First edition

MASTERING MONERO

The future of private transactions

Written by Serhack

Co-authored by the Monero Community

Preface

Writing Mastering Monero book

I am Nico ("SerHack"), an Italian security researcher, a Monero contribuitor, and the publisher of this book. Finding good resources and learning about cryptocurrencies can be a daunting task. For new users, it can be especially challenging to track down documentation written at an understandable technical level. When I first started learning about Monero, I had to spend a great deal of time seeking out and evaluating many different resources on the topic.

The community decided to write Mastering Monero to guide you along this journey, whether you're setting up your first wallet or curious about the 'under the hood' technical details. The first few chapters are written for anybody curious about why and how to use Monero; they contain easy-to-understand explanations and examples, alongside instructions for practical use. Later chapters progress into more advanced topics, compiling information for developers who wish to build and contribute to the Monero project.

My adventure into the world of cryptocurrencies began when I learned about Bitcoin in January 2016. From the beginning, I have been concerned about the ramifications of its transparent public ledger. Since Bitcoin and most other cryptocurrencies are built around openly-linked addresses and coins with clear histories, transactions often inadvertently expose users' personal financial details. Every address balance is public information, which allows anybody to research your income, spending habits, and amount of cryptocurrency wealth. This can lead to undesirable consequences, such as price manipulation based on wallet balance.

I thought that Bitcoin was the only cryptocurrency until a friend introduced me to Monero in May 2017. I was blown away by its beautiful new paradigm: a world where vulnerable details such as account balances and transaction amounts are kept confidential to protect both the sender and the receiver. With privacy features implemented by default and always required, the entire Monero blockchain is veiled and users do not even have the option to accidentally send revealing transactions.

Recognizing the importance of this project, I began looking for ways to contribute to the community. I quickly saw an opportunity to support mass adoption by building payment gateways for online businesses, so I spearheaded the Monero Integrations project. This open-source codebase is designed around Monero's privacy-centric mentality: no signup or third-party service is required, since funds are routed directly to the recipient's wallet. The Monero community was very supportive throughout this endeavor, and the entire enterprise was crowdfunded by donations through the Monero Forum Funding System (FFS).

While working on the Monero Integrations project, I learned that the lack of a comprehensive guide to Monero was an obstacle both for end users and prospective contributors. This need for a thorough guide inspired me to write Mastering Monero as a universal resource for our global community. I am grateful for the generous FFS support that has made it possible to publish this document as a free eBook (and physical book!) for the general public. Whether you read Mastering Monero cover-to-cover or jump through sections pertinent to your questions, I hope you enjoy learning about Monero and the exciting projects within the community.

How this resource is organized

This book is organized roughly in line with the dependencies between the different topics covered.

The first chapter will show how the blockchain resolves several problems with our mainstream economic system and banking system in particular. However, the blockchain is not a full solution to our cryptocurrency needs. One problem still remains: Assuring the privacy of online transactions. With Monero, we will realize what privacy is and why we care about it. This will be helpful and useful for newbies and for users that sometimes forgot the Monero principles.

The second chapter starts to explore the "practical" applications of Monero: we will understand the different types of existing wallets, learn how to create one with Monero GUI, and finally find out how to get our first Monero.

We will explore how Monero actually works in the third chapter. Here we will discover how the Monero Team developed a cryptocurrency that hides transactions from third parties by default.

The fourth chapter is for any users that want to help the community in order to translate, build or improve Monero in any way. No worries about how we can help, the important part is doing that! We will join the Monero community!

The fifth chapter overviews a “hot”-topic argument: the mining process which is confirming transactions for other users. We’ll see what it’s and why it’s important in order to guarantee a solid and trustable system for our transactions.

After five chapters of introduction based on getting started, mining, building, and learning how Monero works we will dive into the internals Monero more deeply. This chapter includes a lot of technical details about Monero, especially Cryptography details. Stealth addresses, Ring Transactions, and Ring Confidential Transactions won’t be buzzwords anymore since you’ll be informed on how they work from the math-up. For developers and experts only, the sixth chapter will be the technical explanation of the CryptoNote Protocol. If you can’t understand any of the explanations included in this chapter, don’t say we didn’t warn you: this book is called Mastering Monero for a reason.

In the seventh chapter, we will step back to look at the Monero network and a sub Monero project Kovri, an open source C++ I2P implementation. We’ll know why it’s important and why it’s being developed. You will be an expert about Nodes and P2P protocol.

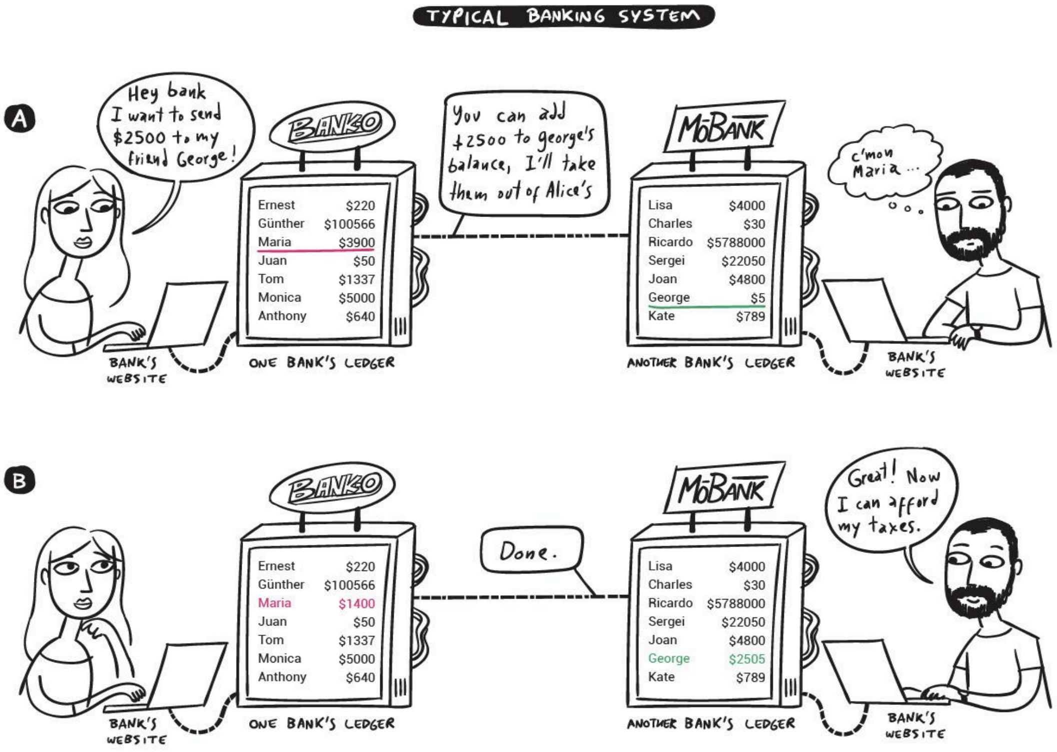
When we have finished read the first seven chapters of the book, we’ll begin to think how to incorporate Monero into our finances. If Monero is such a revolutionary cryptocurrency, how I can integrate Monero to my business? The eighth chapter will provide you all the answers to these questions. From the JSON RPC to the OpenAlias sub project, everyone can start accepting Monero.

Chapter 1
Introduction to Cryptocurrency

Meet Maria and her best friend George, who decide to meet up for a vacation. George's budget is tight, so Maria offers to send some money to help pay for the flight, hotel room, and food.

If Maria sends the money to George through the traditional banking system, they trust two intermediate parties (their respective banks) to symbolically move the funds for them.

There is no actual movement of physical bills or assets, both banks simply edit their respective database to show that the funds have been moved. When Maria submits the transaction to her bank (whether that's online, on her bank app, or a check), her bank subtracts $2,500 from her account balance on their ledger, then contacts George's bank and requests that they add $2,500 to George's balance, so that he can withdraw the funds to pay for travel expenses.


TYPICAL BANKING SYSTEM
A
Hey bank I want to send $2500 to my friend George!
BANKO
You can add $2500 to george's balance, I'll take them out of Alice's
MōBANK
c'mon Maria ...
BANK'S WEBSITE
ONE BANK'S LEDGER
ANOTHER BANK'S LEDGER
BANK'S WEBSITE

Ernest	$220
Günther	$100566
Maria	$3900
Juan	$50
Tom	$1337
Monica	$5000
Anthony	$640

Lisa	$4000
Charles	$30
Ricardo	$5788000
Sergei	$22050
Joan	$4800
George	$5
Kate	$789

Ernest	$220
Günther	$100566
Maria	$1400
Juan	$50
Tom	$1337
Monica	$5000
Anthony	$640

Lisa	$4000
Charles	$30
Ricardo	$5788000
Sergei	$22050
Joan	$4800
George	$2505
Kate	$789

Figure 1 Maria sends some money to George by using a traditional banking system

There are a few drawbacks and risks to this system, and it requires total trust of banks. Maria, George, and the banks must act on faith that transactions are legitimate and that the ledgers are kept honestly. This trust in the intermediate third parties poses a risk, since the banks or a nefarious actor may create unlimited money by fraudulently editing the ledger balances or transaction database.

Furthermore, Maria does not actually have possession of $977241, only an IOU from her bank that she must trust is redeemable. She has no way to audit her bank to verify whether they actually have $977241.

In fact, they may not hold that much, since most banks legally operate on "fractional reserve" - meaning that their actual assets are allowed to be significantly less than the total balance promised to account owners.

Depending on how the funds were sent, it could take anywhere from minutes to days before the $2,500 shows up in George's bank account. Since George is not privy to the banks' ledgers or communications, the entire process is opaque and cannot be monitored.

