Introduction

What is Bitcoin?

Bitcoin is collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoins 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.

Users can transfer bitcoin over the network to do just about anything that can be done with conventional currencies, such as buy and sell goods, send money to people or organizations, or extend credit. Bitcoin technology includes features that are based on encryption and digital signatures to ensure the security of the bitcoin network. Bitcoins 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, bitcoins are entirely virtual. There are no physical coins or even digital coins per se. The coins are implied in transactions which transfer value from sender to recipient. Users of bitcoin own keys which allow them to prove ownership of transactions in the bitcoin network, unlocking the value to spend it and transfer it to a new recipient. Those keys are stored in a digital wallet on each user's computer. Possession of the key that unlocks a transaction is the only prerequisite to spending bitcoins, putting the control entirely in the hands of each user.

Bitcoin is a fully-distributed, peer-to-peer system. As such there is no "central" server or point of control. Bitcoins are created through a process called "mining", which involves looking for a solution to a difficult problem. Any participant in the bitcoin network (i.e. any device running the full bitcoin protocol

stack) may operate as a miner, using their computer's processing power to attempt to find solutions to this problem. Every 10 minutes on average, a new solution is found by someone who then is able to validate the transactions of the past 10 minutes and is rewarded with brand new bitcoins. Essentially, the currency issuance function of a central bank and the clearing function are de-centralized and turned into a global competition.

The bitcoin protocol includes built-in algorithms that regulate the mining function across the network. The difficulty of the problem that miners must solve is adjusted dynamically so that, on average, someone finds a correct answer every 10 minutes regardless of how many miners (and CPUs) are working on the problem at any moment. The protocol also halves the rate at which new bitcoins are created every 4 years, and limits the total number of bitcoins that will be created to a fixed total of 21 million coins. The result is that the number of bitcoins in circulation closely follows an easily predictable curve that reaches 21 million by the year 2140. As a result, the bitcoin currency is deflationary and 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 network and a distributed computing innovation. The bitcoin currency is really only the first application of this invention. 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 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.

History of 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. Two fundamental questions for anyone accepting digital money are:

1. Can I trust the money is authentic and not counterfeit?
2. Can I be sure that no one else can claim that this money belongs to them and not me? (aka the "double-spend" problem)

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 this case 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.

While these earlier digital currencies worked, they were centralized and as a result they 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 they are legitimate governments or criminal elements, a digital currency is needed to avoid the use of a central currency issuer or transaction clearing authority that could be a single point of attack. Bitcoin is such a system, completely de-centralized by design, lacking any central authority or point of control that can be attacked or corrupted.

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 de-centralized peer-to-peer network (the bitcoin protocol);
- A public transaction ledger (the blockchain);
- A de-centralized mathematical and deterministic currency issuance (distributed mining), and;
- A de-centralized transaction verification system (transaction script)

Bitcoin was invented in 2008 by Satoshi Nakamoto with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System". Satoshi Nakamoto combined several prior inventions such as b-money and HashCash to create a completely de-centralized 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 Proof-Of-Work algorithm to conduct a global "election" every 10 minutes, allowing the de-centralized 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. During the first four years of operation, the network has grown to include an enormous amount of Proof-Of-Work computation, thereby increasing its security and resilience. In 2013, the total market value of bitcoin's primary monetary supply measure (M0) is estimated at more than 10 billion US dollars. The largest transaction processed by the network was $150 million US dollars, transmitted instantly and processed without any fees.

Satoshi Nakamoto withdrew from the public in April of 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers. The name Satoshi Nakamoto is an alias and the identity of the person or people behind this invention is currently unknown. However, neither Satoshi Nakamoto nor anyone else exerts control over the bitcoin system, which operates based on fully transparent mathematical principles. 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 solution to a previously unsolved problem in distributed computing, known as the Byzantine Generals problem. Briefly, the problem consists of trying to agree on a course of action 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 science and has wide applicability beyond currency. It can be used to achieve consensus on decentralized networks for provably-fair elections, lotteries, asset registries, digital notarization and more.

