⎇ main ▾   ⋯

nitda-blockchain-scholarship / **ch01.asciidoc**

☰ 246 lines (154 sloc)   36.3 KB   ⋯

🔗 Introduction

🔗 What Is Bitcoin?

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoin are used to store and transmit value among participants in the Bitcoin network. Bitcoin users communicate with each other using the Bitcoin protocol primarily via the internet, although other transport networks can also be used. The Bitcoin protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily accessible.

> Tip   Notice how the unit of currency is called "bitcoin" with a small *b*, and the system is called "Bitcoin", with a capital *B*.

Users can transfer bitcoin over the network to do just about anything that can be done with conventional currencies, including buying and selling goods, sending money to people or organizations, or extending credit. Bitcoin can be purchased, sold, and exchanged for other currencies at specialized currency exchanges. Bitcoin in a sense is the perfect form of money for the internet because it is fast, secure, and borderless.

Unlike traditional currencies, bitcoin is entirely virtual. There are no physical coins or even digital coins per se. The coins are implied in transactions that transfer value from sender to recipient. Users of Bitcoin own keys that allow them to prove ownership of bitcoin in the Bitcoin network. With these keys, they can sign transactions to unlock the value and spend it by transferring it to a new owner. Keys are often stored in a digital wallet on each user's computer or smartphone. Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.

Bitcoin is a distributed, peer-to-peer system. As such, there is no "central" server or point of control. Bitcoins, i.e. units of bitcoin, are created through a process called "mining," which involves competing to find solutions to a mathematical problem while processing Bitcoin transactions. Any participant in the Bitcoin network (i.e., anyone using a device running the full Bitcoin protocol stack) may operate as a miner, using their computer's processing power to verify and record transactions. Every 10 minutes, on average, a Bitcoin miner can validate the transactions of the past 10 minutes and is rewarded with brand new bitcoin. Essentially, Bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.

The Bitcoin protocol includes built-in algorithms that regulate the mining function across the network. The difficulty of the processing task that miners must perform is adjusted dynamically so that, on average, someone succeeds every 10 minutes regardless of how many miners (and how much processing) are competing at any moment. The protocol also halves the rate at which new bitcoin is created every 4 years, and limits the total number of bitcoin that will be created to a fixed total just below 21 million coins. The result is that the number of bitcoin in circulation closely follows an easily predictable curve that approaches 21 million by the year 2140. Due to bitcoin's diminishing rate of issuance, over the long term, the Bitcoin currency is deflationary. Furthermore, bitcoin cannot be inflated by "printing" new money above and beyond the expected issuance rate.

Behind the scenes, Bitcoin is also the name of the protocol, a peer-to-peer network, and a distributed computing innovation. The bitcoin currency is really only the first application of this invention. Bitcoin represents the culmination of decades of research in cryptography and distributed systems and includes four key innovations brought together in a unique and powerful combination. Bitcoin consists of:

- A decentralized peer-to-peer network (the Bitcoin protocol)

- A public transaction ledger (the blockchain)

- A set of rules for independent transaction validation and currency issuance (consensus rules)

- A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

As a developer, I see Bitcoin as akin to the internet of money, a network for propagating value and securing the ownership of digital assets via distributed computation. There's a lot more to Bitcoin than first meets the eye.

In this chapter we'll get started by explaining some of the main concepts and terms, getting the necessary software, and using Bitcoin for simple transactions. In the following chapters, we'll start unwrapping the layers of technology that make Bitcoin possible and examine the inner workings of the Bitcoin network and protocol.