Many people that have not personally experienced economic disruption take functioning banks and the validity of their IOUs for granted. Few individuals consider the unsettling ramifications of handing their lifelong savings to opaque corporations, often putting all their eggs in a single institutional basket. Losses can occur due to:

- negligence (the bank makes a mistake),
- financial issues (the bank overextends their assets or goes out of business),
- malice and corruption (the bank or a rogue employee steals your money)
- hostile third parties (the bank is robbed or a hacker thieves electronic funds)

Thankfully, an emerging new technology called blockchain is capable of mitigating literally all of the above risks by creating a decentralized database that all parties can equally use, view, and verify.

Introduction to Blockchains

Anybody can learn all about Monero and how the blockchain works without having to understand the underlying mathematics and cryptography (similar to how anybody can become internet-savvy without first studying DNS servers and the IPv6 protocol). This chapter focuses on the key concepts and vocabulary without digging into all of the technical details - you can jump ahead to chapter 6 [crosslink to the 6th chapter] if you want to dive into the cryptographic framework.

The term "blockchain" refers to a new method for securing records in a database that all network users share. It is groundbreaking for being a "trustless" system, where individuals retain full autonomy over their funds, there is no central authority, and each participant can easily verify and audit the system.

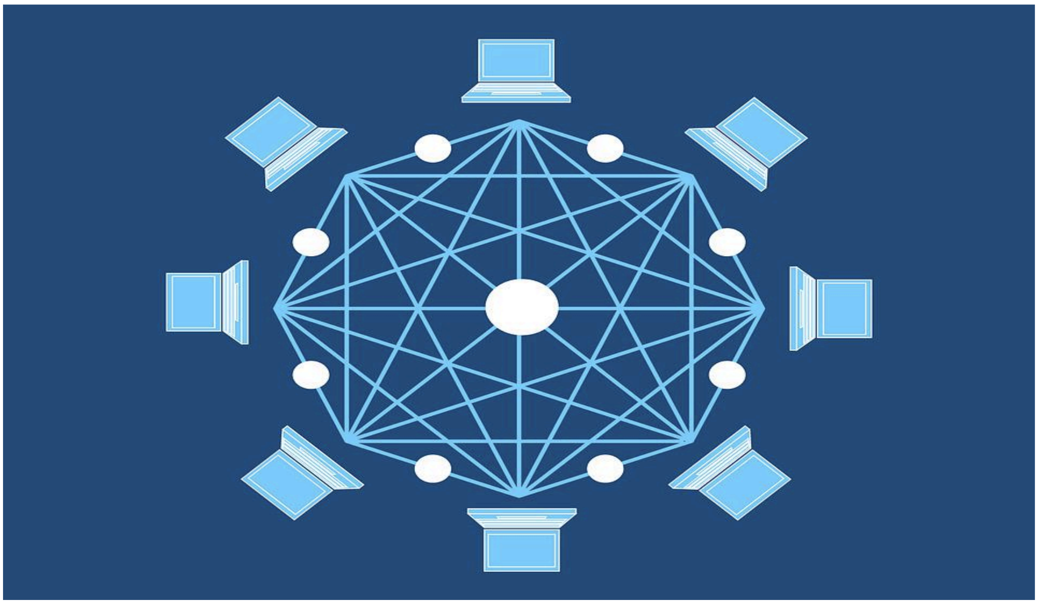


Figure X - Blockchain Network as Distributed Network based on Peer-to-peer

Anyone in the world is welcome to act as a network maintainer, and each participant keeps the others honest by verifying the blockchain. When users broadcast information to be placed on the blockchain, network maintainers group these transmissions into "blocks" and use cryptographic tools to finalize the records and permanently link them onto the blockchain.

Once data is sealed onto the blockchain, it cannot be deleted, moved, or altered in any way. The records are immutable and each participant on the network has matching copy of the blockchain for their own verification. The blockchain uses a clever "mining" model that encourages network participation and keeps all of the records honest and synchronized. These types of "decentralized" systems are incredibly robust since there is no single server or central database that can be maliciously attacked or manipulated.

In 2008, an anonymous individual or group known as Satoshi Nakamoto published a whitepaper describing "Bitcoin: A Peer-to-Peer Electronic Cash System". This worldchanging document laid out the framework for the open-source decentralized cryptocurrency and the revolutionary blockchain technology that makes it possible.

BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
TROYOZ 999 FINE COPPER MJB MONETARY METALS

Figure X.1 in the first section highlighted that sending money through the traditional banking system requires multiple, transactions, ledgers, and trust in multiple banks. Figure X.2 (below) shows how Maria could send money to George using an imaginary cryptocurrency (XYZ) that uses a typical transparent open ledger. Maria will to 10.5 XYZ from her account (1BuUygisXY) to an address controlled by George (PeK5FSykwp).

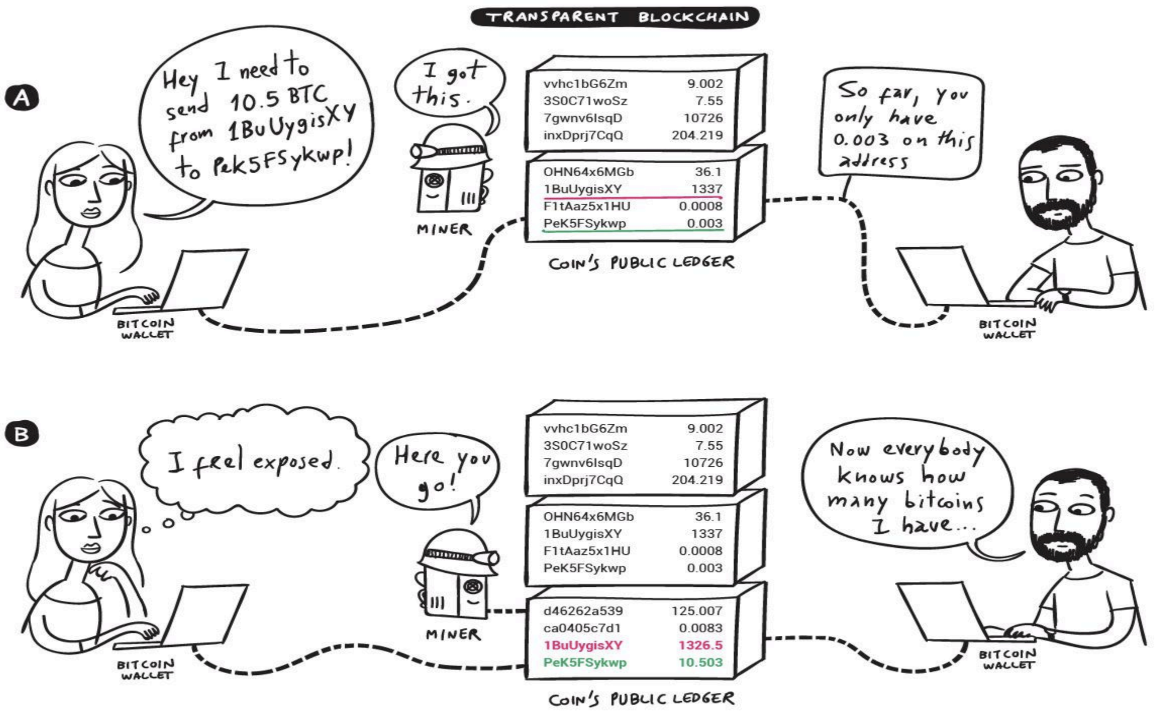


Figure X.2 - Marie sends some money to George by using a Trasparent Blockchain as Bitcoin

A few of the blockchain benefits are immediately apparent:

- Simplicity (& speed): Maria's money is sent to George in a single step to update a single ledger. Whereas bank and wire transfers can take days or weeks, cryptocurrency ledgers typically update in seconds or minutes (the transaction time varies for different cryptocurrencies).

- No third-party risks: Maria and George rely on their own cryptographically-secured and self-maintained system instead of placing their money and trust in the hands of a chain of third parties.

- Pseudo-anonymity: Unlike the banks, cryptocurrency ledgers never learn names like "Maria" and "George" with the accounts. In fact, personal information is never necessary for generating an cryptocurrency address. George will access the funds pseudonymously, using his key for the "PeK5FSykwp" address to which Maria broadcasted the money (from her account, "1BuUygisXY").

Bitcoin and the other cryptocurrencies that followed have launched a financial revolution that is still unfolding. With these new decentralized networks, anybody can personally store and globally transfer funds at their own discretion. Prior to cryptocurrencies, it was difficult to store large amounts of wealth securely without trusting your savings to banks or credit unions. Likewise, transferring money to another individual or business required reliance on third-party payment processors for checks, wire transfers, or credit/debit cards.

Thanks to cryptocurrencies, for the first time, anybody can exercise their basic financial rights without requiring access to a bank and approval from external institutions! In mere moments, any device (computer, phone, tablet) can be used to initialize a new cryptocurrency wallet that is fully functional for sending, storing, and receiving funds. Setting up a wallet does not require any kind of identification, fees, or authorization, and the system identifies users by addresses that look like random strings of numbers and letters instead of personally identifiable details such as street address or city.

Blockchain Drawbacks

Most cryptocurrencies are “pseudo-anonymous”, since their users are identified by unintelligible strings rather than personal identifiers. When you receive a cryptocurrency payment, you do not learn the sender’s name, instead you receive the funds from an address such as: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

While this preserves privacy in some ways, it also exposes some sensitive information. Recall, every participant in a decentralized blockchain possesses a complete copy of the entire record. In the context of cryptocurrencies, this ledger is used to ascertain the account balance for any (e.g. Bitcoin) address.

This transparent ledger means that every account balance is public! In fact, several helpful websites allow you to easily search the blockchain for any address or transaction.