Bitcoin Uses, Users and Their Stories

Bitcoin is a technology, but it expresses money which is fundamentally a language for exchanging value between people. Let's look at the people who are using bitcoin and some of the most common uses of the currency and protocol through their stories. We will re-use these stories throughout the book to illustrate the real-life uses of digital money and how they are made possible by the various technologies that are part of bitcoin.

North American 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.

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.

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.

Remittances and Reverse Remittances

Gopesh, the Indian web developer, is supporting his daughter Radhika who is a student in Essex, England. Gopesh is now considering sending Radhika bitcoin, eliminating the fees he used to pay for remittances. This story will demonstrate the use of local exchange and peer-to-peer exchanges for international remittances with bitcoin.

Import/Export

Mohammed is an electronics importer in Dubai. He's trying to use bitcoin to buy electronics from the USA and China for import into the U.A.E. 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 bitcoins, 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.

Peer Lending

Zenab is a shopkeeper in Kisumu, Kenya and needs a loan to buy new inventory for her shop. With the assistance of a micro-lending organization, she is financing a micro-loan in bitcoin from individual lenders all across the world. This story will demonstrate the potential for bitcoin to offer peer-to-peer micro-lending by aggregating small investments, matching them with borrowers in

developing nations.

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

Getting Started

To join the bitcoin network and start using the currency, all a user has to do is download an application. Since bitcoin is a standard, there are many implementations of the bitcoin client software. There is also a "reference implementation", also known as the Satoshi Client, which is managed as an open source project by a team of developers and is derived from the original implementation written by Satoshi Nakamoto.

The three primary forms of bitcoin clients are:

Full Client

A full client, or "full node" is a client that stores the entire history of bitcoin transactions, manages the user's wallets and can initiate transactions directly on the bitcoin network. This is similar to a standalone email server, in that it handles all aspects of the protocol without relying on any other servers or third party services.

Light Client

A lightweight client stores the user's wallet but relies on third-party owned servers for access to the bitcoin transactions and network. The light client does not store a full copy of all transactions and therefore must trust the third party servers for transaction validation. This is similar to a standalone email client that connects to a mail server for access to a mailbox, in that it relies on a third party for interactions with the network.

Web Client

Web-clients 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.

Mobile Bitcoin

Mobile clients for smartphones, such as those based on the Android system, can either operate as full clients, light clients or web clients. Some mobile clients are synchronized with a web or desktop client, providing a multi-platform wallet across multiple devices but with a common source of funds. See [mobile_bitcoin]

The choice of bitcoin client depends on how much control the user wants over funds. A full client will offer the highest level of control and independence for the user, but in turn puts the burden of backups and security on the user. On the other end of the range of choices, a web client is the easiest to set up and use, but the tradeoff with a web client is that counterparty risk is introduced because security and control is shared by the user and the owner of the web service. If a web-wallet service is compromised, as many have been, the users can lose all their funds. Conversely, if a user has a full client without adequate backups, they may lose their funds through a computer mishap.

For the purposes of this book, we will be demonstrating the use of a variety of bitcoin clients, from the reference implementation (the Satoshi client) to web-wallets. Some of the examples will require the use of the reference client which 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 the reference client.

Quick Start - Web Wallet

A web-wallet is the easiest way to start using bitcoin, and is the choice of Alice who we introduced in [user-stories]. Alice is not a technical user and only recently heard about bitcoin from a friend. She starts her journey by visiting the official website bitcoin.org, where she finds a broad selection of bitcoin clients. Following the advice on the bitcoin.org site, she chooses a web-wallet by blockchain.info, a popular hosted-wallet service. Following a link from bitcoin.org, she opens the blockchain.info wallet page at https://blockchain.info/wallet and selects "Start a New Wallet". To register her new wallet, she must enter an email address, enter a password and prove that she is a human by completing a

CAPTCHA test.