Digital Currencies Before Bitcoin
The emergence of viable digital money is closely linked to developments in cryptography. This is not surprising when one considers the fundamental challenges involved with using bits to represent value that can be exchanged for goods and services. Three basic questions for anyone accepting digital money are:

1. Can I trust that the money is authentic and not counterfeit?

2. Can I trust that the digital money can only be spent once (known as the "double-spend" problem)?

3. Can I be sure that no one else can claim this money belongs to them and not me?

Issuers of paper money are constantly battling the counterfeiting problem by using increasingly sophisticated papers and printing technology. Physical money addresses the double-spend issue easily because the same paper note cannot be in two places at once. Of course, conventional money is also often stored and transmitted digitally. In these cases, the counterfeiting and double-spend issues are handled by clearing all electronic transactions through central authorities that have a global view of the currency in circulation. For digital money, which cannot take advantage of esoteric inks or holographic strips, cryptography provides the basis for trusting the legitimacy of a user's claim to value. Specifically, cryptographic digital signatures enable a user to sign a digital asset or transaction proving the ownership of that asset. With the appropriate architecture, digital signatures also can be used to address the double-spend issue.

When cryptography started becoming more broadly available and understood in the late 1980s, many researchers began trying to use cryptography to build digital currencies. These early digital currency projects issued digital money, usually backed by a national currency or precious metal such as gold.

Although these earlier digital currencies worked, they were centralized and, as a result, were easy to attack by governments and hackers. Early digital currencies used a central clearinghouse to settle all transactions at regular intervals, just like a traditional banking system. Unfortunately, in most cases, these nascent digital currencies were targeted by worried governments and eventually litigated out of existence. Some failed in spectacular crashes when the parent company liquidated abruptly. To be robust against intervention by antagonists, whether legitimate governments or criminal elements, a *decentralized* digital currency was needed to avoid a single point of attack. Bitcoin is such a system, decentralized by design, and free of any central authority or point of control that can be attacked or corrupted.

🔗 History of Bitcoin

Bitcoin was invented in 2008 with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System,"[1] written under the alias of Satoshi Nakamoto (see [satoshi_whitepaper]). Nakamoto combined several prior inventions such as b-money and HashCash to create a completely decentralized electronic cash system that does not rely on a central authority for currency issuance or settlement and validation of transactions. The key innovation was to use a distributed computation system (called a "Proof-of-Work" algorithm) to conduct a global "election" every 10 minutes, allowing the decentralized network to arrive at *consensus* about the state of transactions. This elegantly solves the issue of double-spend where a single currency unit can be spent twice. Previously, the double-spend problem was a weakness of digital currency and was addressed by clearing all transactions through a central clearinghouse.

The Bitcoin network started in 2009, based on a reference implementation published by Nakamoto and since revised by many other programmers. The implementation of the Proof-of-Work algorithm (mining) that provides security and resilience for Bitcoin has increased in power exponentially, and now exceeds the combined processing power of the world's top supercomputers. Bitcoin's total market value has at times exceeded $1 trillion US dollars, depending on the bitcoin-to-dollar exchange rate. The largest transaction processed so far by the network was $1.1 billion US dollars, transmitted instantly and processed for a fee of only $0.68.

Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers. The identity of the person or people behind Bitcoin is still unknown. However, neither Satoshi Nakamoto nor anyone else exerts individual control over the Bitcoin system, which operates based on fully transparent mathematical principles, open source code, and consensus among participants. The invention itself is groundbreaking and has already spawned new science in the fields of distributed computing, economics, and econometrics.

A Solution to a Distributed Computing Problem

Satoshi Nakamoto's invention is also a practical and novel solution to a problem in distributed computing, known as the "Byzantine Generals' Problem." Briefly, the problem consists of trying to agree on a course of action or the state of a system by exchanging information over an unreliable and potentially compromised network. Satoshi Nakamoto's solution, which uses the concept of Proof-of-Work to achieve consensus *without a central trusted authority*, represents a breakthrough in distributed computing and has wide applicability beyond currency. It can be used to achieve consensus on decentralized networks to prove the fairness of elections, lotteries, asset registries, digital notarization, and more.