Suppose you run a shop, and one of your customers pays for a loaf of bread from the Bitcoin address 3P3QsMVK89JBNqZQv5zMAKG8FK3kJM4rjt. You can instantly check the blockchain and see that this account has received more than 5,000 Bitcoins! Knowing that your customer handled $50,000,000 recently, you might be inclined to charge more in the future, or simply rob them now. This privacy issue presents a personal security risk.

In addition to knowing your customer’s balance, you can also see every transaction that they have received or sent: the amount, the timestamp, and both participants’ addresses. Analysis of transaction histories and patterns can be used to profile your spending patterns, wealth, income, and with whom you interact.

A great amount of your personal information is exposed if your blockchain history is linked to your identity (for example, during an online purchase or while registering for a cryptocurrency exchange). Often the owner of an account can be revealed with a little bit of research; for instance, you might have already searched for the two Bitcoin addresses listed above to learn that they belong to Satoshi Nakomoto and the Pineapple Fund charity, respectively.

Several companies exist solely to track and deanonymize transparent blockchains. For example, Elliptic offers an interactive explorer that shows the flow of funds between Satoshi, payment processors and exchanges, forums, marketplaces, gambling services, charities, known individuals, and other services. Figure Y shows a screenshot detailing significant Bitcoin transactions in the early 2010s, including connections between mining pools, Mt. Gox, and the Silk Road marketplace.

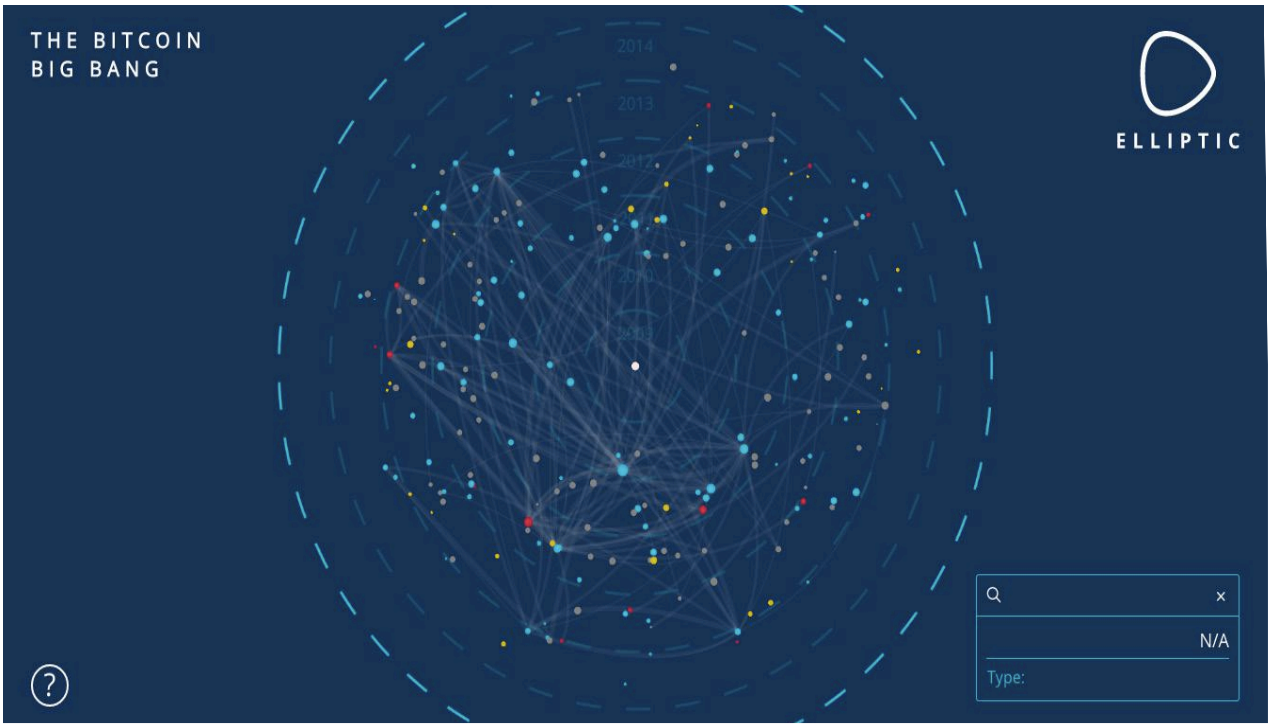


Figure XX.1 Elliptic's blockchain analysis of Bitcoin flow in the early 2010's, from the interactive [Bitcoin Big Bang explorer](#)

Take a moment to consider the valuable sensitive information that you generate each day: credit card transactions, every phrase that you search, products you view or purchase, social media sites that you interact with, etc… Almost all of it is recorded, profiled, and monetized by your banks, payment processors, giant tech/data industries, and governments.

This mass collection of your data results in centralization of your personal and private information in vast troves of sensitive material that are juicy targets for hackers and blackmarket resale. It is quite probable that your personal details (such as name, address, email, phone number, etc) are already in the public domain without your knowledge, perhaps connected with your demographic and/or marketing dossier.

Consider the recent Equifax, Target, Home Depot , Uber, and Panera data breaches. In many cases, both personal and financial information were compromised, putting individuals and their cards at risk.

Accidental data breaches are not the only concern. Big data and tech companies carefully record your activities online, in order to provide better services. Often, this refers to targeted marketing and ads; however, this data can also be leveraged for more questionable uses such as manipulating your feelings or your voting behavior.

Anything that a company tracks about you may be used maliciously or stolen/resold. You should exercise great caution regarding your digital footprint, since information cannot be “unleaked” after your personal details are exposed.

Right now, privacy is conspicuously absent from mainstream economic and commercial systems. Traditional payment processors, banks, and cryptocurrencies leave very clear trails that are used to study, surveil, and profit from you. Once collected, you often have no way to control or track the proliferation of your data, or the privacy and personal security risks that arise from its sale to unknown parties.

The only guaranteed way to exercise your right to financial privacy is to avoid revealing personal information in the first place! To stay safe, we need a way to interact securely - where transactions cannot be linked to your identity, your wealth, or other transactions. The Monero cryptocurrency is your best tool for taking all of these matters into your own hands!

Introducing Monero

Monero (pronounced /mōnĕrō/, plural “Moneroj”) is a leading cryptocurrency with a focus on private and censorship-resistant transactions. The openly verifiable nature of most cryptocurrencies (such as Bitcoin and Ethereum) allows anybody in the world to track your money. Furthermore, links between your financial records and personal identity may jeopardize your safety.

To avoid these dangers, Monero uses powerful cryptographic techniques to create a network that allows parties to interact without revealing the sender, recipient, or transaction amounts. Like other cryptocurrecies, Monero has a decentralized ledger that all participants can download and verify for themselves.

However, a series of mathematical tricks are used to conceal all of the sensitive details and styme any blockchain tracking. Monero users reap all the benefits of a decentralized trustless financial system, without risking the security and privacy downsides of a transparent blockchain.

One of Monero’s crucial defining features is enforced privacy by default. Users are specifically prevented from initializing transactions that are accidentally or intentionally insecure. This provides Monero users with peace of mind since the network will not accept a revealing transaction!

Figure X.3 (below) shows how Maria sends George funds for booking flights using Monero. The process is functionally the same as the cryptocurrency transaction shown in Figure X.2, however the sensitive information is cryptographically obscured. Information like account balances and transaction amounts are secretly encrypted, in contrast to the transparent public record that most cryptocurrencies are built on.

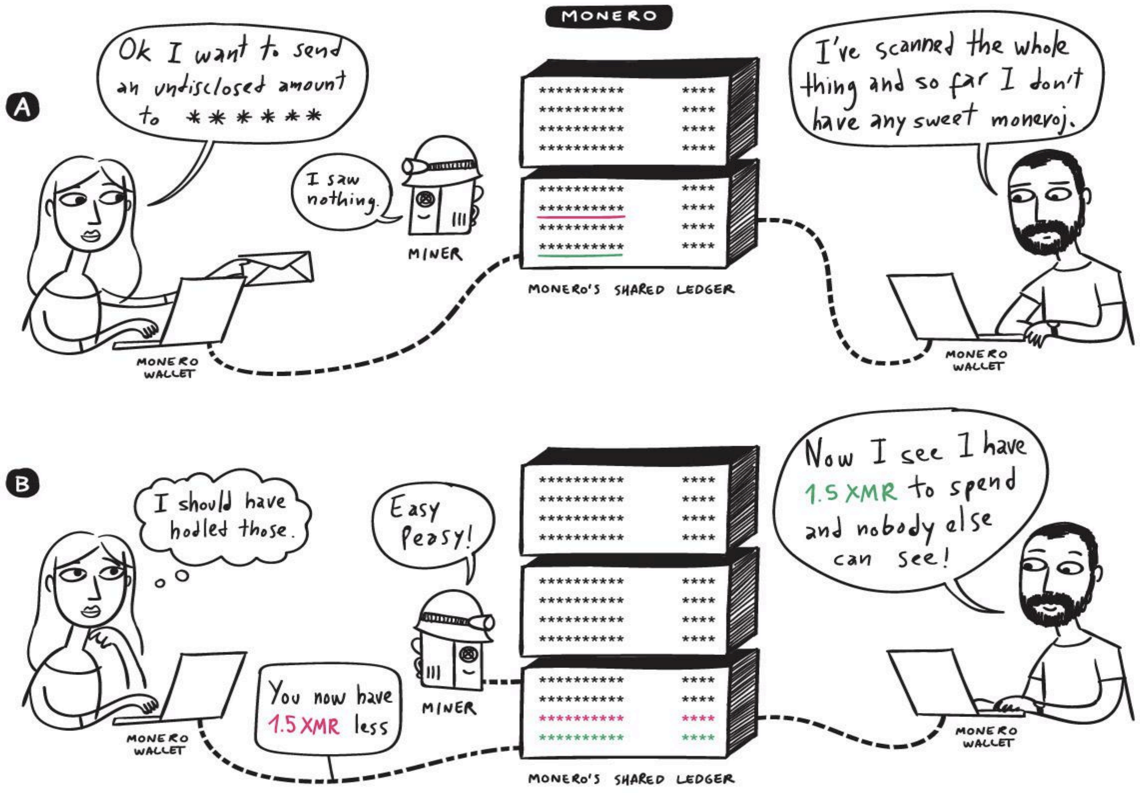

MONERO
A
Ok I want to send an undisclosed amount to ******
I saw nothing.
MINER
MONERO'S SHARED LEDGER
I've scanned the whole thing and so far I don't have any sweet moneroj.
MONERO WALLET
MONERO WALLET
B
I should have hodled those.
Easy Peasy!
MINER
Now I see I have 1.5 XMR to spend and nobody else can see!
You now have 1.5 XMR less
MONERO WALLET
MONERO'S SHARED LEDGER
MONERO WALLET

Figure X.4 - Maria sends XXX money to George by using the Monero cryptocurrency.