Warning

> When creating a bitcoin wallet you will need to provide a password or passphrase to protect your wallet. There are many bad actors attempting to break weak passwords, so take care to select one that cannot be easily broken. Use a combination of upper and lower-case characters, numbers and symbols. Avoid personal information such as birthdates or names of sports teams. Avoid any words commonly found in dictionaries, in any language. If you can, use a password generator to create a completely random password that is at least 12 characters in length. Remember: bitcoin is money and can be instantly moved anywhere in the world. If it is not well protected, it can be easily stolen.

Once Alice has completed the registration form, she is presented with a Wallet Recovery Mnemonic. This is a series of words that can be used to reconstruct her wallet in case she loses the password or account details. Following the instructions on screen, Alice copies the words onto paper, locking it away in a secure location.

Figure 1. Blockchain.info - Wallet Recovery Mnemonic

A few seconds later, Alice can start using her new bitcoin web-wallet by logging in with her account ID and password. In her web browser, she sees the web-wallet home screen:

Figure 2. Blockchain.info - Wallet Home Screen

The most important part of this screen is Alice's *bitcoin address*. Like an email address, Alice can share this address and anyone can use it to send money directly to her new web-wallet. On the screen it appears as a long string of letters and numbers: `1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`. Next to the wallet's bitcoin address, there is a QR code, a form of barcode that contains the same information in a format that can be easily scanned by a smartphone's camera. Alice can print the QR code as a way to easily give her address to others without them having to type the long string of letters and numbers.

> **Tip**
>
> Bitcoin addresses start with the digit "1". Like email addresses, they can be shared with other bitcoin users who can use them to send bitcoin directly to your wallet. Unlike email addresses, you can create new addresses as often as you like, all of which will direct funds to your wallet. A wallet is simply a collection of addresses and the keys that unlock the funds within. There is practically no limit to the number of addresses a user can create.

Alice is now ready to start using her new bitcoin web-wallet.

Getting your first bitcoins

It is not possible to buy bitcoins at a bank or foreign exchange kiosks at this time. It is not possible to use a credit card to buy bitcoins, either. As of 2014, it is still quite difficult to acquire bitcoins in most countries. There are a number of specialized currency exchanges where you can buy and sell bitcoin in exchange for a local currency. These operate as web-based currency markets and include:

- Bitstamp (bitstamp.net), a European currency market that supports several currencies including euros (EUR) and US dollars (USD) via wire transfer
- Coinbase (coinbase.com), a US-based currency market in California that supports US dollar exchange to and from bitcoin. Coinbase can connect to US checking accounts via the ACH system.

Crypto-currency exchanges such as these operate at the intersection of national currencies and crypto-currencies. As such, they are subject to national and international regulations and are often specific to a single country or economic area and specialize in the national currencies of that area. Your choice of currency exchange will be specific to the national currency you use and limited to the exchanges that operate within the legal jurisdiction of your country. Similar to opening a bank account, it takes several days or weeks to set up the necessary accounts with the above services because they require various forms of identification to comply with KYC (Know Your Customer) and AML (Anti-Money Laundering) banking regulations. Once you have an account on a bitcoin exchange, you can then buy or sell bitcoins quickly just as you could with foreign currency with a brokerage account.

A more complete list can be found at http://bitcoincharts.com/markets/, a site that offers price quotes and other market data across many dozens of currency exchanges.

There are three other methods for getting bitcoins as a new user:

- Find a friend who has bitcoins and buy some from them directly. Many bitcoin users started this way.
- Use a classified service like localbitcoins.com to find a seller in your area to buy bitcoins for cash in an in-person transaction.
- Sell a product or service for bitcoin. If you're a programmer, sell your programming skills. If you have an online store, see [bitcoin-commerce] to sell in bitcoin.

Alice was introduced to bitcoin by a friend and so she has an easy way of getting her first bitcoin while she waits for her account on a California currency market to be verified and activated.

Sending and receiving bitcoins

Alice has created her bitcoin web-wallet and she is now ready to receive funds. Her web-wallet application generated a bitcoin address and the corresponding key (an elliptic curve private key, described in more detail in [private keys]). At this point, her bitcoin address is not known to the bitcoin network or "registered" with any part of the bitcoin system. Her bitcoin address is simply a number that

corresponds to a key that she can use to control access to the funds. There is no account or association between that address and an account. Until the moment this address is referenced as the recipient of value in a transaction posted on the bitcoin ledger (the blockchain), it is simply part of the vast number of possible addresses that are "valid" in bitcoin. Once it has been associated with a transaction, it becomes part of the known addresses in the network and anyone can check its balance on the public ledger.