🔗 Bitcoin Uses, Users, and Their Stories

Bitcoin is an innovation in the ancient technology of money. At its core, money simply facilitates the exchange of value between people. Therefore, in order to fully understand Bitcoin and its uses, we'll examine it from the perspective of people using it. Each of the people and their stories, as listed here, illustrates one or more specific use cases. We'll be seeing them throughout the book:

North American low-value retail
Alice lives in Northern California's Bay Area. She has heard about Bitcoin from her techie friends and wants to start using it. We will follow her story as she learns about Bitcoin, acquires some, and then spends some of her bitcoin to buy a cup of coffee at Bob's Cafe in Palo Alto. This story will introduce us to the software, the exchanges, and basic transactions from the perspective of a retail consumer.

North American high-value retail
Carol is an art gallery owner in San Francisco. She sells expensive paintings for Bitcoin. This story will introduce the risks of a "51%" consensus attack for retailers of high-value items.

Offshore contract services
Bob, the cafe owner in Palo Alto, is building a new website. He has contracted with an Indian web developer, Gopesh, who lives in Bangalore, India. Gopesh has agreed to be paid in bitcoin. This story will examine the use of Bitcoin for outsourcing, contract services, and international wire transfers.

Web store

Gabriel is an enterprising young teenager in Rio de Janeiro, running a small web store that sells Bitcoin-branded t-shirts, coffee mugs, and stickers. Gabriel is too young to have a bank account, but his parents are encouraging his entrepreneurial spirit.

Charitable donations

Eugenia is the director of a children's charity in the Philippines. Recently she has discovered Bitcoin and wants to use it to reach a whole new group of foreign and domestic donors to fundraise for her charity. She's also investigating ways to use Bitcoin to distribute funds quickly to areas of need. This story will show the use of Bitcoin for global fundraising across currencies and borders and the use of an open ledger for transparency in charitable organizations.

Import/export

Mohammed is an electronics importer in Dubai. He's trying to use Bitcoin to buy electronics from the United States and China for import into the UAE to accelerate the process of payments for imports. This story will show how Bitcoin can be used for large business-to-business international payments tied to physical goods.

Mining for bitcoin

Jing is a computer engineering student in Shanghai. He has built a "mining" rig to mine for bitcoin using his engineering skills to supplement his income. This story will examine the "industrial" base of Bitcoin: the specialized equipment used to secure the Bitcoin network and issue new currency.

Each of these stories is based on the real people and real industries currently using Bitcoin to create new markets, new industries, and innovative solutions to global economic issues.

🔗 Getting Started

Bitcoin is a protocol that can be accessed using a client application that speaks the protocol. A "Bitcoin wallet" is the most common user interface to the Bitcoin system, just like a web browser is the most common user interface for the HTTP protocol. There are many implementations and brands of Bitcoin wallets, just like there are many brands of web browsers (e.g., Chrome, Safari, Firefox, and Internet Explorer). And just like we all have our favorite browsers (Mozilla Firefox, Yay!) and our villains (Internet Explorer, Yuck!), Bitcoin wallets vary in quality, performance, security, privacy, and reliability. There is also a reference implementation of the Bitcoin protocol that includes a wallet, known as the "Satoshi Client" or "Bitcoin Core," which is derived from the original implementation written by Satoshi Nakamoto.

🔗 Choosing a Bitcoin Wallet

Bitcoin wallets are one of the most actively developed applications in the Bitcoin ecosystem. There is intense competition, and while a new wallet is probably being developed right now, several wallets from last year are no longer actively maintained. Many wallets focus on specific platforms or specific uses and some are more suitable for beginners while others are filled with features for advanced users. Choosing a wallet is highly subjective and depends on the use and user expertise. Therefore it would be pointless to recommend a specific brand or wallet. However, we can categorize Bitcoin wallets according to their platform and function and provide some clarity about all the different types of wallets that exist. Better yet, moving keys or seeds between Bitcoin wallets is relatively easy, so it is worth trying out several different wallets until you find one that fits your needs.

