Pig" become "ig-pay."
- "Latin" becomes "atin-lay."

What we just have done is encryption. Then to understand the words we have encrypted, we need to work backward.

- "Ig-pay" becomes "pig" by removing "ay" from the end and taking the last letter and putting it as the first letter.
- Similarly, "atin-lay" becomes "Latin."

What we have just done is decryption. Children are able to use these techniques to encrypt and decrypt words in a simple form of cryptography.

Encryption/Decryption

Encryption enables you to pass messages between specific parties in a secure manner so excluded parties will not understand them. Throughout history, there was a need to be able to send secret messages between parties. One party sends an encrypted message at one place, and then the other party is able to receive and decrypt the message elsewhere.

In fact, encryption was used a lot during World War I (WWI) and World War II (WWII). The Nazis used a machine called Enigma to encrypt and decrypt messages (see Figure 1-1). The Allies figured out a way to break the Nazi Enigma machine's secret code and decrypt the messages. This is believed to have shortened WWII by years.

Figure 1-1. *Enigma machine. Photo credit: wikimedia.org.*

Encryption and decryption went from pure Army usage to public usage by way of the development of the Data Encryption Standard (DES) by IBM in 1970 and the invention of key cryptography in 1976. In fact, in the past, cryptography and encryption were synonymous.

Encryption + Decryption = Cryptography

As mentioned, cryptography is the process of using the techniques of encryption and decryption. The word *cryptography* came from the Greek word *kryptos*, which means hidden or secret.

In the Pig Latin language example, I described how you can encrypt and decrypt words. That technique of removing the first letter and adding it to the end with "ay," and then vice versa, is cryptography. Without knowledge of the technique, you wouldn't be able to understand the Pig Latin language.

Most people are probably smart enough to figure out the secret Pig Latin language as it's simple in nature; however, a complex encryption example would be a different story.

For instance, going back to the WWII Enigma machine, the Nazis were passing messages over the air. The Allies were capable of receiving these messages (the messages were the "public keys"), but without a way to decode them (the "private keys"), it was not enough. It took a scientist named Turing and others five-and-a-half months to decrypt the Nazi's secret messages.

Note A cryptographic *key* can be used to encrypt a message. The encrypted message can then be decrypted only by using the second key (a private key) that is known only to the recipient.

Turing's contribution was to automate a machine that was capable of figuring out different settings the Nazis made in their Enigma machine so they could decrypt messages In other words, it automated the process of searching for the private key. That machine was called *bombe*.

Digital Assets + Cryptography = Cryptocurrency

Cryptocurrency is a digital asset designed so that electronic cash is able to be exchanged using strong cryptography (encryption and decryption) to ensure the security of funds, transactions, and the creation of new funds.

The cryptography's private key mechanism must be strong enough that it would be almost impossible (in other words, take too much time and effort) to figure out. Otherwise, all users could potentially lose their electronic cash if the cryptography could be figured out within a few months such as with the Enigma machine.

An example of cryptocurrency is bitcoin. Although bitcoin was not the first cryptocurrency invented, it's generally considered the first successful cryptocurrency.

Bitcoin's success is attributed to the following characteristics: no one can break the public-private key, it's distributed without a controlled government, it's publicly available, and it's published as open source code.

Note Bitcoin was invented in 2008 by Satoshi Nakamotoi with the publication of a white paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" (`https://bitcoin.org/bitcoin.pdf`). The actual complete open source software was released a year later in 2009 (`https://github.com/bitcoin/bitcoin`).

Cryptography + Economics = Cryptoeconomics

Cryptoeconomics is the combination of cryptography and economics to provide a platform that gives an incentive to maintain the platform, its scalability, and its security; in addition, it is absent of central or local government control. In other words, it's *decentralized*. The network is made up of a collection of multiple computers instead of one central computer.

Note Decentralized is the opposite of central control; it means without central or local government control.