Monero's privacy features allow the network to assess the validity of a transaction and determine whether or not the sender has a sufficient account balance, without the actually knowing the transaction amount or account balances! Nobody can view others' account balances, and transactions don't reveal the source of the funds being transferred.

These are marked with "***" in the diagram, since an no outside observer can ascertain the values. The mechanics behind these unique privacy features are discussed in chapter X.

Principles of Monero

Monero is designed with the following principles in mind:

- Network Decentralization: The Monero network and ledger are globally distributed. This means that there is no single server or database that can be maliciously controlled or censored. If one government were to shut down Monero nodes in their country, or attempt to limit who can send/receive Monero, the effort would be in vain! The rest of the world will carry on the network and process any valid transactions.

- Financial Security: The globally-distributed Monero has no central weak point that can be hacked to steal your funds. Your Moneroj are secured by immutable cryptographic techniques, so there is no need to trust a third party with responsibility over your funds. Every single Monero participant can verify the validity of the ledger themselves, so you do not even have to trust the node operators! (You can learn more about the cryptographic techniques that secure Monero in chapter X)

- Financial Privacy: Most blockchain projects increase security at the expensive of privacy, however Monero prioritizes your privacy. Transaction amounts, sender identity, and recipient identity are all obfuscated on the blockchain, so your Moneroj storage and spending activities are not trackable.

- Fungibility: The term "fungibility" means that some type of asset is considered interchangeable. For example, imagine that you let your neighbor borrow 1 kilogram of flour for a cake. When they return flour the next week, of course it will be 1 kilogram of flour from a different source (since they used your original flour for baking). This is not a problem, since flour is fungible. However, vehicles are not fungible; if you let your neighbor borrow your car, you probably want the same one back!

In the case of Monero, its fungibility is a feature of its sophisticated privacy practices, and refers to how the obfuscated transaction record means that it is impossible to ascertain the history of any particular Moneroj· If you let your friend borrow 1 Monero, they can return any 1 Monero, since they're indistinguishable. This particular quality may seem like a minor nuance, however fungibility crucially necessary for something to be practically used as a currency (see examples below). This characteristic is absent from most cryptocurrencies, with transparent ledgers and trackable histories.

Real-life “use-case” for Monero

This section talks about some of the difficulties and risks that arise from using insecure cryptocurrencies. For simplicity, the examples refer to “Bitcoin” as the prototypical transparent-blockchain currency. However, these drawbacks are present in essentially all cryptocurrencies; not Bitcoin in particular.

- Price manipulation: Sofia is the only mechanic in a small town. One of her customers paid for an oil change with Bitcoin. Sofia later looked up his address on the ledger and saw that the customer’s wallet contained enough Bitcoin for a new Lamborghini. Next time he needed a repair, she doubled her prices. If the customer had used Monero, Sofia would have been unable view his balance or use such information to manipulate prices.

- Financial surveillance: Oleg’s parents send him some Bitcoin to pay for textbooks, and then continue to snoop on his Bitcoin address and activity. A few months later, Oleg sends some leftover Bitcoin to the public donation address for an organization that does not align with his parents’ political views. He does not realize that they are still monitoring his Bitcoin activity until he receives a furious email from his parents, berating him. If Oleg had used Monero, his family would not have been upset from prying into his transaction activity.

- Supply chain privacy: Kyung-seok owns a small business providing family catering services for local events. A large food company uses blockchain tracing to identify most of his regular clients. The corporation uses this list to contact Kyung-seok’s customers, offering similar deals for 5% less. If Kyung-seok’s business used Monero instead, its transaction history could not have been exploited by rival businesses seeking to steal his customers.

- Discrimination: Ramona finds her dream apartment, conveniently close to her new job in a great neighborhood. She pays her rent on time every month, but the landlord notices that she often receives Bitcoin from a legal online casino. The landlord personally despises gambling, and unexpectedly chooses to not renew Ramona’s lease. If rent was paid in Monero, the landlord would not be able to review and discriminate based on Ramona’s sources of income.

- Transaction security/privacy: Sven sells a guitar to a stranger, and gives the buyer a Bitcoin address from his long-term savings wallet. The buyer checks the blockchain, sees the large sum of money that Sven has saved up, and consequently robs him at gunpoint. If Sven had instead given a Monero address for payment, the buyer would not have been able to view Sven's wealth. Censorship: Makalah purchases some Bitcoin from an online exchange that verified her identity, then transfers a portion to a charity supporting human rights in her country. Two years later, her government analyzes the blockchain and notes the transaction from a known exchange to a blacklisted activist group. The government subpoena the exchange for Makalah's identity and arrests her the next day. If Makalah used Monero for the donation, her government would never have known the source or destination of that contribution.

- Tainted coins: Loki sells some of his artwork online to save up for college. When he pays tuition, he is shocked to receive a "payment INVALID" email from the school. Unbeknownst to Loki, one of his paintings was purchased using some Bitcoin that were stolen during an exchange hack the previous year. Since the school rejects any payment from a blacklist of "tainted" Bitcoins, they refuse to mark the bill "paid." Loki is in an extremely difficult position: the Bitcoin that he saved has already been spent from his account, yet the tuition bill is still unpaid. This entire situation would have been avoided if Loki sold his paintings for Monero instead, since its fungibility precludes tracking or blacklists.

Monero: open-source decentralized community and software

Monero is an open-source project actively developed by cryptography and distributed systems experts from all over the world. Many of these developers freely donate their time to The Monero Project, while others are funded by the Monero community so that they can focus entirely on the project.

The decentralized nature of Monero's development team brings several benefits over a consolidated corporation or organization. The Monero Project is a living entity, greater than any individual or group. Since both the network and development team are spread across the globe, it cannot be shut down by any single country, or controlled within any particular legal jurisdiction.

The term “open-source” means that the source code (software blueprints) are made publicly available for anybody to inspect. The alternative is “closed-source” software, where developers only deliver the final compiled product (“binaries” like .exe files) that cannot be opened and studied. If you use closed-source software, you are trusting the developer and distributor. The problem is that even a developer with the best intentions may make a mistake that hackers later discover and exploit. Only use open-source cryptocurrency software that has been audited by independent parties to verify the absence of that malicious code, accidental mistakes, and implementation weaknesses.

The cryptocurrency community has embraced open-source software from the very start: Bitcoin was released as a public white paper and open-source community-built code, which stood in stark contrast to the opaque and proprietary decision structure endemic to fiat (government-backed) currencies. Of course, the open-source philosophy has been around much longer than cryptocurrencies! Over 25 years, more than 5,000 coders have contributed to the open-source Linux kernel, which is widely considered to be one of the most secure operating systems.

The trust and security benefits of open-source software are of key importance for any cryptocurrency, so The Monero Project is entirely open-source. The developers uses Git [link: https://github.com/monero-project/monero] for version control, which allows anybody to easily review every single line of code proposed to be added, removed, or modified. Over 240 developers have contributed to, reviewed, and tested the Monero code, which drastically lowers the likelihood that any errors have been overlooked. Developers can find more information about interacting with Monero’s codebase in chapter X.

Development team transparency is very important for community trust, especially in the context of cryptocurrencies. In addition to posting code for public scrutiny, The Monero Project also conducts all development team meetings on open IRC channels, [link: https://getmonero.org/community/hangouts/] and all of the logs are archived on the public Monero website.

History of Monero

In 2013 Nicolas van Saberhagen published the “CryptoNote” protocol, which became the foundation for many coins, starting with Bytecoin. Like the unknown Satoshi Nakamoto, the creator of Bytecoin remained anonymous and promoted their coin through a Bitcointalk thread.

Some aspects of Bytecoin appeared dubious under close scrutiny. Bitcointalk member "thankful_for_today" investigated the emissions curve and noted that approximately 82% of the coins had already been emitted, so the circulating coin supply was potentially dangerously centralized.

Ultimately, this greedy premine undermined Bytecoin's credibility and practicality. Thankfully, thankful_for_today recognized the value in CryptoNote's features, and incorporated them into a new project centered around a strong, community-driven development team. The Monero cryptocurrency, spearheaded by thankful_for_today, launched in April 2014. The coin was originally named "BitMonero," however the community quickly elected to shorten it to "Monero."

Ethical Discussion

Monero was carefully engineered to provide characteristics like fungibility and transaction privacy that are necessary for any currency (crypto- or otherwise) to be feasible for general use. As discussed in the section on use cases [internal link], there are significant practical issues that arise with financial systems that do not protect users' privacy.