Bitcoin wallets can be categorized as follows, according to the platform:

Desktop wallet
    A desktop wallet was the first type of Bitcoin wallet created as a reference implementation and many users run desktop wallets for the features, autonomy, and control they offer. Running on general-use operating systems such as Windows and Mac OS has certain security disadvantages, however, as these platforms are often insecure and poorly configured.

Mobile wallet

A mobile wallet is the most common type of Bitcoin wallet. Running on smart-phone operating systems such as Apple iOS and Android, these wallets are often a great choice for new users. Many are designed for simplicity and ease-of-use, but there are also fully featured mobile wallets for power users.

Web wallet

Web wallets are accessed through a web browser and store the user's wallet on a server owned by a third party. This is similar to webmail in that it relies entirely on a third-party server. Some of these services operate using client-side code running in the user's browser, which keeps control of the Bitcoin keys in the hands of the user. Most, however, present a compromise by taking control of the Bitcoin keys from users in exchange for ease-of-use. It is inadvisable to store large amounts of bitcoin on third-party systems.

Hardware wallet

Hardware wallets are devices that operate a secure self-contained Bitcoin wallet on special-purpose hardware. They usually connect to a desktop or mobile device via USB cable or near-field-communication (NFC), and are operated with a web browser or accompanying software. By handling all Bitcoin-related operations on the specialized hardware, these wallets are considered very secure and suitable for storing large amounts of bitcoin.

Another way to categorize bitcoin wallets is by their degree of autonomy and how they interact with the Bitcoin network:

Full-node client

A full client, or "full node," is a client that stores the entire history of Bitcoin transactions (every transaction by every user, ever), manages users' wallets, and can initiate transactions directly on the Bitcoin network. A full node handles all aspects of the protocol and can independently validate the entire blockchain and any transaction. A full-node client consumes substantial computer resources (e.g., more than 125 GB of disk, 2 GB of RAM) but offers complete autonomy and independent transaction verification.

Lightweight client

A lightweight client, also known as a simplified-payment-verification (SPV) client, connects to Bitcoin full nodes (mentioned previously) for access to the Bitcoin transaction information, but stores the user wallet locally and independently creates, validates, and transmits transactions. Lightweight clients interact directly with the Bitcoin network, without an intermediary.

Third-party API client

A third-party API client is one that interacts with Bitcoin through a third-party system of application programming interfaces (APIs), rather than by connecting to the Bitcoin network directly. The wallet may be stored by the user or by third-party servers, but all transactions go through a third party.

Combining these categorizations, many Bitcoin wallets fall into a few groups, with the three most common being desktop full client, mobile lightweight wallet, and web third-party wallet. The lines between different categories are often blurry, as many wallets run on multiple platforms and can interact with the network in different ways.

For the purposes of this book, we will be demonstrating the use of a variety of downloadable Bitcoin clients, from the reference implementation (Bitcoin Core) to mobile and web wallets. Some of the examples will require the use of Bitcoin Core, which, in addition to being a full client, also exposes APIs to the wallet, network, and transaction services. If you are planning to explore the programmatic interfaces into the Bitcoin system, you will need to run Bitcoin Core, or one of the alternative clients.

🔗 Quick Start

Alice, who we introduced in Bitcoin Uses, Users, and Their Stories, is not a technical user and only recently heard about Bitcoin from her friend Joe. While at a party, Joe is once again enthusiastically explaining Bitcoin to all around him and is offering a demonstration. Intrigued, Alice asks how she can get started with Bitcoin. Joe says that a mobile wallet is best for new users and he recommends a few of his favorite wallets. Alice downloads "Bluewallet" (available for iOS and Android) and installs it on her phone.