Alice meets her friend Joe who introduced her to bitcoin at a local restaurant so they can exchange some US dollars and put some bitcoins into her account. She has brought a print out of her address and the QR code as shown on the home page of her web-wallet. There is nothing sensitive from a security perspective about the bitcoin address. It can be posted anywhere without risking the security of her account and it can be changed by creating a new address at any time. Alice wants to convert just $10 US dollars into bitcoin, so as not to risk too much money on this new technology. She gives Joe a $10 bill and the printout of her address so that Joe can send her the equivalent amount of bitcoin.

First, Joe has to figure out the exchange rate so that he can give the correct amount of bitcoin to Alice. There are hundreds of applications and web sites that can provide the current market rate, here are some of the most popular:

- bitcoincharts.com, a market data listing service that shows the market rate of bitcoin across many exchanges around the globe, denominated in different local currencies
- bitcoinaverage.com, a site that provides a simple view of the volume-weighted-average for each currency
- ZeroBlock, a free Android and iOS application that can display a bitcoin price from different exchanges

Figure 3. ZeroBlock - A bitcoin market-rate application for Android and iOS

Using one of the applications or websites above, Joe determines the price of bitcoin to be approximately

$100 US dollars per bitcoin. At that rate he should give Alice 0.10 bitcoin, also known as 100 milliBits, in return for the $10 US dollars she gave him.

Once Joe has established a fair exchange price, he opens his mobile wallet application and selects to "send" bitcoin. He is presented with a screen requesting two inputs:

- The destination bitcoin address for the transaction
- The amount of bitcoin to send

Figure 4. Bitcoin mobile wallet - Send bitcoin screen

In the input field for the bitcoin address, there is a small icon that looks like a QR code. This allows Joe to scan the barcode with his smartphone camera so that he doesn't have to type in Alice's bitcoin address (`1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK`), which is quite long and difficult to type. Joe taps on the QR code icon and activates the smartphone camera, scanning the QR code from Alice's printed wallet that she brought with her. The mobile wallet application fills in the bitcoin address and Joe can check that it scanned correctly by comparing a few digits from the address with the address printed by Alice.

Joe then enters the bitcoin value for the transaction, 0.10 bitcoin. He carefully checks to make sure he has entered the correct amount, as he is about to transmit money and any mistake could be costly. Finally, he presses "Send" to transmit the transaction. Joe's mobile bitcoin wallet constructs a transaction that assigns 0.10 bitcoin 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 from one of his addresses 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.

If Alice has a smartphone or laptop with her, she will also be able to see the transaction. The bitcoin

ledger - a constantly growing file that records every bitcoin transaction that has ever occurred - is public, meaning that all she has to do is look up her own address and see if any funds have been sent to it. She can do this quite easily at the blockchain.info website by entering her address in the search box. The website will show her a page (https://blockchain.info/address/1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK) listing all the transactions to and from that address. If Alice is watching that page, it will update to show a new transaction transferring 0.10 bitcoin to her balance soon after Joe hits "Send".

Confirmations

At first, Alice's address will show the transaction from Joe as "Unconfirmed". This means that the transaction has been propagated to the network but has not yet been included in the bitcoin transaction ledger, known as the blockchain. To be included, the transaction must be "picked up" by a miner and included in a block of transactions. Once a miner has discovered a solution to the Proof-of-Work algorithm for this block (in approximately 10 minutes), the transactions within the block will be accepted as "confirmed" by the network and can be spent. The transaction is seen by all instantly, but it is only "trusted" by all when it is included in a newly mined block. The more blocks mined after that block, the more trusted it is, as more and more computation is "piled" on top of it.

Alice is now the proud owner of 0.10 bitcoin which 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.

Last updated 2014-06-25 19:31:48 CDT