Bitcoin is able to achieve cryptoeconomics' goals by using the private-public key concepts; cryptography and cryptographic hashing functions are used indirectly. In fact, the relation between cryptography and cryptocurrency is indirect not just for bitcoin but for most cryptocurrency out there.

For instance, cryptography is used in bitcoin in other ways such as the following:

- Bitcoin uses private keys (bitcoin calls these *digital signatures*) with the help of an algorithm function (called the ECDSA elliptic curve) to prove ownership.
- Hashing algorithms are used for holding the structure of the database ledger data (or blockchain) via a hash generator called SHA256.
- The hashing algorithms are used to generate math puzzles that a computer tries to solve for a prize. Once the puzzle is solved, the computer is selected to help handle the transactions.

- Hashing algorithms are also used to generate account addresses.
- There is the concept of Merkle trees (covered in the next chapter), which use the hashing keys of large data in small pieces. This is useful for lightweight wallets that are needed on constrained hardware devices such as mobile devices.

Bitcoin does not gather identity information for its users; however, the transactions are public, meaning that all the information is transmitted and available online. Think of the Enigma example again; this means that anyone can intercept the messages transmitted. However, without the private key, no one can decrypt the messages.

Since the release of bitcoin in 2009, there are many other platforms that use different types of privacy for sending information in a secure manner and that use encryption for more portions of the process so that less information is public. Platforms such as Monero and Zcash use anonymity via cryptography even for messaging a transaction's details.

Blockchain Explained

As I mentioned, bitcoin was the first successful open source digital cash. Blockchain is the core technology, or the heart behind bitcoin and in fact behind all cryptocurrency platforms.

But what is blockchain?

In short, a *blockchain* is a shared digital ledger. Think of a database that instead of storing all the database entries on one computer it stores the data on multiple computers. A fancier definition would be that a blockchain is a decentralized and distributed global ledger.

Blocks + Chain = Blockchain

Each block contains records and transactions; these blocks are shared across multiple computers and should not be altered absent an agreement (consensus) of the entire network. The network is ruled according to a specific policy. The computers are connected on one network and called *peers* or *nodes*.

Note What is blockchain? A *blockchain* is a digital decentralized (no financial institutions involved) and distributed ledger. In layperson's terms, it is a database that stores records and transactions on multiple computers without one controlling party and according to an agreed policy. The data that is stored is a block, and the blocks are linked (chained) together to form a blockchain.

Linked Blocks

A blockchain consists of a collection of data (a *block*) linked to the previous block. How are they linked? A block contains data, and each block references the block preceding it, so they are linked just as a chain link would be connected to the chain link before it. Take a look at Figure 1-2; as you can see, each block is referencing the previous block.

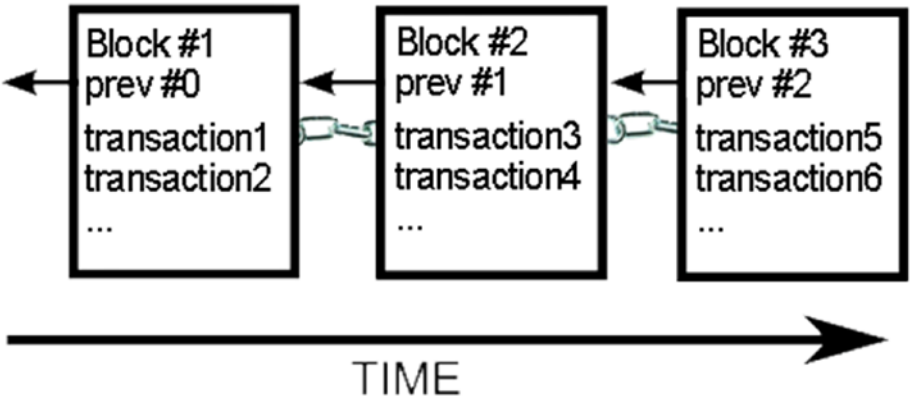


Figure 1-2. *Blocks chained together*

So, a blockchain contains blocks, which hold records of transactions. The private keys are held by the owner to show proof of ownership (this is the digital signature), so no one without the private key can decrypt the string and claim ownership. This combination of public keys and private keys represents the electronic cash.