The very features necessary to keep Monero safe for day-to-day users and businesses are unfortunately also appealing to those wishing to conceal illicit activity. Because of Monero's privacy features and ease of mining, it has been utilized by criminals, ransomware, and covert mining (employing "botnets" of many victims' hijacked devices).

Monero is not intended to facilitate illegal activity, which has plagued every currency since the idea of money was conceived thousands of years ago. The scale of illegal transactions conducted using cryptocurrencies is dwarfed by the staggeringly-vast amount of criminal activity that occurs every day denominated in fiat currencies like Euros, Rupees, Yen, or Dollars.

The creators of "Mastering Monero" and the entire Monero Community do not condone illegal activities, and we do not wish to assist criminals. If you wish to use Monero for exploitation or dark purposes, please close this book now, and do not use our project for harmful ends.

Chapter 2

Getting Started

The last chapter focused on WHY to use Monero; in this chapter you will learn HOW to use Monero. You can master using Monero without needing to learn any of the complex cryptographic or network technical details, so that extra information is saved for later in the book. Chapter 2 will cover all the practical skills you'll need to get started receiving, storing, and spending your Moneroj.

The first part of this chapter covers key concepts and terminology for Monero use, as general information that will apply to any wallet or software. Toward the end of the chapter, you'll find handy guides for carrying out these steps using the free official open-source Monero command line interface (CLI) or graphical user interface (GUI) software.

What is a wallet?

Before you obtain some Moneroj, you must plan ahead for where you will receive and store your funds. You will need a "wallet" to help you store and spend your Moneroj. Just like physical wallets for your bills, there are lots of different types of Monero wallets, and you can always move some of your money from an old wallet to a new one.

Wallets take care of the complicated cryptographic processes for you, so you don't need to know any fancy mathematics to use Monero. You will only need to manage a seed and your address(es). Other details like "public keys" and "private keys" are managed behind-the-scenes by your wallet, so they are not discussed until chapter VI.

Your Monero seed is a secret number that your wallet uses to locate and spend your Moneroj, though it is converted into a series of 12-25+ words for convenience. This secret is like a treasure map to your money on the blockchain, and anybody who learns your seed can use their wallet to access and spend your Moneroj. For this reason, you must be extremely careful when you generate and store your seed. Do not set up a wallet in a coffee shop, where other patrons or cameras may see your secret. It is dangerous to store your seed electronically (e.g. in a text file or email) since malicious software or services may run off with your Moneroj.

Your seed is used to generate your address(es), which you can share with others. Most wallets will show your address in two different formats - a written string of numbers/letters, and a visual QR code. These are redundant, and you can safely share either form.

If your wallet is physically damaged, you can simply import your seed into a new wallet, and pick up right where you left off! As long as you have a copy of your seed, you can always access your funds. However, if you lose your seed, there is no way to ever recover access to your Moneroj. You may be familiar with passwords, which can usually be reset by contacting an administrator. Seeds are not like passwords - nobody else knows your secret, and the network is unable to shift your Moneroj to a account if you lose the old one.

Most software will prompt you to write down the seed when you initialize a new wallet, however some apps do this in the background, and you must take the initiative to backup your wallet. Be sure to do this immediately, or else a damaged device will cause you to permanently lose your funds.

Selecting the best wallets for your needs

There are various storage solutions, and they vary in terms of convenience, privacy, and security. Your individual needs will determine which type(s) of wallets are best for you. Many people use multiple storage solutions: often a convenient "hot wallet" that holds small amounts for day-to-day use, complemented by a more secure "cold wallet" for long-term savings or large amounts. The varying wallet types described below differ primarily in where the secrets are stored.

Software and Mobile Wallets

Software wallets (on a desktop PC or mobile device) are convenient for storing and using Monero. Many Monero users have a handy "hot wallet" on their phones, to pay for small purchases. A good rule of thumb is to only walk around carrying as much cryptocurrency money as you would feel comfortable holding in regular cash. The secrets are stored on your device, so your Moneroj could be stolen if you catch a virus or keylogger.

Hardware Wallets

Hardware wallets are special physical devices that generate your seed, store the secrets based on your seed and carry out transactions, while never revealing your secret information to the connected device. While hardware wallets are less convenient than software wallets, they are extremely secure! Because of how they store your seed, you can safely use a hardware wallet to send transactions from a device that you suspect or know is compromised with malicious software. The Monero community is releasing the first-ever open-source cryptocurrency hardware wallet, called .

Paper Wallets

Paper wallets provide an inexpensive way to stash Moneroj that you do not plan to move frequently; you simply print out a physical copy of your public and secret information for safe storage. Since the secrets from your Monero seed are saved only on paper, not digitally, you do not have to worry about viruses or data leaks. However, paper wallets are not convenient for frequent use, since you must transfer the secrets to a digital device every time you wish to send Moneroj.

Web Wallets

Web wallets refer to platforms running on third-party services that you control through their website. Web are extremely convenient, at the expense of security and privacy. The wallet is only as trusted as the third party, and there are extra security risks associated with accessing your Moneroj through a web browser. Some of the more secure web wallets are designed to keep the seed and secrets on your device as MyMonero. If a web wallet provider is going to hold your seed on their computers (and let you log in to access your funds) then you should be very suspicious.

Cold Wallets

Cold wallets refer to any device that is generally kept offline and used only for storing your secrets. They could use any operating system, and you must be very deliberate with strong security (including a firewall, antivirus, and extreme caution regarding accessing only trusted websites/software). The seed is still on the computer, however you keep the device sequestered from the rest of the world, as much as possible.

Monero Wallet Links

Regardless of which type(s) of wallet you choose, be careful to only download vetted software from through proper channels. Phishing schemes and scam wallets are numerous, so be sure to double-check that you are installing legitimate software! If you enter your seed into a malicious wallet, your Moneroj will be gone before realize your mistake.

This section contains links to several open-source wallets that are developed and trusted by the Monero community.

- Mac/Windows/Linux: An official Monero wallet is available with command line interface (CLI) and graphical user interface (GUI) versions. https://getmonero.org/downloads
- Android: Monerujo
- iOS : CakeWallet and XWallet
- Web Wallet : Mymonero.com doesn't reveal your seed's secrets to the server

Using Monero

This section explains what you need to know for sending and receiving Monero. All of the examples in this book use the following seed:

```
MASTERING MONERO DEMO SEED: lamb hexagon aces acquire twang
bluntly argue when unafraid awning academy nail threaten sailor
palace selfish cadets click sickness juggled border thumbs remedy
ridges border
```

You can import this seed in yourself to practice generating addresses, checking transaction history, and verifying payments. You can use this seed to follow along with examples in the book, but do not send your Monero to it! Anybody else reading Mastering Monero will be able to spend it!

Receiving Monero

To receive Monero, all you have to do is find your address through your wallet and share it with the person sending you Moneroj. Most wallets will show your address in two formats: an alphanumeric string that is easy to cut+paste, and a QR code that is handy for scanning with a camera. Here are examples of both formats, from the DEMO seed above:

This address that you share is not stored on the blockchain (thanks to a Monero feature known as "stealth addresses" that are discussed in Chapter III and Chapter VI). Monero also allows you to generate multiple "subaddresses" from your single secret seed, so you can share many different addresses that all deposit to the same wallet.

Wallets may wait 10 - 20 minutes for "confirmation" before marking funds as received and safe to spend (you can learn why in Chapter IV). This is a common security practice, and wallets usually show the "unconfirmed" transaction during the waiting period. If your wallet is waiting for a 0.06 XMR payment to confirm, you may see something like this:
Balance: 0.075 XMR Available balance: 0.015 XMR
There is no need for concern when this occurs! Within less than a half hour, the funds will confirm and transfer to your available balance.

Sending Monero

To send Monero, you only need to input the recipient's address and the amount that you wish to transfer. If you are sending Moneroj to a business, they may also ask you to include a "payment ID" to connect your payment to your order. If you are sending Moneroj to yourself or a friend, you can leave the payment ID field blank.

Your wallet will add small network fees to pay for sending your transaction. The fee associated with a given transaction varies depending on current network load and the location of your funds. Wallets will usually suggest an appropriate fee to send your transaction in a reasonable time.

Proof of Payment

Given Monero's anonymity, you might wonder how somebody can prove that a payment was sent. Besides optional payment IDs, Monero has a second feature to selectively reveal proof that you sent funds. A legitimate "transaction key" can only be generated by the true sender.

Example

Suppose your friends Khan and Maria each owe you 0.06552376 XMR for a meal that you split. You only receive 1 payment, with the information below:

Amount: 0.06552376 XMR
Transaction ID: 4b540773ddf9e819f0df47708f3d3c9f7f62933150b90edc89103d36d42ca4b7
Received to (your) sub-address: 899Ao1NQtu4ezACgw1QKXK4QBf5s8a3WHHtAjFfPm3Nf71mAkREEgAuKzASXHt8E7vVJFKsQJuvApBfu21WY9WN97Put8M5

This is a real transaction received by the DEMO wallet on 20-Apr 2018. You can see some information through a blockchain explorer, however the Monero sender is always unknown. Both Khan and Maria claim that they sent the payment, so you ask each to provide the transaction key.