When Alice runs her wallet application for the first time, she chooses the option to create a new Bitcoin wallet, and takes a moment **away from Joe and all other parties** to write down a secret mnemonic phrase *in order* on a piece of paper. As explained by the mobile wallet and by Joe earlier, the mnemonic phrase allows Alice to restore her wallet in case she loses her mobile device and grants her access to her funds on another device. After creating her wallet and securing her mnemonic phrase, Alice can tap on her wallet to see her bitcoin amount, transaction history, as well as two buttons that allow her to either *receive* or *send* bitcoin, shown in Alice uses the Receive screen on her Bluewallet mobile Bitcoin wallet, and displays her address to Bob in a QR code format.

🔗 Mnemonic Words

A modern Bitcoin wallet will provide a *mnemonic phrase* (also sometimes called a "seed" or "seed phrase") for Alice to back up. The mnemonic phrase consists of 12-24 English words, selected randomly by the software, and used as the basis for the keys that are generated by the wallet. The mnemonic phrase can be used by Alice to restore all the transactions and funds in her wallet in the case of an event such as a lost mobile device, a software bug, or memory corruption.

Tip	The correct term for these backup words is "mnemonic phrase". We avoid the use of the term "seed" to refer to a mnemonic phrase, because even though its use is common it is incorrect.

🔗 Storing the Mnemonic Safely

Alice needs to be careful to store the mnemonic phrase in a way that balances the need to prevent theft and accidental loss. If she doesn't protect it enough, her mnemonic will be at risk of being stolen. If she protects it too much, her mnemonic will be at risk of being permanently lost. The recommended way to properly balance these risks is to write two copies of the mnemonic phrase on paper, with each of the words numbered as the order matters.

Once Alice has recorded the mnemonic phrase, she should plan to store each copy in a separate secure location such as a locked desk drawer or a fireproof safe.

Warning

Never attempt a "DIY" security scheme that deviates in any way from the best practice recommendation in Storing the Mnemonic Safely. Do not cut your mnemonic in half, make screenshots, store on USB drives, email or cloud drives, encrypt it, or try any other non-standard method. You will tip the balance in such a way as to risk permanent loss or theft. Many people have lost funds, not from theft but because they tried a non-standard solution without having the expertise to balance the risks involved. The best practice recommendation is carefully balanced by experts and suitable for the vast majority of users.

❎ BluewalletWelcome

Figure 1. Alice uses the Receive screen on her Bluewallet mobile Bitcoin wallet, and displays her address to Bob in a QR code format
The main wallet view displays the bitcoin amount, transaction history, and *Receive* and *Send* buttons. In addition, many wallets feature the ability to purchase Bitcoin directly through an exchange or similar service where you can offer fiat money in return for cryptocurrency, which is done by [bitcoin_price] and selling to the wallet user at or above this price. The *Buy Bitcoin* button would allow Alice to purchase Bitcoin in this fashion.

Alice is now ready to start using her new bitcoin wallet. Her wallet application randomly generated a private key (described in more detail in [private_keys]) which will be used to derive Bitcoin addresses that direct to her wallet. At this point, her Bitcoin addresses are not known to the Bitcoin network or "registered" with any part of the Bitcoin system. Her Bitcoin addresses are simply random numbers that correspond to her private key that she can use to control access to the funds. The addresses are generated independently by her wallet without reference or registration with any service. In fact, in most wallets, there is no association between a Bitcoin address and any externally identifiable information including the user's identity. Until the moment an address is referenced as the recipient of value in a transaction posted on the bitcoin ledger, the Bitcoin address is simply part of the vast number of possible addresses that are valid in bitcoin. Only once an address has been associated with a transaction does it become part of the known addresses in the network.

Alice uses the *Receive* button, which displays a QR code along with a Bitcoin address. The QR code is the square with a pattern of black and white dots, serving as a form of barcode that contains the same information in a format that can be scanned by Joe's smartphone camera. Next to the wallet's QR code is the Bitcoin address it encodes, and Alice may choose to manually send her address to Joe by copying it onto her clipboard with a tap. Of note, when receiving funds to a new mobile wallet for the first time, many wallets will often re-verify that you have indeed secured your mnemonic phrase. This can range from a simple prompt to requiring the user to manually re-enter the phrase.