Note Peers form a network of nodes, so throughout this book, you may see the word *peer* or *node*. These words are synonymous for the purpose of this book.

As I said, digital assets can be anything—a music file, video file, electronic document, and so on. In cryptocurrency, a digital asset is represented as electronic cash; you can think of the public key as your bank account and routing number and the private key as the actual cash in your account. Yes, you can share your bank's information with others, but the funds will stay in your account. To claim your cash, you need to prove ownership. You go to the bank and show a form of ID and prove it's you by a way of signature; only then can you get your money out of your account. A similar process happens with cryptocurrency. There is a public address

that represents your account, and only the owner holds the private key to prove ownership.

Double Spending Problem

A digital signature (public keys and private keys) securely ensures a party's identity is kept private and electronic cash is stored.

This concept of a private-public key combo enables you to encrypt and decrypt strings and keep a string safe, just as you saw with the Enigma machine. However, it is still not enough to solve the biggest problem of digital currency—double spending.

When you use fiat money (a paper money made legal by a government) such as U.S. dollars or euros, the paper is inconvertible, which means that once you gave the paper away, you cannot spend it again. In cryptocurrency, what happens if you prove ownership and send your digital asset twice at the exact same time? This could lead to *double spending*.

Hackers can try to reproduce digital assets as well as potentially double spend them, which cryptocurrency had to solve before it could be used as a digital currency.

Note *Double spending* is the risk that digital currency can be spent twice because the digital signature could be reproduced and one could prove ownership and send a digital asset twice at the same time.

Blocks that hold keys are not enough to provide security and solve the double-spending potential issue to form a digital currency.

Bitcoin solves this problem by creating a network of computers and proving that no attempts of double spending have occurred. This is done by having all the computers on the network aware of every transaction. All the transactions are shared with all the computers in the network.

Double Spending Solution: P2P Network

In cryptocurrency, using a peer-to-peer network provided the solution to solve the double-spending problem.

Note *P2P networking* is a distributed application architecture that splits the tasks that need to be performed between different peers, with each peer having the same privilege. Together the peers create a P2P network of nodes.

Any computer that is connected on the network is called a *peer*. The peer can be any computer that meets the network requirements such as a laptop, mobile device, or server. The computers are connected to each other on the Internet via a P2P network protocol and form a network of nodes.

The P2P network protocol is not new. It has been used extensively on the Web for years now, from downloading files via Kazaa or LimeWire networks to having video chats via Skype.

As I mentioned, bitcoin was the first viable cryptocurrency, and it solved the double spending issue as well as allows electronic cash to be stored without going through financial institutions by utilizing P2P to form the blockchain protocol.

> *"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."*
>
> —Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*

Cryptomining by Cryptominers

As noted, each computer that holds a copy of the shared ledger and is connected to the P2P network is a peer. A peer can help to add records and verify transactions. The process is called *cryptocurrency mining* or *cryptomining*, and the peer that helps record and verify the transactions is called a *cryptominer* or a *miner* for short.

Each miner helps to verify and add transactions to the blockchain digital ledger. The miners are often rewarded with a fee for the work, and to stay competitive with other miners, the miner usually needs a computer with specialized hardware.

Cryptocurrency Wallet

I covered what the public keys and private keys are and how they are used to encrypt and decrypt strings. The strings are digital currency or cryptocurrency, and the keys represent digital money.

A *cryptocurrency wallet* stores one or multiple public key and private key combinations and is used to receive or spend cryptocurrency.

A good analogy is to think of a wallet like your bank account. Cryptocurrency can be created by getting a reward by doing the miner work, or it can be purchased. I will expand on wallets later in the book.

Cryptocurrencies Overload

Before diving deeper into the blockchain P2P network, you should know that another concept that can cause confusion is the difference between coins and tokens. According to Coinmarketcap.com, at the time of writing, there are 1,833 listed cryptocurrencies with a market cap of $200 billion.