Khan: OutProofV1N4Y5pUJEnRACJyB5C3zK1zTqAihdnN8MfVZhEWfD13Z2N7Npt1uxa1EY7N7jnvuJF76tXUwKrakvZSxTj4Zux5SpavFb4X1jRcLAJ2b5hqviQPiS58j2qH53QL44CJEgHtY5

Maria: OutProofV1To53Qu2gegZbUevosKCTwrEdqiECgFyUygutXMEdhrHg1EtXMrFNaszWYFjdU4aXFZ2iPF8G8jzoDJzCoW5dsWvb4mVN65abAya3U47cGXs7WABrTzG5aPfV4YBANhwPgwD2

When you check both of their transaction keys, Maria's confirms payment to your address and Khan's key returns "bad signature." You can practice this yourself using the above address and transaction keys!

Connecting to a remote node (optional)

You can reduce sync time and disk usage by connecting to a "remote node" instead of storing the entire blockchain on your device. Most mobile wallets are automatically configured to connect to a remote node. If you need to manually direct your software to a remote node, you can use the community resources at `node.moneroworld.com` port `18089`.

Nodes are computers that have downloaded the entire blockchain, and assist other users by syncing their wallets and relaying their transactions. Running your own (local) node is best for privacy, and you can choose to share your node publically if you wish to help secure the network. Remote nodes are convenient, and allow a user to quickly begin using Monero without downloading the entire blockchain.

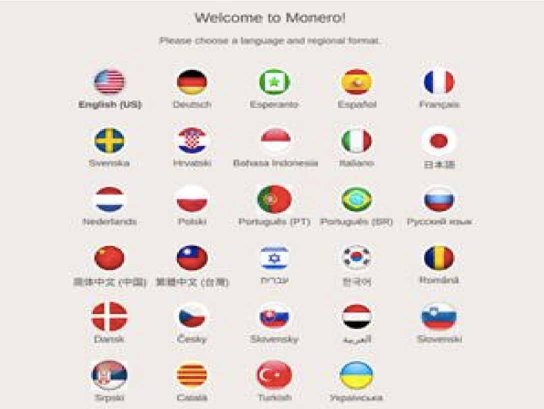
Running a node is not the same as "mining" Monero. Mining is a different resource-intensive process, not discussed until Chapter IV. Running a local node is a network/ CPU-light process after the blockchain has synced once.

Specific instruction for Monero Official GUI

The following instructions show how to carry out the tasks described above through the Monero graphical user interface (GUI). If you are using a different wallet, you can skip this section.

1. Choose a language

The official Monero GUI can be downloaded through www.getmonero.org. Once you have unpackaged and loaded the application, you will be presented with a language selection screen:

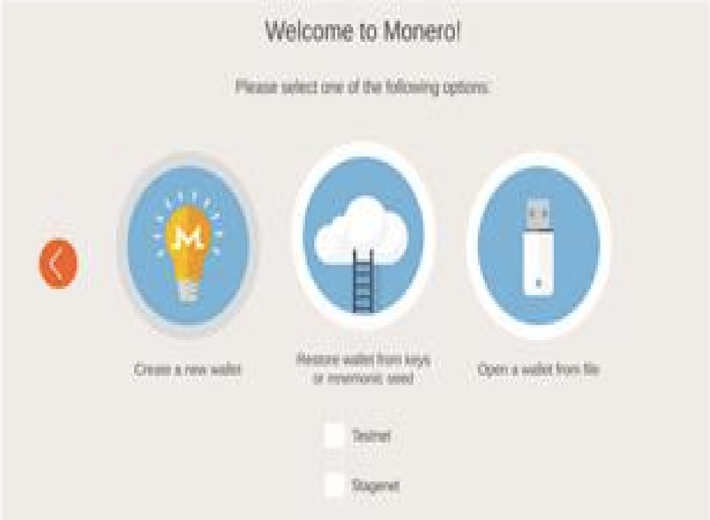

Welcome to Monero!

Please choose a language and regional format.

If you don't see your language above, please feel free to submit a translation to help others!

2. Specific an option

The Testnet and Stagenet are for developers, so do not check either option. If this is your first Monero wallet, press "create new wallet." The Monero software will generate a new seed for you, and show you the 25-word seed mnemonic.


Welcome to Monero!

Please select one of the following options.

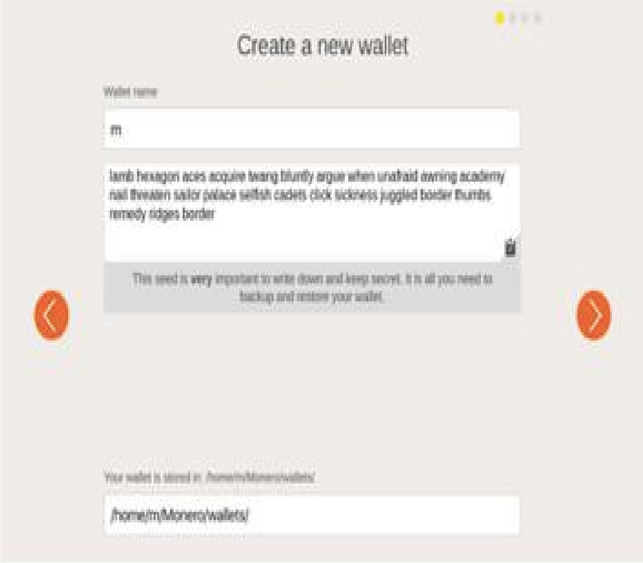
□ Testnet

□ Stagenet

3. Write down the seed

Remember the seed is not like a password!

Be sure to write this down and store it in asafe place where nobody else will find it!



Create a new wallet

Wallet name

m

lamb hexagon aces acquire twang bluntly argue when unafraid owning academy nail threaten sailor palace selfish cadets click sickness juggled border thumbs remedy ridges border

This seed is very important to write down and keep secret. It is all you need to backup and restore your wallet.

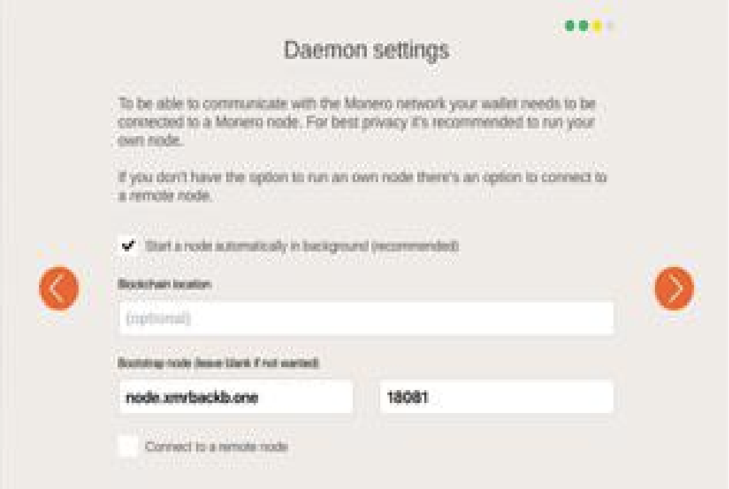
Your wallet is stored in: /home/m/Monero/wallets/

/home/m/Monero/wallets/

4. Download the Monero Blockchain

Next, you will have the option to start your own node, or connect to a remote node.

If you have an old personal computer, we would like to suggest you to connect to a remote node by following the “*Connecting to a remote node*” section.



Daemon settings

To be able to communicate with the Monero network your wallet needs to be connected to a Monero node. For best privacy it's recommended to run your own node.

If you don't have the option to run an own node there's an option to connect to a remote node.

☑ Start a node automatically in background (recommended)

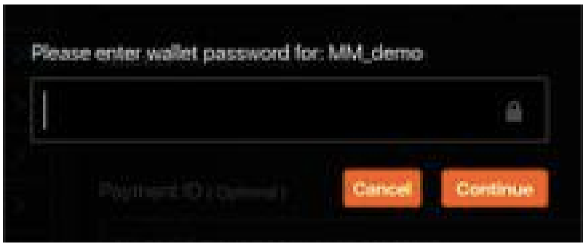
Blockchain location

(optional)

Bootstrap node (leave blank if not wanted)

node.xmrbackb.one 18081

☐ Connect to a remote node



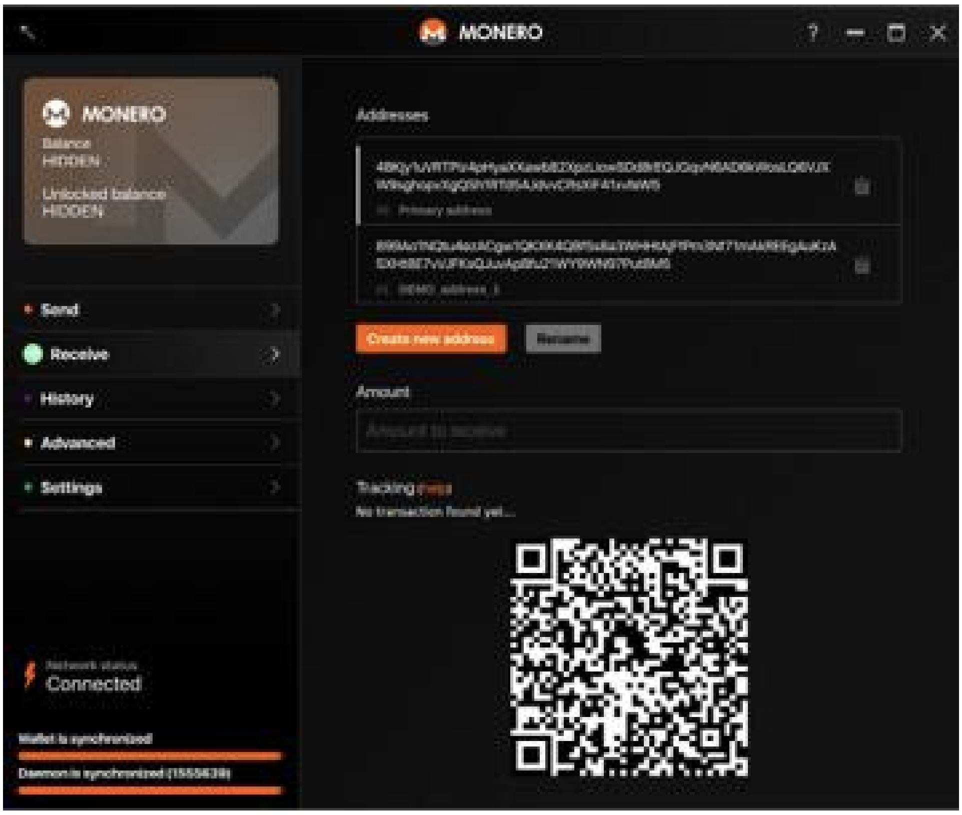
Please enter wallet password for: MM_demo

5. Digit a password

You can enter a wallet password, to keep your fund secure if somebody else accesses your computer. The wallet password is a local security feature, like a PIN screen unlock. It does not impact the cryptography or how your Moneroj are stored on the blockchain, so restoring your wallet from the seed will bypass the local passphrase.