Tip

Bitcoin addresses start with 1, 3, or bc1. Like email addresses, they can be shared with other bitcoin users who can use them to send bitcoin directly to your wallet. There is nothing sensitive, from a security perspective, about the Bitcoin address. It can be posted anywhere without risking the security of the account. Unlike email addresses, you can create new addresses as often as you like, all of which will direct funds to your wallet. In fact, many modern wallets automatically create a new address for every transaction to maximize privacy. A wallet is simply a collection of addresses and the keys that unlock the funds within.

==== Getting Her First Bitcoin

There are several ways Alice can acquire bitcoin:

- She can exchange some of her national currency (e.g. USD) at a cryptocurrency exchange

- She can buy some from a friend, or an acquaintance from a Bitcoin Meetup, in exchange for cash

- She can find a *Bitcoin ATM* in her area, which acts as a vending machine, selling bitcoin for cash

- She can offer her skills or a product she sells and accepts payment in bitcoin

- She can ask her employer or clients to pay her in bitcoin

All of these methods have varying degrees of difficulty, and many will involve paying a fee. Some financial institutions will also require Alice to provide identification documents to comply with local banking regulations/anti-money laundering (AML) practices, a process which is known as Know Your Customer (KYC). However, with all these methods, Alice will be able to receive bitcoin.

Tip	One of the advantages of bitcoin over other payment systems is that, when used correctly, it affords users much more privacy. Acquiring, holding, and spending bitcoin does not require you to divulge sensitive and personally identifiable information to third parties. However, where bitcoin touches traditional systems, such as currency exchanges, national and international regulations often apply. In order to exchange bitcoin for your national currency, you will often be required to provide proof of identity and banking information. Users should be aware that once a Bitcoin address is attached to an identity, all associated bitcoin transactions are also easy to identify and track. This is one reason many users choose to maintain dedicated exchange accounts unlinked to their wallets.

Alice was introduced to bitcoin by a friend so she has an easy way to acquire her first bitcoin. Next, we will look at how she buys bitcoin from her friend Joe and how Joe sends the bitcoin to her wallet.

==== Finding the Current Price of Bitcoin

Before Alice can buy bitcoin from Joe, they have to agree on the *exchange rate* between bitcoin and US dollars. This brings up a common question for those new to bitcoin: "Who sets the bitcoin price?" The short answer is that the price is set by markets.

Bitcoin, like most other currencies, has a *floating exchange rate*. That means that the value of bitcoin vis-a-vis any other currency fluctuates according to supply and demand in the various markets where it is traded. For example, the "price" of bitcoin in US dollars is calculated in each market based on the most recent trade of bitcoin and US dollars. As such, the price tends to fluctuate minutely several times per second. A pricing service will aggregate the prices from several markets and calculate a volume-weighted average representing the broad market exchange rate of a currency pair (e.g., BTC/USD).

There are hundreds of applications and websites that can provide the current market rate. Here are some of the most popular:

Bitcoin Average

A site that provides a simple view of the volume-weighted-average for each currency.

CoinCap

A service listing the market capitalization and exchange rates of hundreds of crypto-currencies, including bitcoin.

Chicago Mercantile Exchange Bitcoin Reference Rate

A reference rate that can be used for institutional and contractual reference, provided as part of investment data feeds by the CME.

In addition to these various sites and applications, most bitcoin wallets will automatically convert amounts between bitcoin and other currencies. Joe will use his wallet to convert the price automatically before sending bitcoin to Alice.

==== Sending and Receiving Bitcoin

Alice has decided to exchange $10 US dollars for bitcoin, so as not to risk too much money on this new technology. She gives Joe $10 in cash, opens her Bluewallet mobile wallet application, and selects Receive. This displays a QR code with Alice's first Bitcoin address.