Receiving Monero with GUI

The “Receive” tab of the Monero GUI contains both the text and QR-code forms of your receiving addresses. The “Create new address” button generates as more “subaddresses,” which will all direct to this same wallet (seed). You can indicate an “Amount to receive,” which will be encoded into the QR code.



Balance
HIDDEN

Unlocked balance
HIDDEN

Addresses

[illegible]
Primary address

[illegible]
DEMO: address_1

Amount
Amount to receive

Tracking (help)
No transaction found yet...

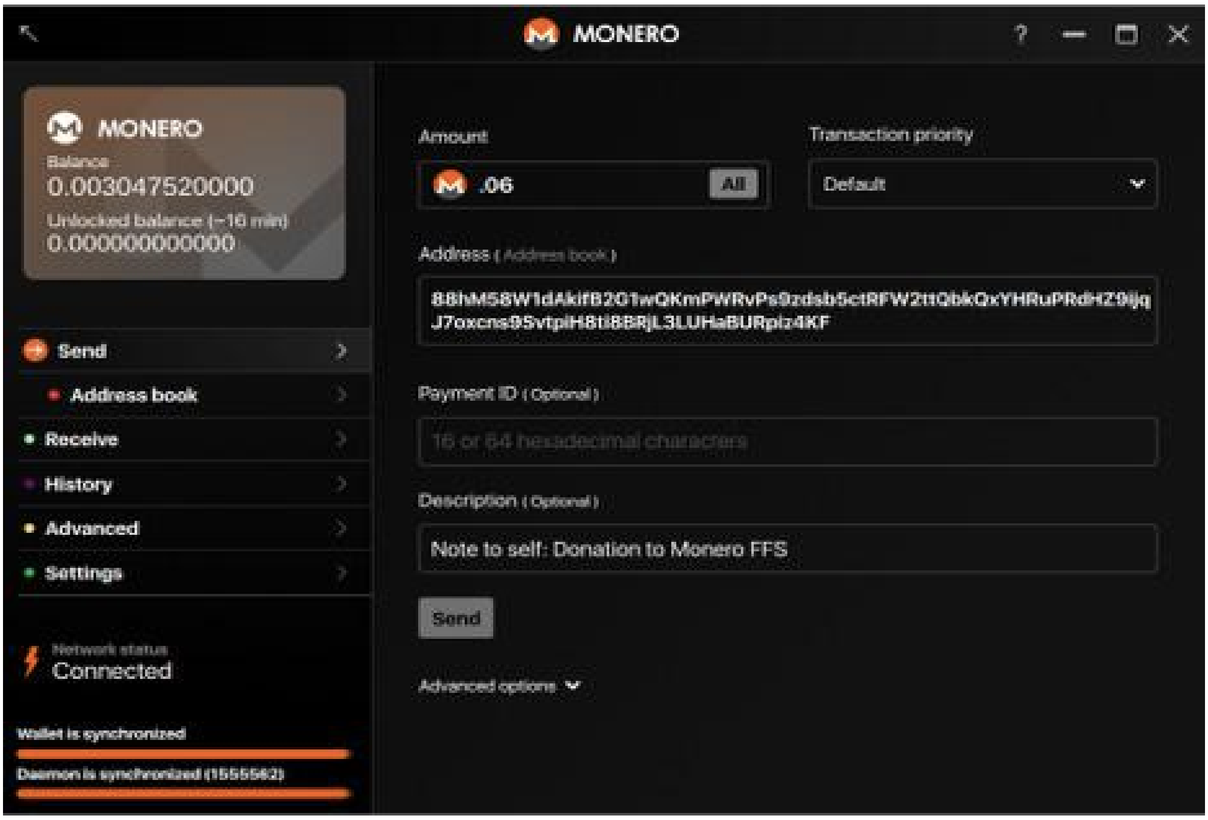
Network status
Connected

Wallet is synchronized

Daemon is synchronized (1555639)

Sending Monero with GUI

To send Monero, you simply specify the amount that you wish to send and the recipient’s address. The Payment ID field can be left blank, unless your recipient specifies a Payment ID in advance. The Description field is stored locally, so you can leave notes for yourself.



MONERO

Balance
0.003047520000

Unlocked balance (~10 min)
0.000000000000

Amount
.06

Transaction priority
Default

Address (Address book)
88hM58W1dAkifB2G1wQKmPWRvPs9zdsb5ctRFW2ttQbkQxYHRuPRdHZ9ijq J7oxcns95vtpiH8ti8BRjL3LUHaBURpiz4KF

Payment ID (Optional)
16 or 64 hexadecimal characters

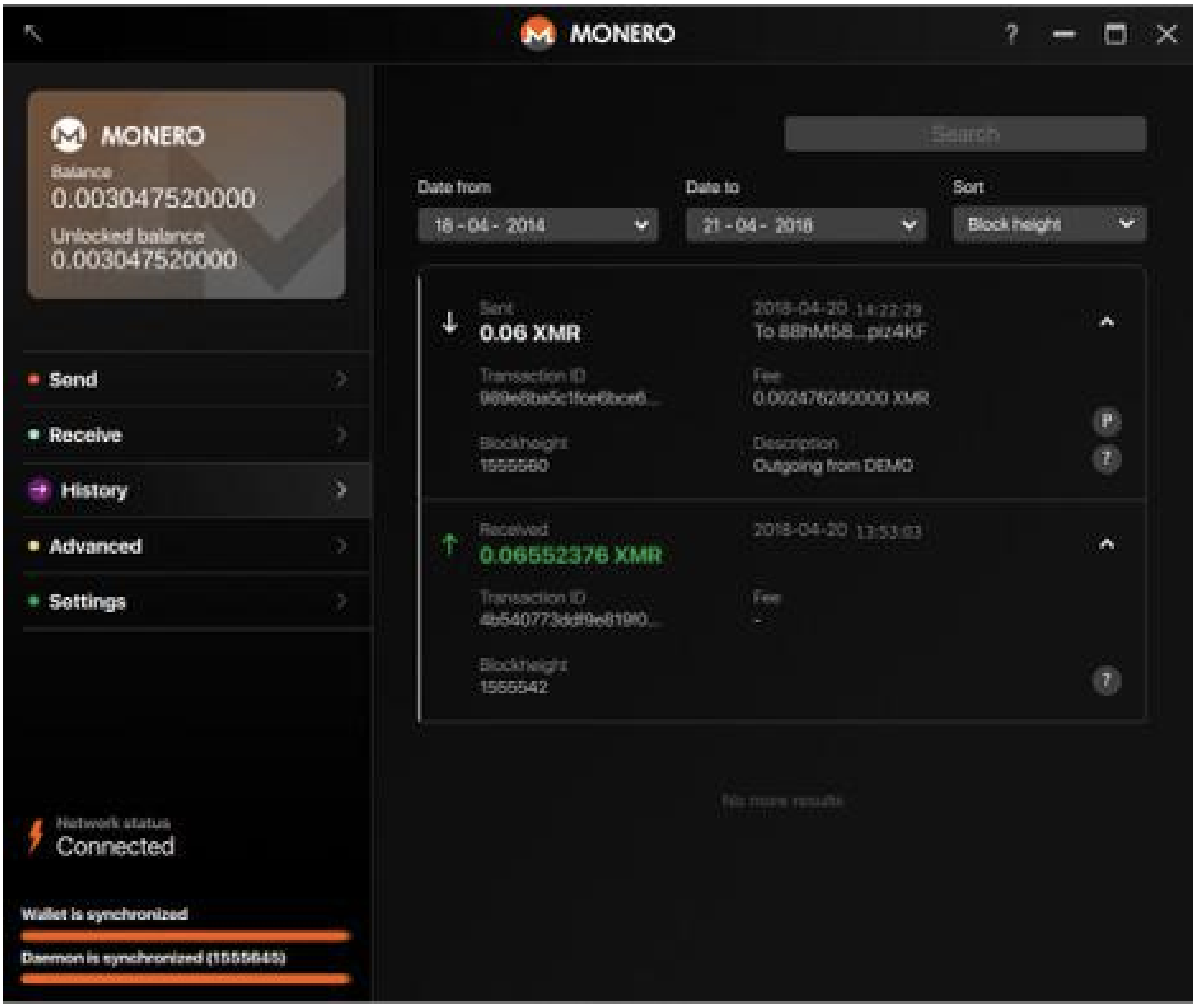
Description (Optional)
Note to self: Donation to Monero FFS

Network status
Connected

Wallet is synchronized

Daemon is synchronized (1555562)

Transaction History



MONERO

Balance
0.003047520000

Unlocked balance
0.003047520000

Date from
18 - 04 - 2018

Date to
21 - 04 - 2018

Sort
Block height

Sent
0.06 XMR
2018-04-20 14:22:29
To 88hM58...piz4KF

Transaction ID
989e8ba5c1fce6bce6...

Fee
0.002476240000 XMR

Blockheight
1555560

Description
Outgoing from DEMO

Received
0.06552376 XMR
2018-04-20 13:53:03

Transaction ID
4b540773ddf9e81910...

Fee
-

Blockheight
1555542

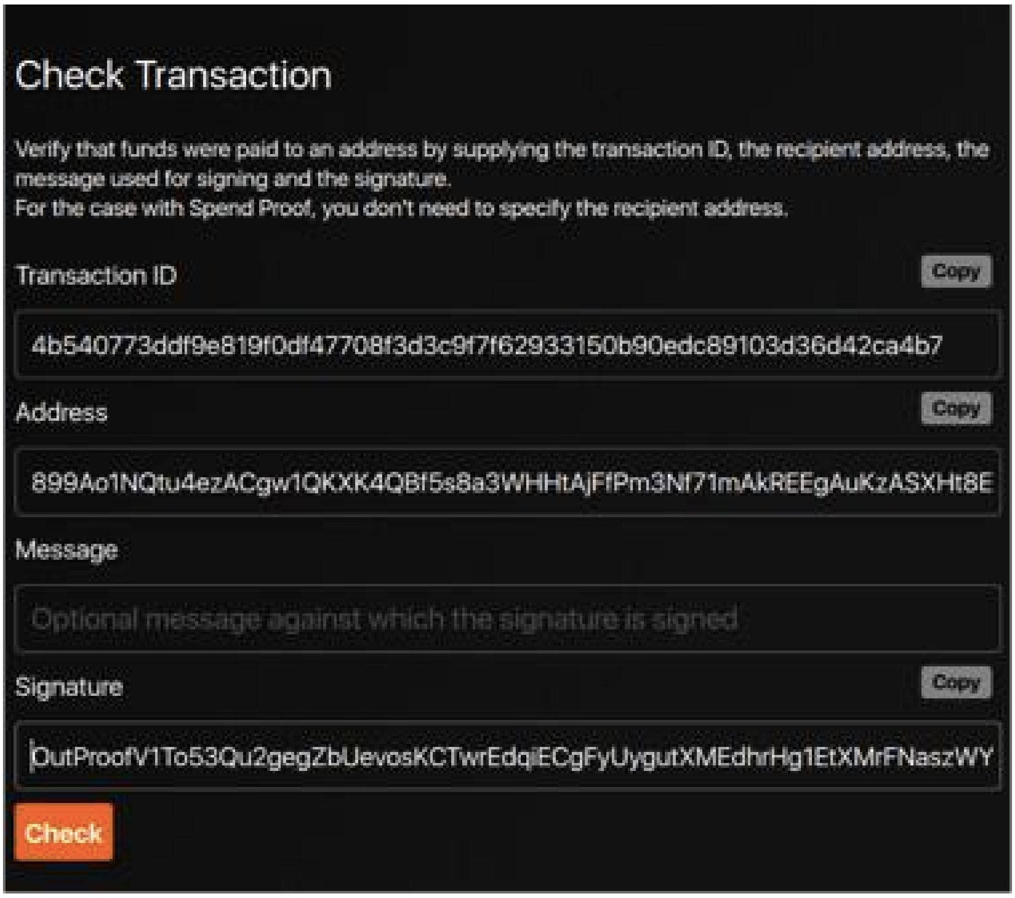
No more results

Network status
Connected

Wallet is synchronized

Daemon is synchronized (1555645)

Proof of Payment with GUI



Check Transaction

Verify that funds were paid to an address by supplying the transaction ID, the recipient address, the message used for signing and the signature.
For the case with Spend Proof, you don't need to specify the recipient address.

Transaction ID: 4b540773ddf9e819f0df47708f3d3c9f7f62933150b90edc89103d36d42ca4b7

Address: 899Ao1NQtu4ezACgw1QKXK4QBf5s8a3WHHtAjFfPm3Nf71mAkREEgAuKzASXHt8E

Message: Optional message against which the signature is signed

Signature: OutProofV1To53Qu2gegZbUevosKCTwrEdqiECgFyUygutXMEdhrHg1EtXMrFNaszWY

Proof of payment verification is available through the GUI under "prove/check." The below screenshot shows the transaction ID, address, and transaction key from the Maria & Kahn example above.

Chapter 3

How Monero works

General Presentation of Monero Technologies

The technology that first enabled the development of cryptocurrencies was the blockchain. A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. A hash pointer, predictably, consist of a pointer and a cryptographic hash. A pointer is a piece of data that “points” to some other data. A cryptographic hash is a digital signature of some data that can be reproduced independently to verify the data’s integrity. Hash pointers thus let us retrieve and then validate the previous blocks in the blockchain.

Blockchains are “open, distributed ledgers that can record transactions between two parties efficiently and in a verifiable and permanent way”. For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Transaction

Each transaction within the Monero network involves the use of inputs and outputs, where inputs consume Monero from the sender and outputs transfer them to the recipient.

The transaction is digitally signed by the sender, who authorizes the transfer of Monero. The transaction is then broadcasted to the network and grouped with several other transactions in the form of a block, It is not enough, however, for a cryptographic system to use strong cryptography in order to be secure. Someone must validate the signatures on the block to make sure someone is not forging them or else there is no point in signing payments in the first place.

This job is done by the miners. Cryptocurrency mining is thus not just an arbitrary method for a network to give out coins - miners play a critical role in making coin payments are not fraudulent. As a reward for gifting the network CPU power and speeding up the processing time for transactions, input users each pay a fee to the miners, and in this way incentivize participation in the mining process to further secure the network.

Once the block is accepted, the transactions get recorded on the blockchain (which, as you may recall, is a public ledger) in chronological order. Whenever this process is successfully completed, the network distributes new Monero to miners for each block that has been solved/validated. This is referred to as a block reward.

There is a catch to this process though, and that the validation pipeline can be hijacked by someone with an extremely large amount of processing power. If you control at least 51% of the CPU cycles in an entire mining network, you will be capable of reversing transactions you send while you maintain control. These attackers would be double-spend their monero and thus make transactions withthey didn't have. A majority attack has never been observed in practice on a large cryptocurrency; however, it has been demonstrated on some smaller altcoins as a proof of concept.

This is why people refer to mining as "securing the network": the more people that mine monero, not only does the speed of transactions and fees for miners go down, but the cryptocurrency also gets more resistant to a possible attack of this nature.

How does Monero work?

As we mentioned in Chapter 1, Monero is based on the CryptoNote protocol and the gifts of modern cryptography to protect the privacy of the sender, recipient, and obfuscate the amount transacted.

Below, you will be provided more detail on the underlying cryptographic techniques that Monero utilizes to ensure the privacy of every Monero user during the transaction process.

How Monero protects your privacy

Monero uses three unique methods in order to protect your privacy. We are going to review in a simple approach these techinques.

Stealth Address

What we have learned is that Monero uses a distributed peer-to-peer consensus network to record transaction outputs on a blockchain. If Leo owns Monero, it means that he has exclusive control over some of these outputs. When Leo sends Monero to George, Leo is announcing to the network that he wishes to transfer the value of some of his outputs to a new output for George, which only he can control. In other words, a transaction is the transformation of old outputs belonging to one wallet into new outputs belonging to another. Let's take this a step further, to see how stealth addresses enhance a user's privacy.

In every transaction, a stealth address, also known as a one-time public key, is automatically generated and recorded as part of the transaction to indicate who can spend an output in a later transaction. An outside observer cannot tell if funds are moving from Leo to George nor link wallet addresses together by just looking at the blockchain. Therefore, when Leo sends Monero to George, the output George receives will not be publicly associated with George's wallet address. However, if Leo ever needs to prove that he in fact sent Monero to George, his wallet has the ability to verify that payment was sent. George can rest assured that no one else can see when or if any Monero was sent to him.

If George were a merchant, this feature would be a great benefit, because no one can tell how many different customers he has, whether any of them are repeat customers, or if he has any customers at all.

A Monero wallet address is a 95-character string, which consists of a public view key and a public spend key. When Leo sends Monero to George, Leo's wallet will use George's public view key and public spend key as well as some random data to generate a unique onetime public key for George's new output.

Everyone can see the one-time public key on the blockchain, but only Leo and George know Leo sent Monero to George. The output is created in such a way that George is able to locate the output destined for him by scanning the blockchain with his wallet's private view key. Once the output is detected and retrieved by George's wallet, he would be able to calculate a one-time private key that corresponds with the one-time public key and spend the relevant output with his wallet's private spend key.

This whole process occurs without ever having George's wallet address publicly linked to any transaction. As you can see, stealth addresses prevent outputs from being associated with a recipient's public address. This is accomplished by the use of one-time destination public keys. One-time public keys are only spendable by the recipient, and only the recipient is able to detect their designated output on the blockchain. Since all outputs are unlinkable, the privacy of the recipient is ensured. On the input side of the transaction, the sender's privacy is protected with the use of ring signatures.

This document is a preview of the first chapter of the upcoming book
“Mastering Monero : The future of private transactions”.
It was written by several contributors. SerHack, 4matter,
cryptochangements and Uncaged Potential helped in writing this preview.

WOULD YOU LIKE TO SUGGEST US NEW IDEAS OR TO IMPROVE THE CONTENT?
CONTACT US SUPPORT@MASTERINGMONERO.COM OR /U/SERHACK

Website: https://masteringmonero.com
Github repository: https://github.com/monerobook/monerobook