Joe then selects Send on his Bluewallet smartphone wallet and is presented with a screen containing the following inputs:

- The amount to send, in bitcoin (BTC) or his local currency (USD)

- A destination Bitcoin address

- A transaction note (description)

- A transaction fee

In the input field for the Bitcoin address, there is a small *Scan* button. This allows Joe to scan the QR code with his smartphone camera so that he doesn't have to type in Alice's Bitcoin address, which is quite long and difficult to type. Joe taps the *Scan* button and it activates the smartphone camera, scanning the QR code displayed on Alice's smartphone.

Joe now has Alice's Bitcoin address set as the recipient. Joe enters the amount as $10 US dollars and his wallet converts it by accessing the most recent exchange rate from an online service. The exchange rate at the time is $100 US dollars per bitcoin, so $10 US dollars is worth 0.10 bitcoin (BTC), or 100 millibitcoin (mBTC) as shown in the screenshot from Joe's wallet (see Bluewallet mobile bitcoin wallet send screen).

In the transaction note/description input, Joe enters "Alice". He can use this field to add some information regarding his transaction for future reference. This function is for his record keeping only. The transaction note will be stored in his wallet and only Joe will be able to see it. It will not be sent to Alice, nor stored on the blockchain.

He also selects a transaction fee for his transaction. The higher the transaction fee, the faster his transaction will be confirmed (included in a block by a miner). He selects the minimum transaction fee possible at that time (0 satoshis/byte).

Tip	The price of bitcoin has changed a lot over time, and an incredible amount since the first edition of this book was written. As of March 2021, a person would need approximately $54,000 USD to purchase one whole bitcoin. Many examples in this book reference real-life past transactions, when the price of bitcoin was much lower and transactions with zero fees were still possible. Think about how generous of a friend Joe would have been if he had made the same agreement with Alice today!

bluewallet mobile send screen

Figure 2. Bluewallet mobile bitcoin wallet send screen

Using Bluewallet, Joe carefully checks to make sure he has entered the correct amount, because he is about to transmit money and mistakes are irreversible. For simplicity sake, we will assume that Joe does not pay any transaction fees. The purpose and setting of transaction fees are covered in subsequent chapters. After double-checking the address and amount, he presses *Send* to transmit the transaction. Joe's mobile bitcoin wallet constructs a transaction that assigns 0.10 BTC to the address provided by Alice, sourcing the funds from Joe's wallet and signing the transaction with Joe's private keys. This tells the Bitcoin network that Joe has authorized a transfer of value to Alice's new address. As the transaction is transmitted via the peer-to-peer protocol, it quickly propagates across the Bitcoin network. In less than a second, most of the well-connected nodes in the network receive the transaction and see Alice's address for the first time.

Meanwhile, Alice's wallet is constantly "listening" to published transactions on the Bitcoin network, looking for any that match the addresses it contains. A few seconds after Joe's wallet transmits the transaction, Alice's wallet will indicate that it is receiving 0.10 BTC.

Tip	Each bitcoin can be subdivided into 100 million units, each called a "satoshi" (singular) or "satoshis" (plural). Named for bitcoin's creator, the Satoshi is the smallest unit of bitcoin, equivalent to 0.00000001 BTC.

Confirmations

At first, Alice's wallet will show the transaction from Joe as "Unconfirmed." This means that the transaction has been propagated to the network but has not yet been recorded in the bitcoin transaction ledger, known as the blockchain. To be confirmed, a transaction must be included in a block and added to the blockchain, which happens every 10 minutes, on average. In traditional financial terms this is known as *clearing*. This book will cover in detail the propagation, validation, and clearing (or confirmation) of bitcoin transactions.

Alice is now the proud owner of 0.10 BTC that she can spend. In the next chapter we will look at her first purchase with bitcoin, and examine the underlying transaction and propagation technologies in more detail.

1. "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf).