



**ANONYMOUS
BITCOIN**
/Kristov Atlas/

How To Keep Your \$ All To Yourself

First Edition

About this Document

This is a preview version of the book, “Anonymous Bitcoin: How to Keep Your ₿ All To Yourself”, by Kristov Atlas.

In order to acquire the full book, please visit:

<http://anonymousbitcoinbook.com>

Table of Contents

Information			
About the Author	ii		
Copyright	iii		
Disclaimers	iv		
About This Book	v		
Acknowledgements	vi		
Preface	vii		
A Quote	viii		
Chapter 1: An Offer You Can't Refuse	9		
The Appointment	11		
Chapter 2: What is Bitcoin?	14		
Bitcoin Basics	15		
Chapter 3: Anonymous Bitcoin Ownership	18		
Understanding Anonymity	19		
Anonymous Bitcoin	22		
Chapter 4: Challenges to Bitcoin Anonymity	24		
A Timeline of Bitcoin Ownership	26		
The Blockchain	32		
The Worst-Case Investigator	41		
		Chapter 5: Buying Anonymously	49
		Anonymity as Frosting	51
		Immediate Anonymity	56
		Selecting Software for Your Anonymous Bitcoin Toolkit	59
		Configuring Your Anonymous Bitcoin Toolkit	69
		White Market BTC – Coinbase Walk-Through	94
		LocalBitcoins.com Walk-Through	101
		Mixer Chain Walk-Through	108
		Chapter 6: Maintaining Anonymity After Purchase	130
		Maintaining Anonymous Ownership	131
		Chapter 7: Selling and Spending Anonymously	134
		Important Considerations for Selling and Spending Anonymously	135
		Selling Bitcoins Anonymously	138
		Spending Bitcoins Anonymously	141
		Chapter 8: The Future of Bitcoin Anonymity	143
		Decentralized Exchanges	144
		Decentralized Mixers	145
		Protocol-Level Mixers	149

Appendices	151
Appendix I: Online Services and JavaScript Requirements	152
Appendix II: Copying Linux to a USB Drive in Windows	153
Appendix III: Copying Linux to a USB Drive in OS X	155
Appendix IV: Creating a Fresh Anonymous Bitcoin Session	158
Appendix V: Opening TrueCrypt in Tails Linux	160
Appendix VI: Opening Bitcoin-Qt in Offline Mode	165
Appendix VII: Safely Shutting Down Tails Linux	169
Appendix VIII: Retrieving Bitcoins from Cold Storage Using Bitcoin-Qt	170
Appendix IX: Formatting a USB Drive in Windows 7	181
Appendix X: Formatting a USB Drive in OS X	182
References	184
Images Used	185
Links	186
Citations	190

About the Author



Kristov is a philosopher, entrepreneur, and security expert.

He holds a B.S. in Computer Science, and an M.S. in Computer Science with a focus on security.

His background in security includes privacy, static code analysis, malware forensics, and application security.

Kristov provided slides for the Bitcoin primer, "[The Truth About Bitcoin](#)".



© 2014, Kristov Atlas

Published February 4th, 2014.

The author of this book defensively reserves all legal rights.

Since this book is for sale, I prefer that you not transmit it to friends for free, but either purchase a copy on their behalf, or encourage them to do so. Writing a book requires time and brainpower, and I would like for myself and other authors to feel encouraged to produce work in the future by being compensated for our labor.

The book is published and distributed in a completely DRM-free format.

If you have received this book for free and find it to be of value, please consider purchasing it through my online store:

<http://anonymousbitcoinbook.com>

You can also send Bitcoin donations of your own specified size at the same website.

If you have any questions or comments on this topic, feel free to contact me at:

author@anonymousbitcoinbook.com

Disclaimers



This book is not intended to serve as legal advice. Some techniques for achieving anonymous bitcoin ownership, as well as bitcoin ownership in general may be illegal in certain tax jurisdictions. Nothing in the book should be construed as encouragement to break laws. Before making any decisions about bitcoin ownership, you should consult qualified legal and tax professionals.

Chapter 1 describes a dark scenario in which a criminal gang seeks to steal part or all of your bitcoins. As unlikely as this scenario might be, it presents a model for the worst-case adversary of a bitcoin owner, and illustrates potential motivations for anonymous ownership of bitcoins.

Chapter 2 explains the basic elements of Bitcoin required in order to understand how to own bitcoins anonymously.

Chapter 3 explains exactly what anonymity entails and how it applies to Bitcoin.

Chapter 4 provides more in-depth analysis on how Bitcoin anonymity can be taken away from owners.

Chapter 5 presents multiple approaches for the anonymous purchasing of bitcoin ownership, and provides a systematic walk-through of the most recommended method for doing so.

Chapter 6 explains how to keep your bitcoins anonymous after purchase until you're ready to send them to someone else.

Chapter 7 explores the tricky task of trading your bitcoins for other currencies, products, and services without compromising your anonymity.

Chapter 8 takes a look into the future of up-and-coming software projects that will define the coming months and years of Bitcoin anonymity.

Acknowledgements

Chief Editor: Cheryl Hulseapple

Preface author: Jeffrey Tucker

Editors: Greg Andres, Pepe Giménez, Jack Sterling, Jake Desyllas, Luna Grey, Hannah Braime, and Cody Dodd

Diagrams: Luna Grey, Kristov Atlas

Special thanks to:

Martin Harrigan, Gregory Maxwell, and Peter Todd for providing their time and insight into Bitcoin anonymity, as well as their respective projects.

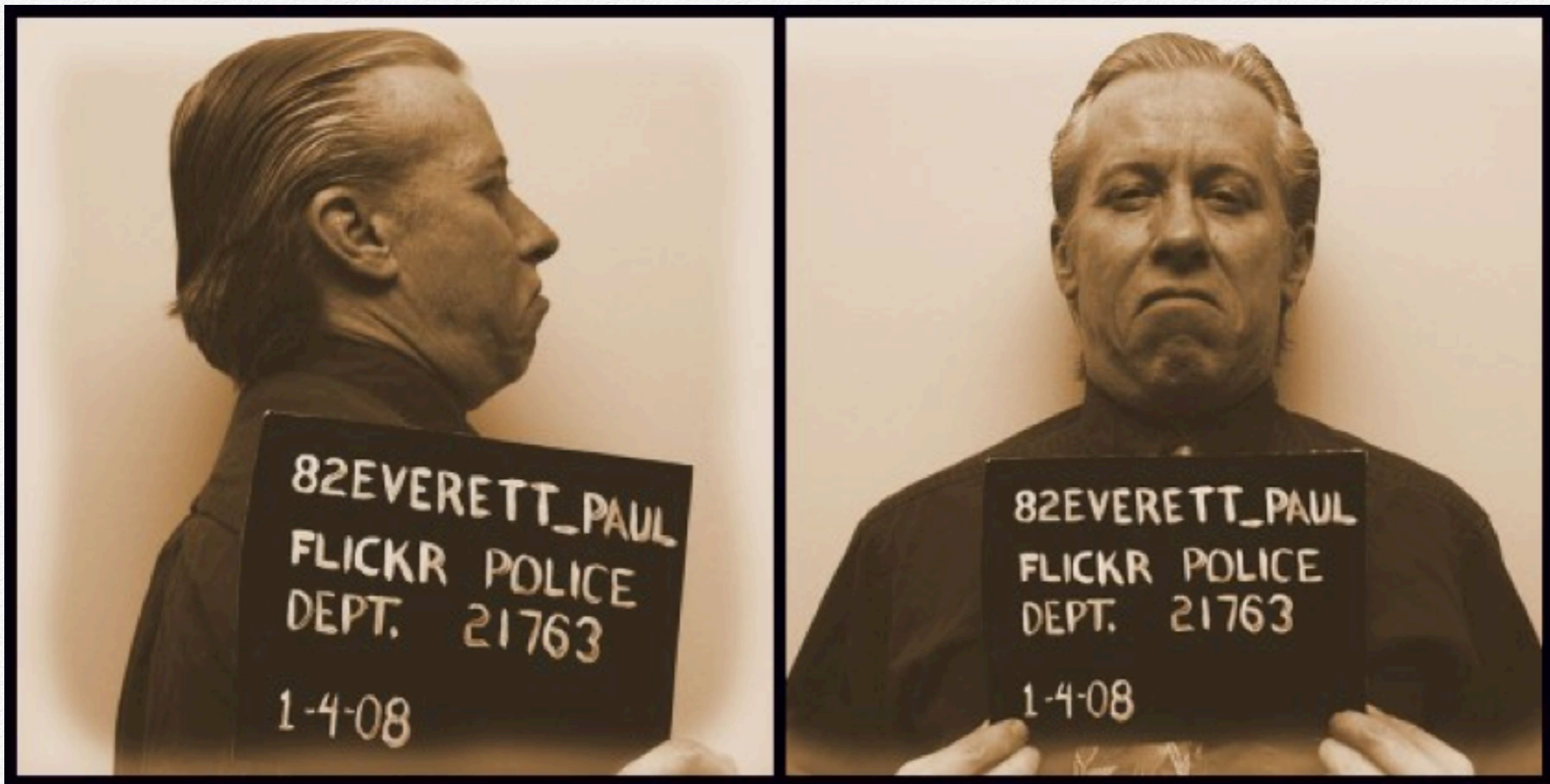
Rich Godwin, Stephan Kinsella, and GrugQ for their input on the book.

Dan Kaminsky, Dorit Ron, Adi Shamir, Fergal Reid, and Martin Harrigan for their security research into the anonymity of Bitcoin.

Satoshi, and the countless programmers, evangelists, and entrepreneurs for giving Bitcoin to the world and growing its value.

An Offer You Can't Refuse

A crime mob moves into your neighborhood and starts shaking down individuals and businesses for “protection services”. They are delighted to discover that some members of the neighborhood – including you – own a difficult-to-trace form of electronic cash called “Bitcoin”. What do you do?



82EVERETT_PAUL
FLICKR POLICE
DEPT. 21763
1-4-08

82EVERETT_PAUL
FLICKR POLICE
DEPT. 21763
1-4-08

The Appointment

A bead of sweat rolls down your forehead as you grasp the door handle, pausing on the threshold of the office of Giovanni Collections Center. After ten long minutes spent in a waiting area, alternating between folding your hands together in your lap and adjusting your collar, you're invited to a back area of the building, to a dark room with two chairs and a small table in the center. A man in an expensive-looking suit pulls out a chair and gestures toward it. "Have a seat", he says coldly, drawing out his A's with an apparent North Jersey drawl. You ease into the seat and glance around the room, and then toward the man. He slides his own chair out and removes his suit jacket, resting it on the back of the chair. A jolt of adrenaline surges through your system as you notice that the jacket was concealing a holstered revolver strapped around the man's chest. He rolls up his sleeves to reveal a series of crude-looking tattoos running up his forearms, depicting snakes, crucifixes, and Italian names written in script after the word "R.I.P."

Shit.

"Thanks for coming down to meet us", says the man across the table, now seated. Behind him, the steel door to the meeting room is locked, separating the two of you from the rest of the "Collections Center".

As if I had a choice.... You draw a thin, strained smile across your face, nodding in response.

Looking directly into your eyes, the man continues, "We have a little problem. We've noticed that your collection payments have been declining over the last year."

"Yes... yes. I know. Business has been slow this last year", you reply cautiously. A lump forms in your throat.

"I hear that from a lot of folks. Times have been tough for everyone. But collections are *very* important. Don't get us wrong: We're not trying to squeeze the little guy. We want to make sure that he earns his fair share and stays safe. We're here to help. We provide *protection*."

"Safety is important in this crazy world, wouldn't you agree?" he asks, his elbows resting on the table with hands cupped.

"Yes,... of course", you respond slowly.

The man grins broadly. "The Giovanni Corporation is dedicated to preserving the safety of all of our neighbors in this fine city", he continues, imitating the voice of a public

What is Bitcoin?



What is Bitcoin?

Where does it come from?

How does it work?

Bitcoin Basics

This chapter is intended to explain a few basic things about Bitcoin to newcomers. If you are already familiar with the fundamentals of Bitcoin, you can skip this chapter and move ahead to chapter three.

The goal of this chapter is to explain the basic elements of Bitcoin *required to understand anonymous ownership*. It is not intended to be a comprehensive explanation of the many facets of the Bitcoin technology and community. For a general introduction to Bitcoin, check out [We Use Coins](#). For a thorough explanation of how Bitcoin works and the many services that have spawned around the Bitcoin community, check out the Bitcoin Wiki. In general, the [Bitcoin Wiki](#) is an excellent resource for understanding the fundamentals of Bitcoin, and this book occasionally links to pages within this wiki so that you can explore particular Bitcoin topics further, if you wish. For ongoing news and analysis of Bitcoin and other crypto-currencies, subscribe to the [Let's Talk Bitcoin](#) podcast.

What Is Bitcoin?

Bitcoin is an electronic currency. Because people value Bitcoin, it can be purchased with other currencies, purchased for the purpose of investment or speculation, and exchanged for goods and services. The exact value of Bitcoin is often expressed in terms of other world currencies – smugly referred to by many Bitcoin users as “legacy currencies” – such as the US dollar, the euro, the Japanese yen, and so on. These exchange values are tracked by online marketplaces (“Bitcoin exchanges”) where people can exchange Bitcoin for other currencies. Because of economic factors that are unique to each exchange, such as fees and banking partners, exchanges usually have distinct exchange rates from one another. These rates change constantly based on the buying and selling decisions of Bitcoin traders. Because of the diversity of prices, the best way to determine a fair and global Bitcoin price is to average between multiple exchange prices. [BitcoinAverage](#) does an excellent job of determining a weighted global average that excludes unprofessional exchanges. In the same way that US dollars are abbreviated “USD” and euros are abbreviated “EUR”, Bitcoin has its own abbreviation – “BTC”. Many websites publish historical prices and charts. I recommend [Bitcoin Charts](#). I discuss online exchanges in more depth in chapter five. They are only one of several possible methods for buying and selling bitcoins.

Anonymous Bitcoin Ownership



How do identity and anonymity pertain to the ownership of bitcoin?
What are the terms used to describe anonymity as it relates to Bitcoin?

Understanding Anonymity

Definitions And Concepts

In order to understand how anonymity applies to Bitcoin, we have to understand a few basic concepts about anonymity. Anonymity is misrepresented in popular culture, because it is commonly represented as an *absolute*, when in fact it is a *measurement* or *quantity*. The question at any given time is not, “Am I anonymous?” but rather, “How anonymous am I, and to whom?”

What Is Anonymity?

Consider the following scenario: Peter is a private investigator who has been hired to solve a murder mystery. At the beginning of his investigation, he starts off with a list he has compiled of every person on the planet. He doesn't know where the murder has taken place, and he doesn't know much about when. If his list is 7 billion persons long, then the chance that any one person on the list is the murderer is, from Peter's perspective, 1 in 7

billion. Thus, the murderer is not absolutely anonymous, but hidden from Peter among 6,999,999,999 other people.

To talk about anonymity clearly, it's helpful to develop a few terms to describe these scenarios:

- Let's call the murder the “**action**” that Peter is trying to de-anonymize.
- Let's call the murderer the “**actor**”, whom Peter is trying to reveal.
- Let's call Peter the “**investigator**”, who is trying to de-anonymize the **action** in question.

Note that the term “**investigator**” is morally agnostic. An **investigator** could as easily be a criminal as he could be a person who solves crimes.

Peter illustrates the following principle about anonymity:

- The goal of achieving anonymity is to hide your identity among as many other people as possible, or to make it as unlikely as possible that someone could single you out as the **actor** associated with a particular **action**.

Now, suppose Peter never bothers to progress the case, and learns nothing more about it. The grieving family grows quickly dissatisfied, and they fire Peter and hire another private investigator, Ingrid.

Ingrid starts off with the same list of 7 billion people that Peter has. At that point in time, the murderer is still as

Anonymous Bitcoin

What Does Anonymous Ownership Of Bitcoin Mean?

Now that we understand some basic things about Bitcoin and what anonymity means in the abstract, we're ready to talk about what anonymity means to Bitcoin. Recall that when we previously discussed scenarios related to anonymity, we said that **actors** who perform **actions** wish to remain anonymous from **investigators**, and **investigators** try to reveal the identity of those **actors**. In these terms, bitcoin ownership can be explained as follows:

- The **action** is the ownership of a particular Bitcoin address.
- The **actor** is the owner of that Bitcoin address.
- The **investigator** is someone who wants to reveal the owner of a particular Bitcoin address.

Why Own Bitcoin Anonymously?

Ease of use is an ongoing challenge for Bitcoin; methods for acquiring bitcoins, keeping them safe, and selling them remain awkward for many. Trying to do all of these things while maintaining anonymity complicates the process further, so it's worth asking: Why bother? There are a number of reasons why someone might want to control a Bitcoin address anonymously, including:

- **The purchase of embarrassing products or services.** A young woman might not wish for her parents to know that she purchased birth control; a CEO may want to delay shareholders from knowing about a risky medical procedure that he is undergoing.
- **The purchase of temporarily secret products or services.** This might be a surprise engagement ring, or consultation with a divorce lawyer.
- **The purchase of illegal products or services.** This can include so-called "vice" items like drugs, but it can also include things that are considered perfectly legal in most tax jurisdictions, but are illegal in a particular one due to local cultural bigotries. Well-known examples include the [criminalization of sex toy sales in Alabama](#), a [ban on chewing gum in Singapore](#), and bans on sales of locally unapproved medicines and medical treatments.
- **The threat of someone stealing your bitcoins.** If someone knows that you own bitcoins, they can threaten you physically and demand some or all of your bitcoins, such as in the mob scenario from chapter one.

Challenges to Bitcoin Anonymity

By what methods can
bitcoin owners' identity be
uncovered?

4

A Timeline of Bitcoin Ownership

This Chapter

In chapter four, I'll explain some of the core concepts necessary to understand what makes anonymous use of Bitcoin difficult. If you're already persuaded that you want to use the techniques in this book and don't care to understand the details of why you should, you can skip ahead to chapter five. If you're still skeptical that such techniques are necessary, or if you wish to learn about the core concepts in order to become a more independent anonymous user of Bitcoin, read on.

Three Phases Of Risk

The period of time during which a person owns bitcoin can be broken down into three phases that are convenient for understanding how ownership can be de-anonymized. We'll discuss phases one and three first, and phase two last, for reasons that will become clear later.

The First Risk, Phase One: Acquiring Bitcoins

In the first phase, the owner takes possession of a bitcoin. This can happen when someone generates a new bitcoin through the mining process, or when someone receives bitcoins from another Bitcoin address.

Bitcoin Mining And Anonymity

Some people regard mining as the most anonymous way to acquire bitcoins because there is no transaction history associated with newly mined bitcoins. However, with deeper understanding of ownership anonymity, we can see the following potential issues:

- In an initial network process, the Bitcoin network associates a newly mined bitcoin with the address of the person who mined it. The network messages associated with this process may be subject to de-anonymization attacks by determined adversaries; an **investigator** with insight into the topology of the Bitcoin peer-to-peer network may be able to determine some information about the originator of the messages.
- Increasingly, mining requires specialized hardware. Long gone are the days of casual users firing up mining software on their home computers and mining bitcoins in the background, because the market competition has driven up the level of complexity of the mathematical challenges that need to be solved in order to mine. If

The Blockchain

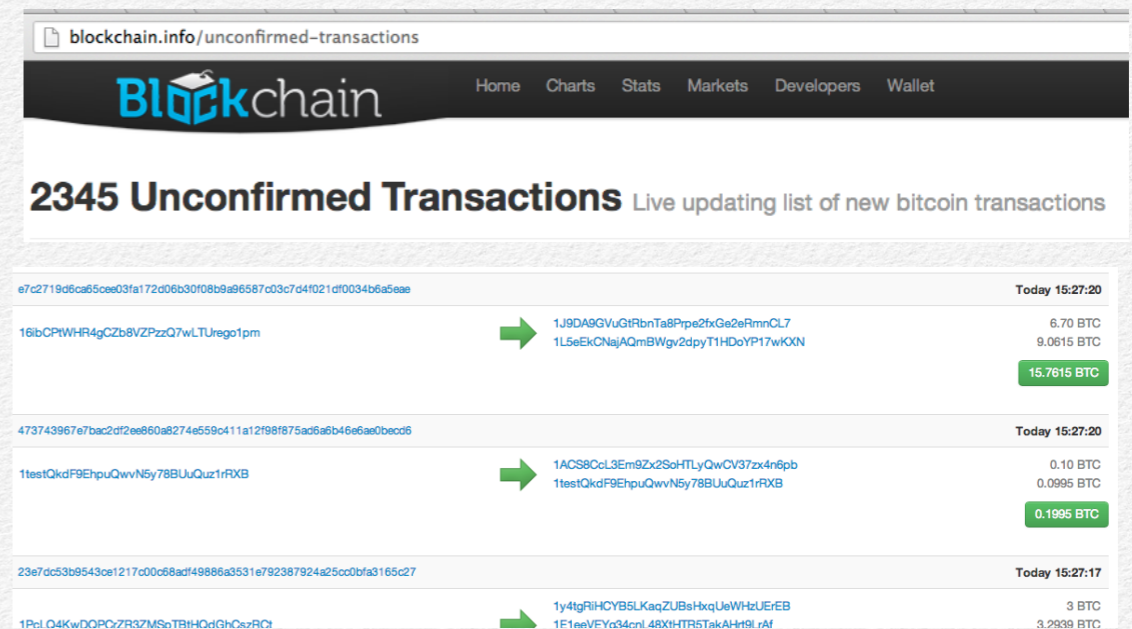
Tools For Viewing The Blockchain

In chapter two, we introduced the concept of the Blockchain, which is a public record of all Bitcoin transactions that take place.

In order to understand how the Blockchain works, it's helpful to refer to a couple websites that publish information from the Blockchain and make the transaction data more clear to human readers. The two websites are blockchain.info and blockexplorer.com. In the future, these particular websites may disappear from the Internet, but as long as the Bitcoin network exists, you can expect that there will be similar tools to help you see what's going on in the Blockchain.

How Transactions Are Recorded To The Blockchain

When someone sends bitcoins, Bitcoin software distributes a message throughout the network, letting other people know about the transaction. However, this step by itself does not commit the transaction to the Blockchain. At first, these transactions exist in a pool of “[unconfirmed transactions](#)”. The first website, blockchain.info, tells us how many such unconfirmed transactions there are currently in existence, and provides a list of them:



By design, bitcoin miners are the only agents in the Bitcoin network who can record things to the Blockchain. When they discover new bitcoins through mining and let the network know by sending a mining discovery message,

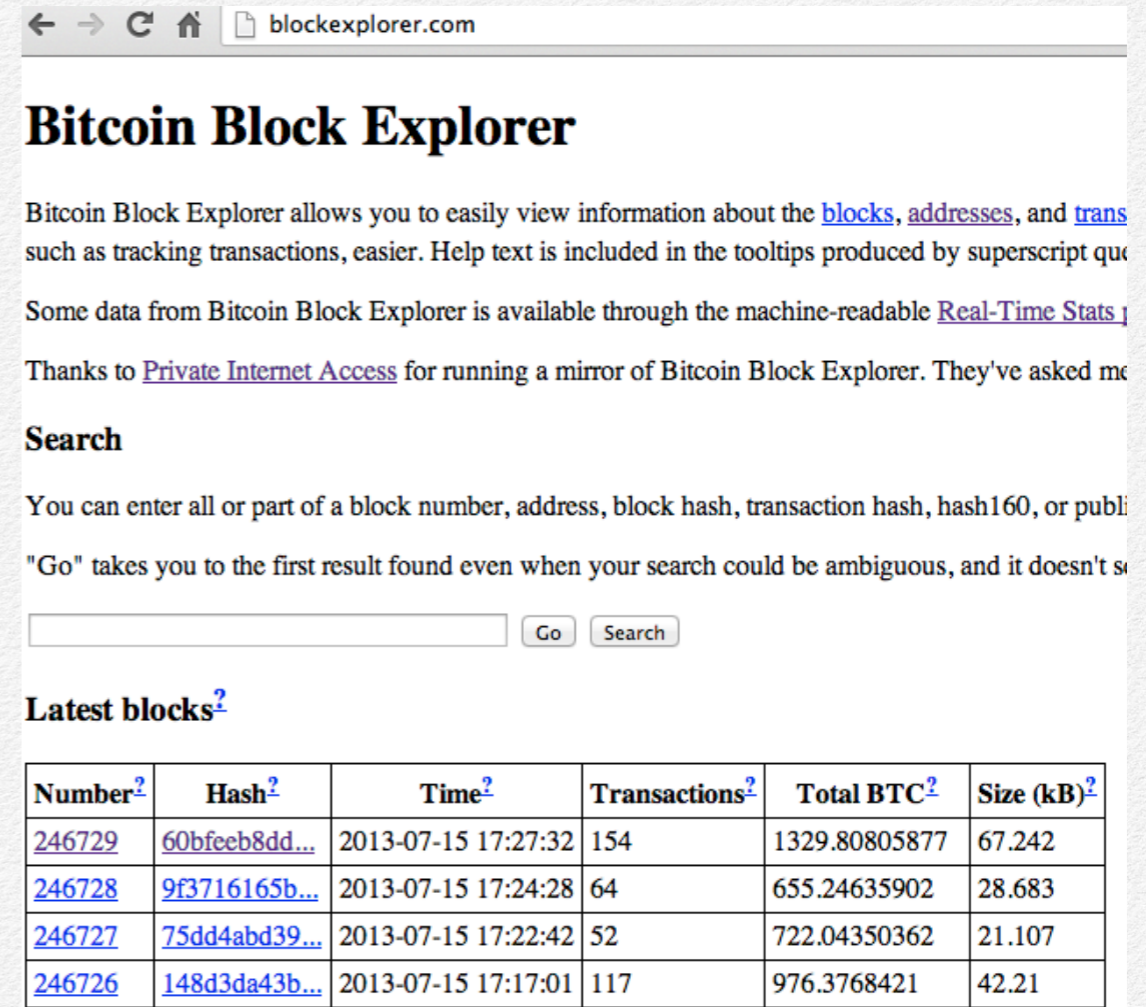
they also have the opportunity to choose transactions from the pool of unconfirmed transactions and include those along with their discovery message. Frequently, a person trying to send bitcoins to another address will offer up a bounty called a “miner fee”; this consists of a small number of bitcoins that will be given away to any miner who is willing to commit the sender’s transaction to the Blockchain. This is the process by which transactions go from sitting in an unconfirmed pool, to being confirmed and written to the Blockchain.

BITCOIN JARGON

The Blockchain consists of a list of “blocks” that is added to over time. When a bitcoin miner discovers a new bitcoin, she will create a new block to notify the network about the bitcoin, and to provide her Bitcoin address, to which the new bitcoin will be assigned. She can also add a record of other users’ unconfirmed transactions to the block. This is how Bitcoin transactions are added to the Blockchain.

Each time a new mining discovery message is committed to the Blockchain by a miner, this is recorded as a “block” on the Blockchain.

The second website, Blockexplorer.com, gives a sequential list of these blocks, with the most recent at the top:



The screenshot shows the Bitcoin Block Explorer website. At the top, there is a search bar with a "Go" button and a "Search" button. Below the search bar, there is a section titled "Latest blocks²" which contains a table with the following data:

Number ²	Hash ²	Time ²	Transactions ²	Total BTC ²	Size (kB) ²
246729	60bfeeb8dd...	2013-07-15 17:27:32	154	1329.80805877	67.242
246728	9f3716165b...	2013-07-15 17:24:28	64	655.24635902	28.683
246727	75dd4abd39...	2013-07-15 17:22:42	52	722.04350362	21.107
246726	148d3da43b...	2013-07-15 17:17:01	117	976.3768421	42.21

If you click on an individual block, the site will give you more details, including a list of all of the transactions that the miner included from the unconfirmed transaction pool.

which addresses are used repeatedly at the same times on different days to potentially discover Bitcoin users owning multiple addresses. This is based on the observation that a Bitcoin user might habitually use several different addresses in a single, short period of time.

Most importantly, the authors pointed out that the behaviors of Bitcoin users and clients often leak information about their ownership. This can happen in the following ways:

- If a person has a wallet containing multiple Bitcoin addresses, and she sends more bitcoins than is contained in any one of the addresses, the client will make the transaction possible by pooling together bitcoins from multiple addresses, and thus reveal their common ownership on the Blockchain. (See Figure 1 below.)
- If a person sends some, but not all, of the balance of a Bitcoin address, the left-over “change” will either be sent back to the same address, or the client will create a new “change address” in which to deposit it. In the latter case, this will reveal common ownership of the original address and the change address. (See Figure 2 below.)
- Bitcoin users by habit, and services by design, tend to move bitcoins in bursts. A rapid succession of transactions through a series of addresses often indicates that a bitcoin owner is acting alone, whereas long pauses between transactions may indicate the participation of multiple bitcoin owners. Analysis of the

Blockchain based on the timestamps attached to transactions is referred to as “temporal analysis”.

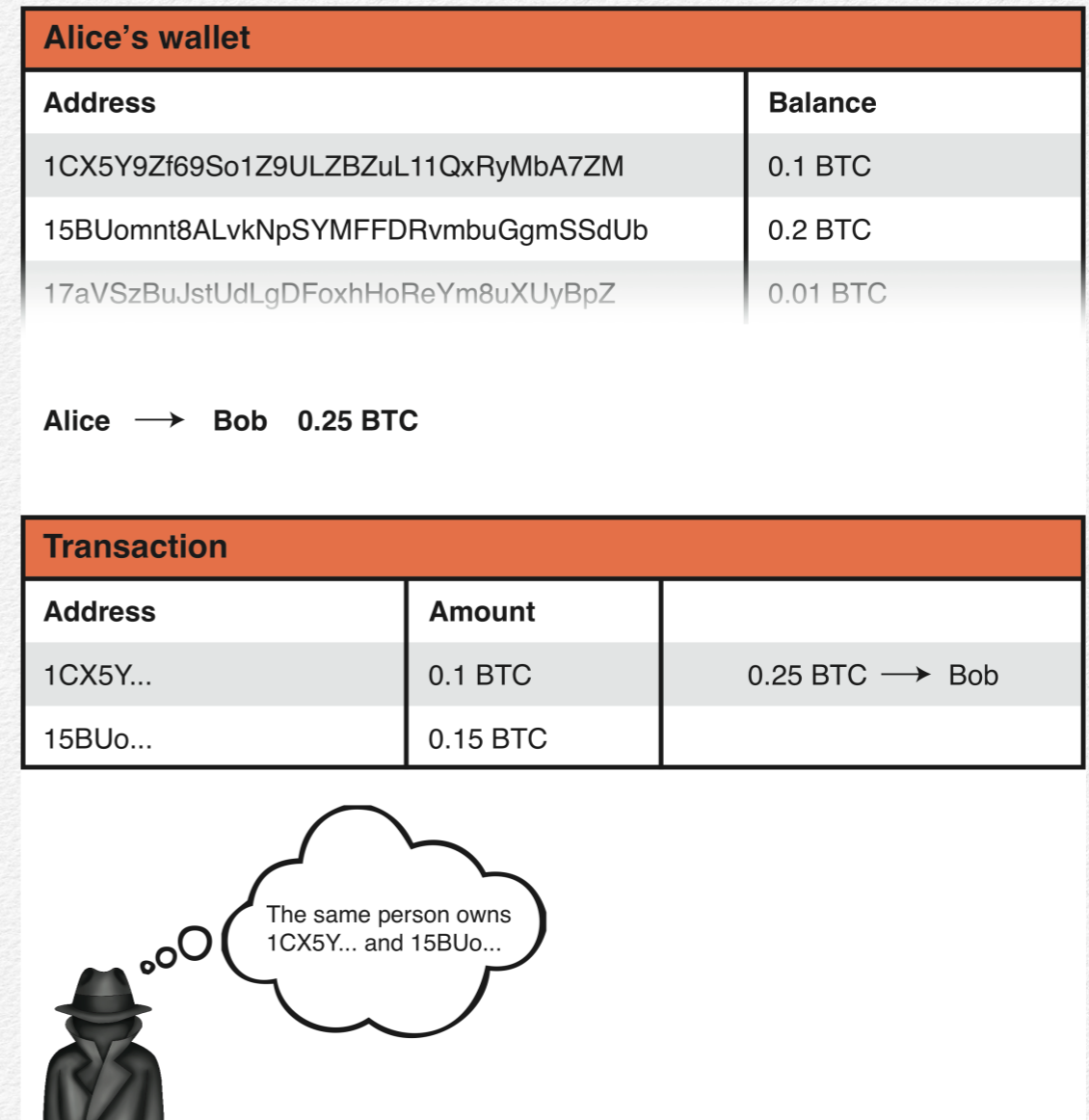


FIGURE 1: ALICE'S FUNDS ARE POOLED FROM MULTIPLE ADDRESSES IN HER BITCOIN WALLET.

The Worst-Case Investigator

Considering Current Capabilities

In the first chapter, we described a scenario in which a criminal organization demands all or a portion of bitcoin owners' digital wealth. In this scenario, the thugs probably wouldn't be the ones working to de-anonymize bitcoin owners, but they would instead hire other amoral actors who have the right skills.

In chapter three, we introduced the principle that methods to anonymize your bitcoin ownership should consider the capabilities of the person or organization that would be most effective at de-anonymizing your Bitcoin addresses. In order to defend against this worst-case **investigator**, we need to understand his capabilities.

The passage of time is important. The Blockchain records transactions forever, and an **investigator** may have interest in transactions from a year ago, five years ago, or ten years ago. The passage of time does not grant safety. It's also trivial work for **investigators** to collect additional,

de-anonymizing information now and store it indefinitely. We can guarantee that **investigators** will get better over time, while the methods that bitcoin owners use to anonymize their ownership are frozen in time when recorded in the Blockchain.

We cannot anticipate the capabilities of **investigators** in the future, but we can consider what's possible today and defend against those capabilities, as long as we keep in mind the inherent risk in assuming that what is impossible in the present will remain unchanged in the future.

Alexei, A.k.a. “молния”

Alexei is a fictional computer hacker hired by the mob to de-anonymize bitcoin owners so that the mob can extort the owners. He became interested in computers at a young age. Originally he planned to attend a local Russian university and acquire a computer science degree, but before he turned eighteen, he observed that he had already taught himself much of what would be included in the curriculum, and he could audit classes through MIT for free on the web. While he originally dreamed of working for Google one day, he discovered that he could make more money operating in the black market.

Today, Alexei mostly pays the bills by selling access to his botnets. He purchases malware components from the black market, making custom modifications, redistributing the malware to the Internet, and attempting to infect as

laptop or smartphone, and exchange it only for cash in person. However, the vast majority of Bitcoin users interact with websites to obtain bitcoins, to store them, to send and receive them, and to sell them.

Whenever a web browser interacts with a website, it transmits a large amount of information to that website's web server. Most of this is unseen by the user, since the HTTP protocol under which websites operate is uninteresting to most web users. However, because such a rich amount of data is transmitted from web users to websites, this information can potentially be used to identify users, linking multiple visits to the same website and single visits to various websites. The identifying information sent from a web browser to a website is referred to as the browser's fingerprint.

The Electronic Frontier Foundation has created a useful tool for understanding just how unique browser fingerprints tend to be. [Panopticlick](#) will gather information about your browser, just as any website is capable of doing, and tell you how unique your browser fingerprint is, compared to the many browsers who have visited the Panopticlick site. The browser configuration that you use when being profiled can make a world of difference. For instance, when JavaScript is disabled, Panopticlick will examine basic information about the version of the browser you are using. With JavaScript enabled, Panopticlick will also gather information about the following characteristics of your browser:

- Browser plug-ins installed and their respective versions

- Your time zone
- Your screen resolution and color settings
- Fonts installed on your computer
- And many other settings.

When visiting Panopticlick in Firefox on my Mac with JavaScript disabled, I found that I shared a browser fingerprint with 33,527 other visitors:

When visiting again with JavaScript enabled, my browser fingerprint was unique among all three million plus visitors:

Panopticlick
How Unique — and Trackable — Is Your Browser?

Within our dataset of several million visitors, only **one in 33,527 browsers** have the same fingerprint as yours.

Currently, we estimate that your browser has a fingerprint that conveys **15.03 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size: [Email](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#)

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	11.52	2945.4	Mozilla/5.0 (Macintosh; Intel Mac OS X
HTTP_ACCEPT Headers	6.03	65.23	text/html,
Browser Plugin Details	1.75	3.36	no javascript
Time Zone	1.74	3.35	no javascript
Screen Size and Color Depth	1.74	3.35	no javascript
System Fonts	1.75	3.35	no javascript
Are Cookies Enabled?	0.44	1.35	Yes
Limited supercookie test	1.74	3.35	no javascript

Buying Anonymously

5

What are the best methods for purchasing bitcoins anonymously?

How do we use popular services to achieve this goal?

Anonymity as Frosting

Introduction

Imagine that someone asks you to bring a cake with chocolate frosting to a party. At the grocery store, you find that you have the option of buying a pre-made vanilla cake and chocolate icing that you can add on top, or buying all of the ingredients for a chocolate cake and baking it from scratch. Which would be easier?

In this section, I'll explain the simplest approach to owning bitcoins anonymously. Rather than focusing on anonymity immediately, you'll purchase your bitcoins legitimately through online or in-person exchanges, with no expectations of anonymity – your vanilla cake. You'll then use Bitcoin mixers to scatter the trail between your non-anonymous Bitcoin address and your final, anonymous one; This will be the chocolate frosting layer on top. This section will explain why this approach is appealing, and address some important considerations related to this approach.

In the second section of this chapter, “Immediate Anonymity”, I'll discuss some approaches with which it's possible to be more anonymous immediately after purchase.

In the remaining sections, I'll walk you through how to set up your computer for anonymous bitcoin ownership, how to purchase bitcoins when you're new to purchasing, and how to use a Bitcoin mixing service to make bitcoins anonymous – or as anonymous as they can be, anyway.

Buying From The White Market

In chapter four, I pointed out some of the ways that bitcoin purchasing differs between online and in-person exchanges.

On one hand, interacting with online exchange services inherently leaves a footprint on the web. Increasingly, online exchanges are also required by financial regulators to collect personal information about their customers in order to comply with know-your-customer (KYC) rules.

On the other hand, people who sell bitcoin through in-person exchanges like [LocalBitcoins.com](https://localbitcoins.com) and btcnearme.com are not necessarily subject to these KYC rules. However, beware: even though various governments have intimated that person-to-person exchanges of bitcoin are free from financial regulation, there have been [vague legal warnings](#) lobbed at

Selecting Software for Your Anonymous Bitcoin Toolkit

The Toolkit

We'll need a few elemental software tools in order to hold bitcoins anonymously. Some of these tools are software that we'll copy to USB drives or DVDs, and others are websites we'll use with a specific web browser. These tools include:

- An *operating system* on which to run software. This should be a secure system that resists attacks from **investigators**.
- A *web browser* for visiting Bitcoin-related websites.
- A *privacy network* through which we can connect to the Internet while hiding our identities.
- A *Bitcoin client* for sending and receiving bitcoins.
- A *Bitcoin mixer*, to obfuscate the flow of our bitcoins from one address to the next.

- *Encryption software* for securely storing our bitcoins and account information.

How To Choose Software For Your Toolkit

While it's incredibly useful to have a list of software that helps anonymize bitcoins, that list is only useful until the existing tools become obsolete. To help you choose your own tools in the future, I'll explain the motivations behind my recommendations.

Selecting an Operating System

An operating system should be secure and leak as little information about you to the Internet as possible when you go online. For this reason, we will use the Tails Linux operating system. Linux is an open source family of operating systems, which means that people from around the world can inspect its source code to find intentional or unintentional vulnerabilities that could be exploited by attackers. Minimizing vulnerabilities is important when it comes to using Bitcoin anonymously. Operating systems with substantial vulnerabilities are gold mines for **investigators**, who can exploit those vulnerabilities in order to extract information about you – including serial numbers specific to your computer hardware, information about your physical address or ISP customer information, and Bitcoin addresses that you own.

Tails Linux is run in a **live disk** configuration, meaning that, rather than installing the operating system on the hard

Alice



Bob



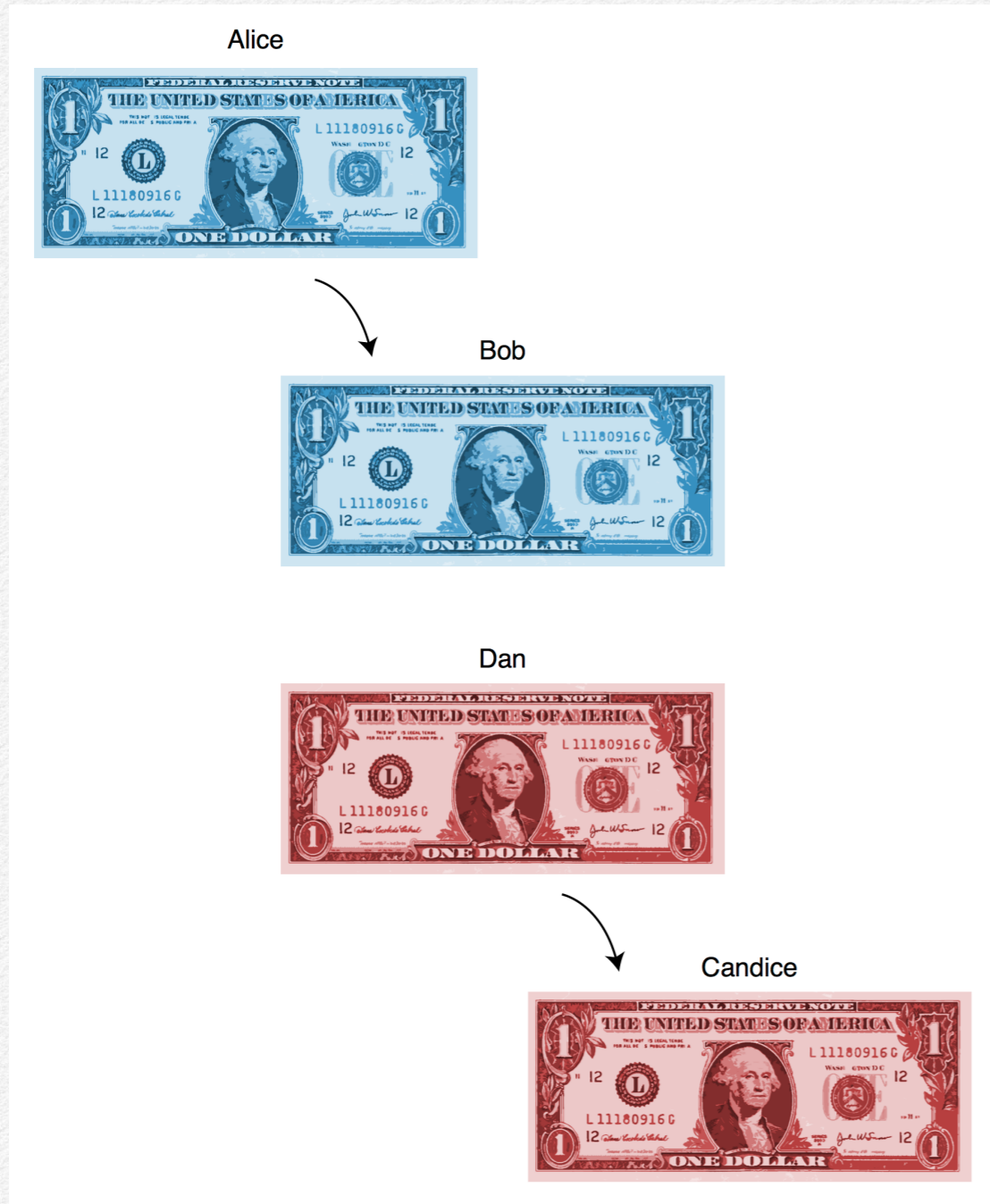
Candice



The record of transactions would look like this:

- Alice hands a \$1 bill to Bob.
- Bob hands 25¢ to Candice.
- Bob hands another 25¢ to Candice.
- Bob hands another 25¢ to Candice.
- Bob hands a final 25¢ to Candice.

Then consider the following scenario. Rather than simply redirecting money to Candice, Bob could replace the money received from Alice with an equivalent amount not associated with him. If Bob asks Daniel to share fund ownership with him, then the transactions might look like this:



The record of transactions in this case would be:

- Alice hands a \$1 bill to Bob.
- Dan hands a \$1 bill to Candice.

The causal chain in this second ledger is not so clear. Note that Bob and Daniel are essentially simulating a \$1 transfer between them, but this transfer takes place outside of the public ledger and thus the information is not readily available.

A smart observer might notice that the amounts passed from Alice to Bob and from Daniel to Candice, respectively, are equivalent, and he could use this information to build a statistical probability that Bob and Daniel are colluding. To prevent someone from inferring this, the mixing agreement between Bob and Daniel should be more sophisticated, introducing randomness in the values that they pass between them. At the very least, there should be some uniformity to hide behind. Two \$1 transactions could be easily linked together, but the relationships between a thousand \$1 transactions taking place roughly at the same time would be more difficult to follow. In reality, there are a variety of attacks that an **investigator** could use to link Bob and Daniel together, and Bob and Daniel must perform competent mixing in order to thwart these attacks.

Selecting Encryption Software

Encrypting our Bitcoin-related files serves two purposes: to keep those files secret, and to keep them safe from Bitcoin thieves.

Two tools that we've already selected have encryption capabilities: Tails Linux has a respectable file encryption feature built in, and the Bitcoin-Qt client can encrypt Bitcoin-related files with a password. One limitation of Tails' built-in encryption is that it is specific to Linux, so it would be difficult to decrypt your Bitcoin-related files on a non-Linux operating system. Bitcoin-Qt's encryption works on any platform that runs it, but it only encrypts a portion of the wallet, while revealing other information that we want to keep secret.

TrueCrypt is a free, open source, and highly regarded file encryption software that we'll be using in this book. In addition to being thoroughly reviewed for vulnerabilities and cross-platform, TrueCrypt also allows us to create hidden partitions to help hide encrypted files, in order to protect you if your USB drives are physically confiscated by an **investigator**. With TrueCrypt, we'll encrypt the entirety of our Bitcoin wallets, instead of the partial encryption offered by Bitcoin-Qt.

Software Selection Principles

By using this software, we will have a disposable and generic operating system, a disposable and generic

identity with which to connect to the Internet, and encrypted Bitcoin files for keeping our bitcoins safe. All three of these are helpful in keeping them anonymous.

All of the tools that I have selected for this book are open source. It's more difficult for a malicious software developer to sneak a backdoor vulnerability into open source code, which other programmers review, than it is to sneak one into closed source code. I chose software that is developed by programmers who have a favorable track record of quickly and competently fixing security vulnerabilities as they are identified. I also chose software developed by people who make reasonable attempts to protect users' privacy.

As Bitcoin grows and evolves, and as new tools come along, you should strive to select your toolkit with these principles in mind.

Configuring Your Anonymous Bitcoin Toolkit

In this section, I'll explain, step-by-step, how to set up your computer for anonymous Bitcoin. Once you're set up, the walk-throughs in later sections will show you how to purchase bitcoins anonymously, and how to maintain your anonymity over time.

Equipment Required

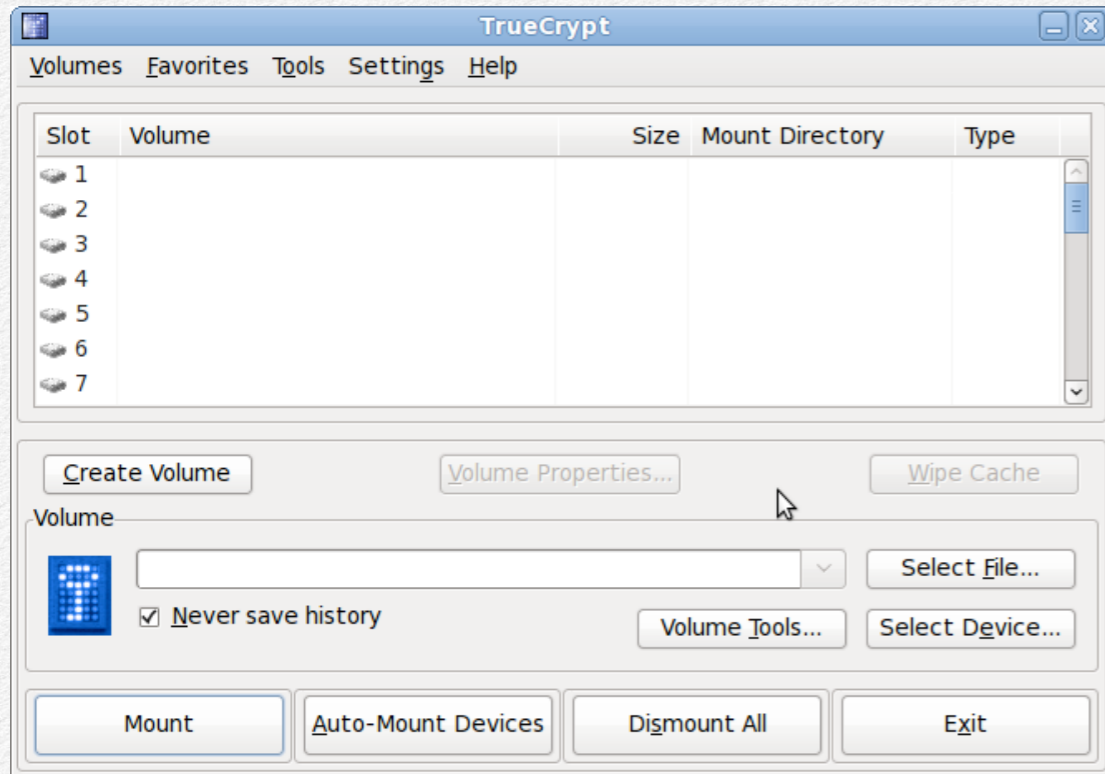
You will need the following equipment:

- A computer, running any modern Operating System (Windows, OS X, Linux, etc.), for downloading applications. We'll call this **Operating System A**.
- A computer for performing Bitcoin transactions. The computer must be capable of booting into an operating system off a USB drive, because we're going to boot Linux this way to do all of our anonymous Bitcoin work. We'll call the Linux installation **Operating System B**. If you can't boot off a USB drive, you may be able to achieve a similar effect by booting off a DVD. (Look up

“LiveCD” installations of Linux.) Check with your computer manufacturer regarding booting options for your machine. Ideally, you would have a computer dedicated only for anonymous Bitcoin usage, but this may not be affordable. If you don't have a dedicated machine, you can just run **Operating System B** on the same computer as **Operating System A**. If you would like a dedicated computer, consider purchasing a relatively inexpensive netbook, preferably a new one from the manufacturer, rather than a used one. You'll want a modern computer, but the system requirements will be low. A \$200 Asus Eee PC would work fine.

- A USB drive or a blank DVD-R with at least 2 GB of space to store Linux. Ideally, this USB drive should have a write protection switch (hardware enforced, not software enforced) to reduce the chance that it could become infected with malware after we copy Linux to it. I recommend the [Kangaru Flashblu 2 USB Flash Drive](#) (\$18).
- One or more additional USB drives on which to store your bitcoins. You can purchase 1 GB USB drives cheaply online.

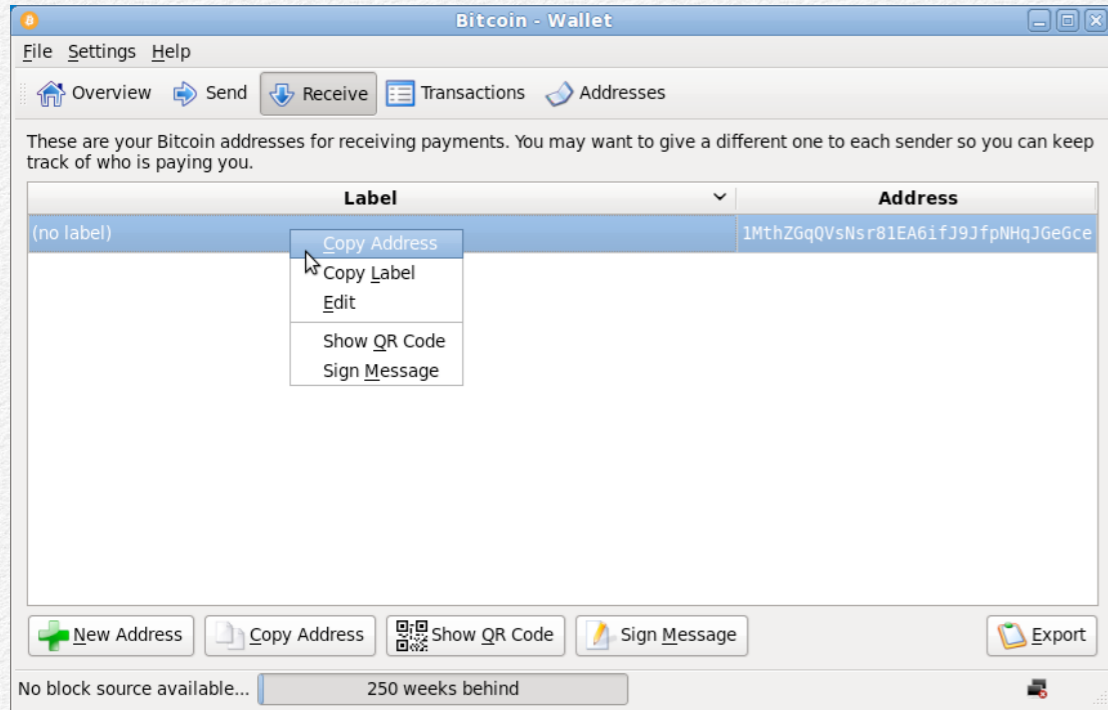
TrueCrypt in Tails Linux” to install TrueCrypt within Operating System β . You will need to follow this procedure each time you want to use TrueCrypt within this operating system.



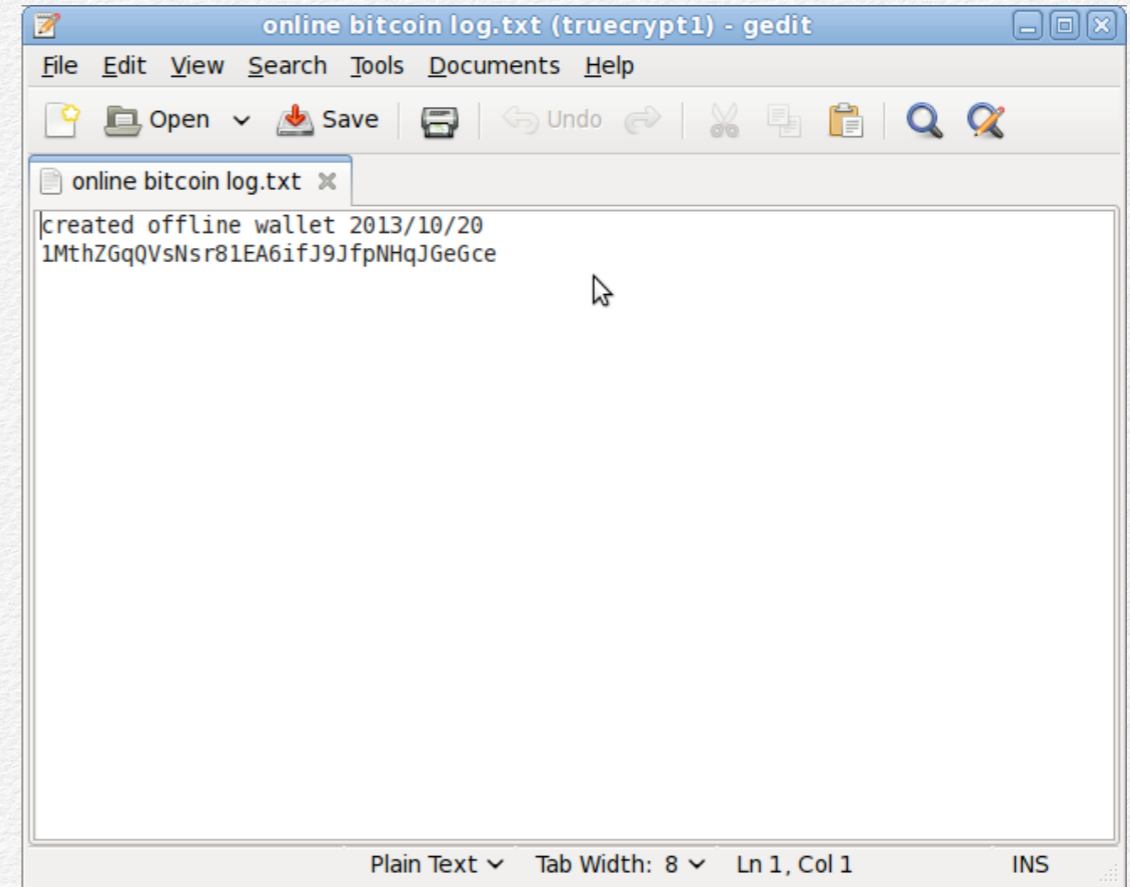
3. After you follow the instructions to install and open TrueCrypt, you'll see the TrueCrypt window as shown in the screenshot above. TrueCrypt provides a number of options, including creating a new volume, selecting an existing file to mount, mounting a selected file, and dismounting a selected volume. You will create a new volume on which to store your Bitcoin-related files. Clicking on the **Create Volume** button will open the TrueCrypt Volume Creation Wizard.



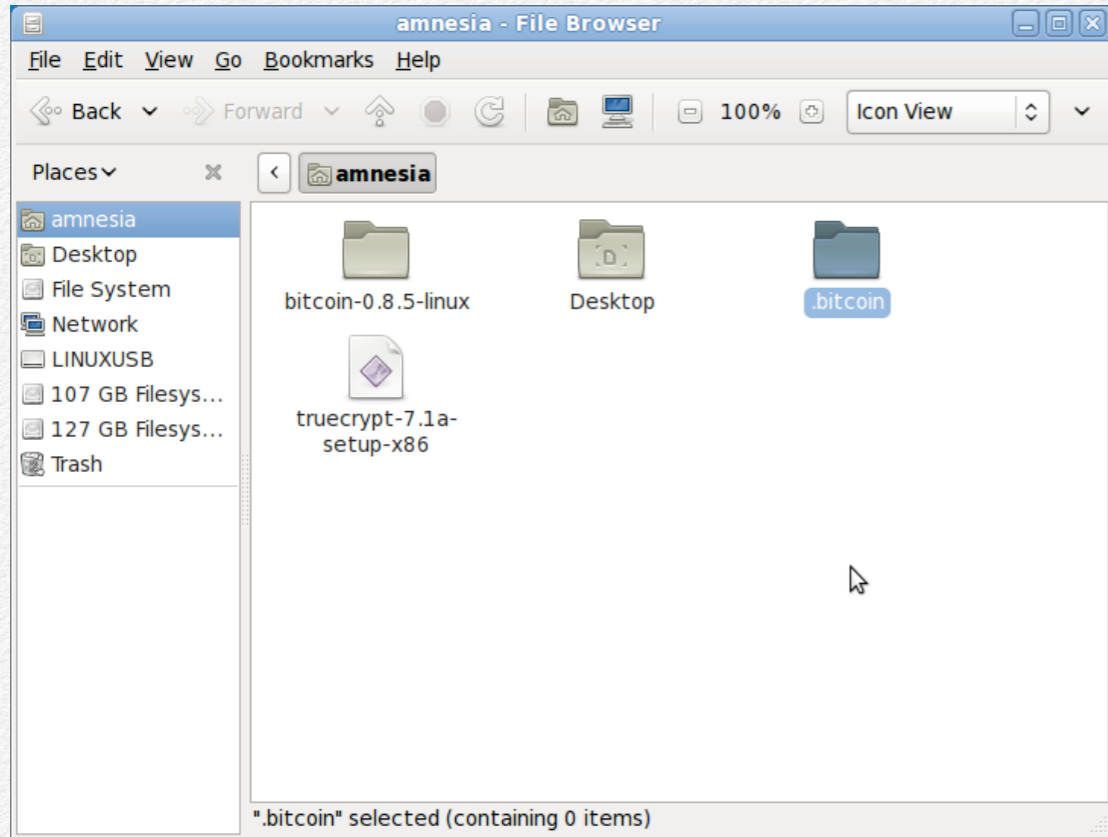
4. Within the TrueCrypt Volume Creation Wizard, select **Create an encrypted file container**, as shown above, and then click **Next**.



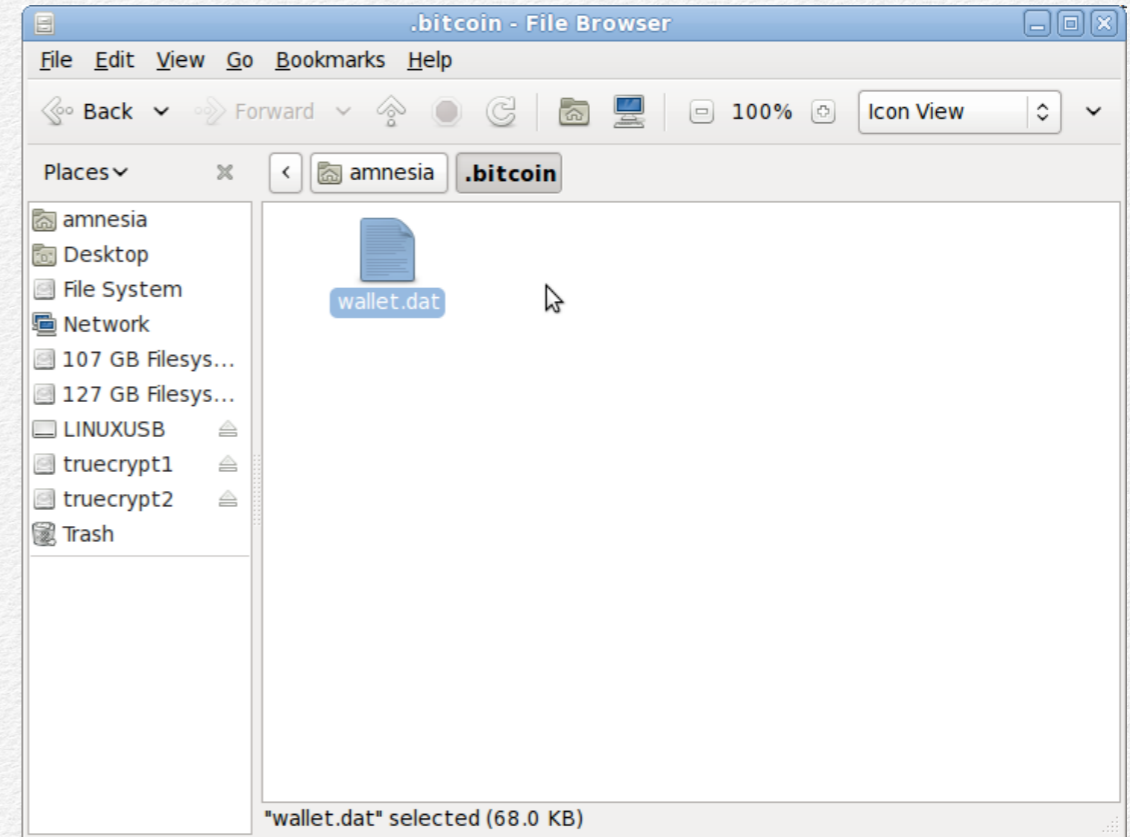
7. Return to the Bitcoin-Qt client and the **Receive** tab. Right click the address listed there, and select the **Copy Address** option.



8. Switch back to gedit and the log file that you just created, and paste the address you copied. To help you remember which addresses are which, record information here about the date when you created the address and its intended purpose.



26. Name the new folder “.bitcoin”, including the leading period.



27. Paste the wallet file into the “.bitcoin” directory. Rename the file “wallet.dat”.

White Market BTC – Coinbase Walk- Through

Choosing A Bitcoin Vendor

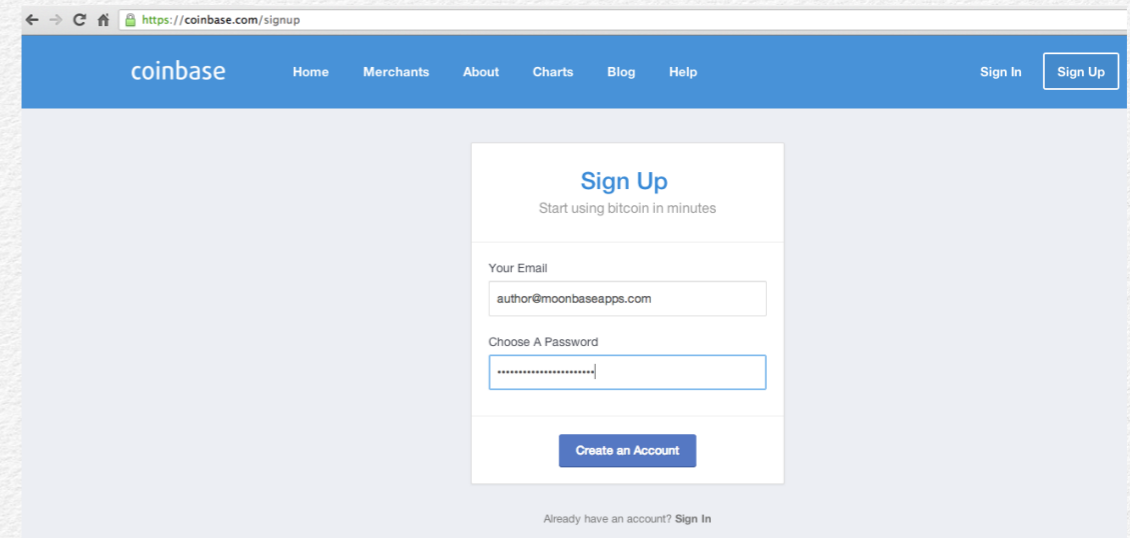
In this section, I'll cover the first step of the “anonymity as frosting” approach and explain how to purchase bitcoins at an online exchange that links your legal identity to bitcoins.

When purchasing bitcoins above the table, it doesn't matter which exchange you choose. All such exchanges collect know-your-customer information and require you to link a bank account to your exchange account. I've chosen to walk you through Coinbase because it's simple and easy to use.

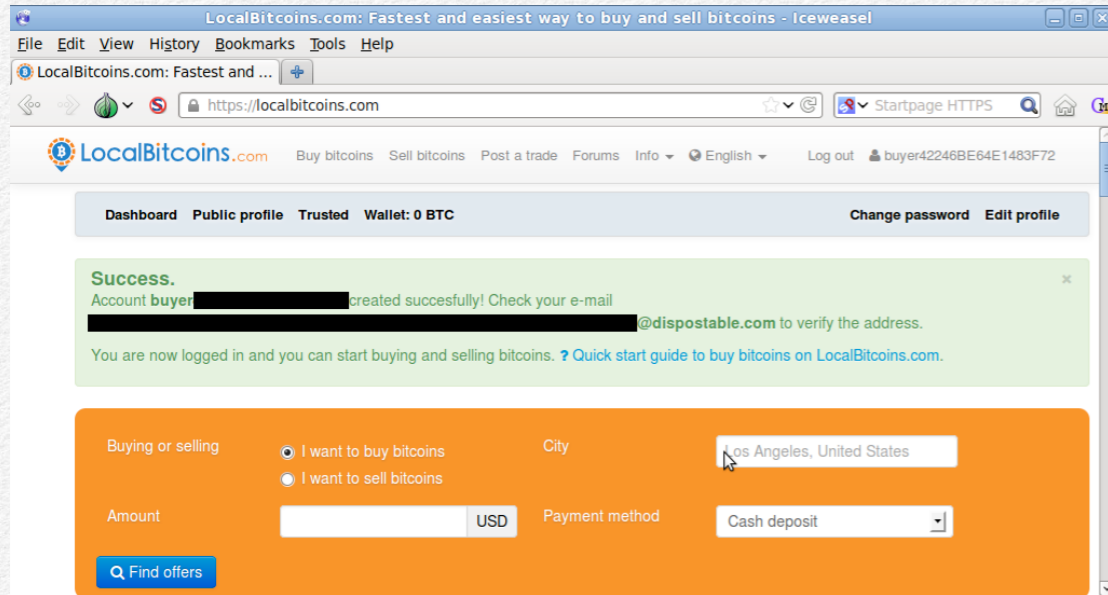
Step One: Creating A Coinbase Account

Estimated Time: 30 Minutes to set up, four banking days to receive bitcoins

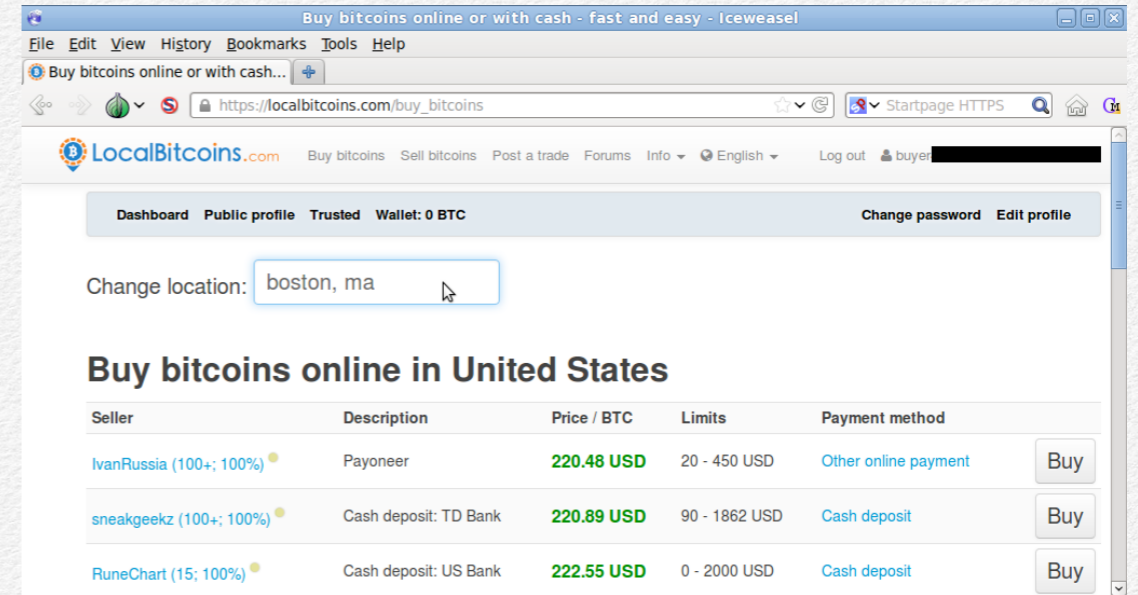
Since you're not trying to keep your bitcoins anonymous at this phase, it doesn't matter which computer you use to set up a Coinbase account; use any computer that you consider safe for regular online banking.



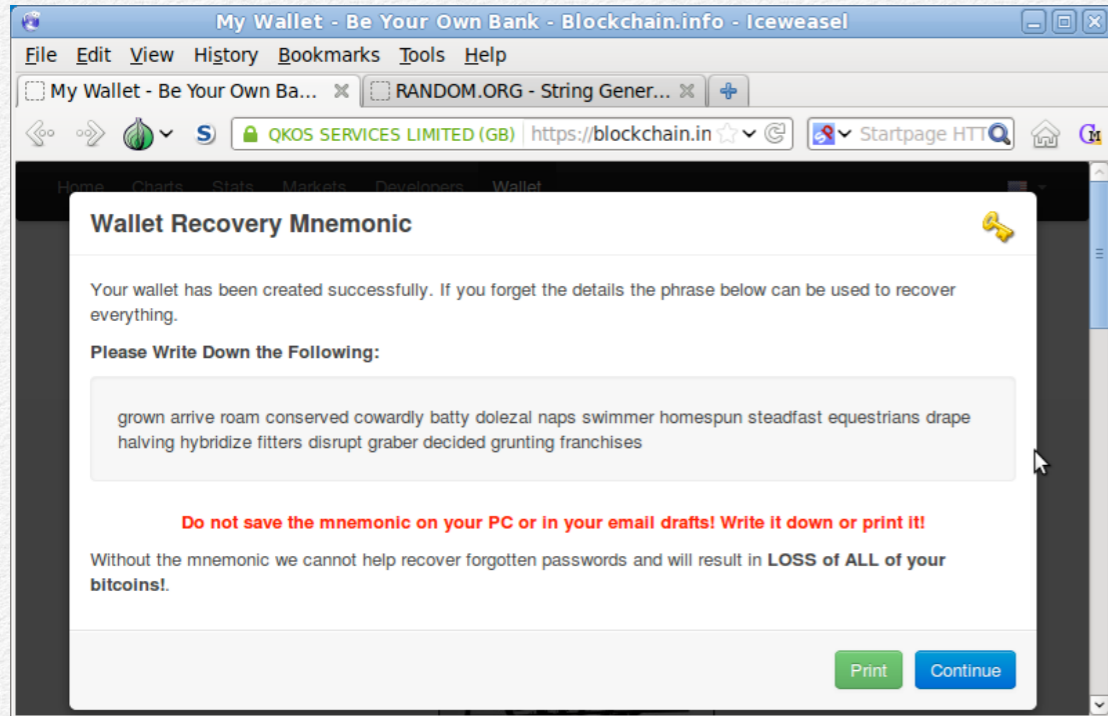
1. From **Operating System A**, visit the <https://www.coinbase.com/signup> web page. Register with an e-mail address and password.



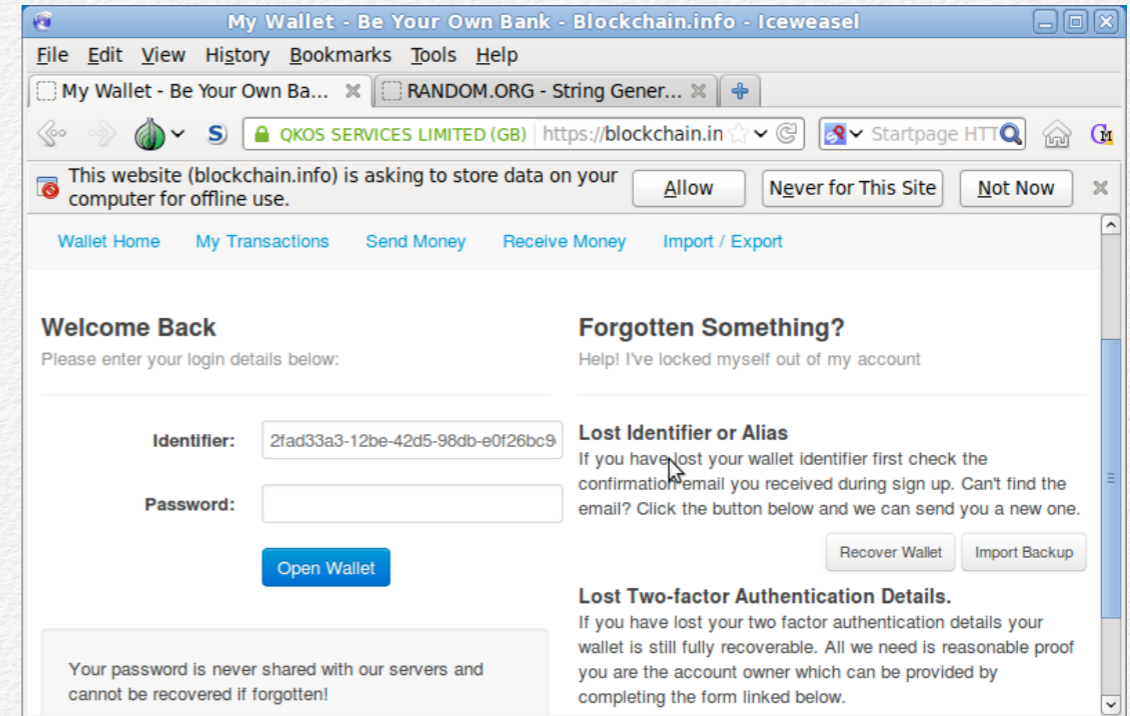
4. The site should notify you that the account was created successfully.



5. Log in using your account credentials. (**Tip:** If LocalBitcoins.com requires you to go through a “pre-login” verification process, it may ask you to solve a captcha, and then copy text from one box and paste it into another. When you paste, make sure you replace any extra spaces that pre-populate the second text box.) Click the **Buy bitcoins** link in the navigation area at the top. In the **Change location** field, type the city where you want to find sellers, and press Enter.



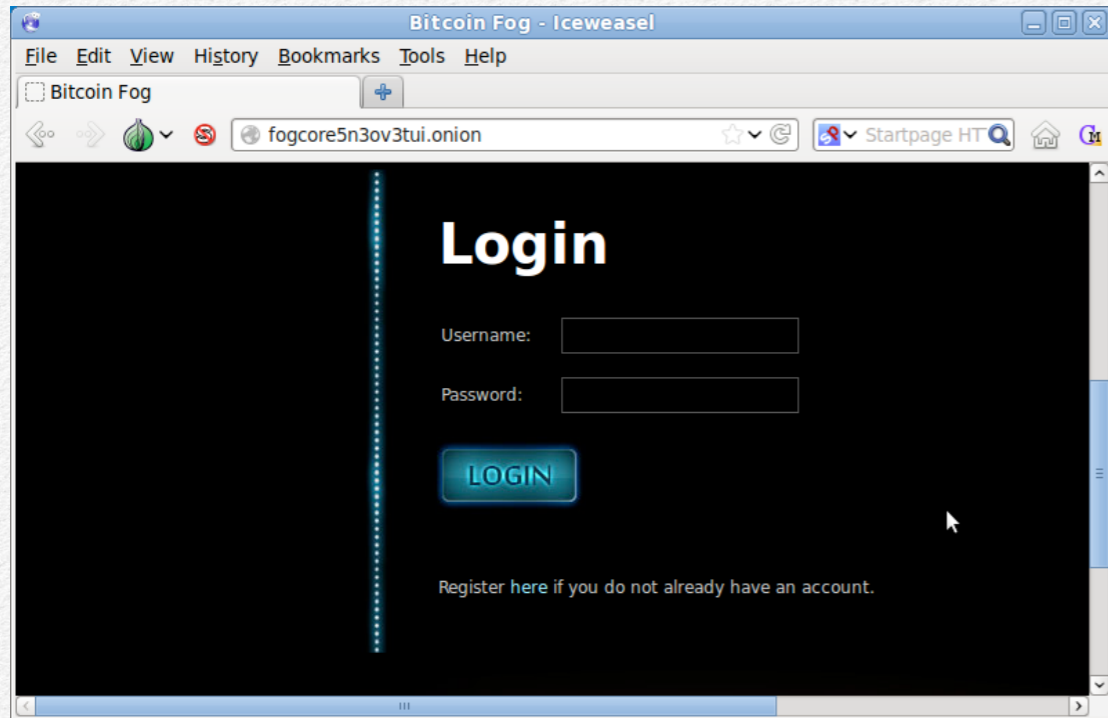
5. Blockchain.info will provide you with a password recovery mnemonic. Record this in the text file where you recorded the password. On the web page, click **Continue**.



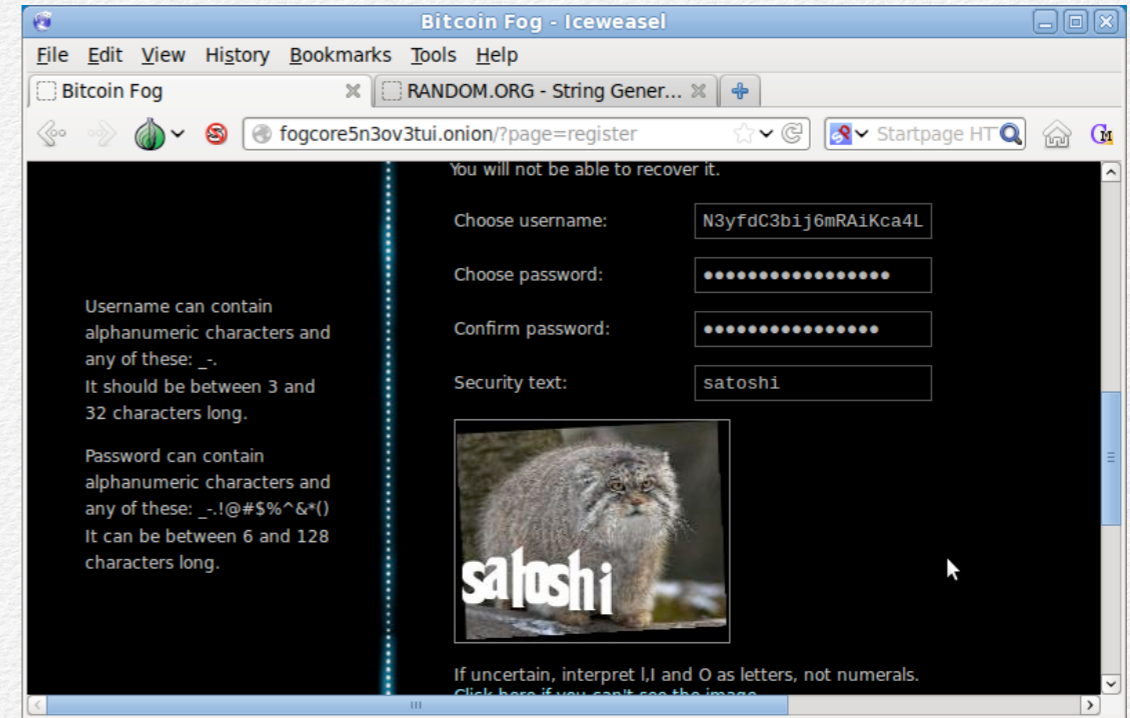
6. Blockchain.info will take you to a login page. Fill in your wallet identifier. Copy the identifier and record it in the same text file with your password and recovery mnemonic.

you just created.

<https://random.orgs/strings/>



4. Go to the Bitcoin Fog home page, and click the **Register here** link to create a new account.



5. On the registration page, enter your username, password, and captcha solution.

Maintaining Anonymity After Purchase

Once you've acquired
bitcoins, how do you
maintain their anonymity?

6

-
- From where you purchased bitcoins originally, and under what conditions you purchased them, such as the date and time.
 - Methods that you used to anonymize bitcoins, such as which mixers you used, the order of your **mixer chain**, or when you used particular mixers.
 - How many bitcoins you own anonymously, their storage addresses, or how many addresses you own.

Whenever you are working within **Operating System** **⌘** in **online mode** and have some of your Bitcoin-related files decrypted, refrain from activities that are likely to lead to malware infection, such as surfing the web, interacting with e-mail attachments, and so on. Malware might be able to access the decrypted files and de-anonymize your ownership of any addresses associated with the information stored there.

Online Identities

One of the most common ways that people lose anonymity online is through the *contamination* of online identities. For instance, if you own two Bitcoin addresses that you wish to keep dissociated from one another, but reference both of them using the same account on LocalBitcoins.com, then their separation from each other will become contaminated. Websites like LocalBitcoins.com encourage the reuse of accounts for building reputation, but in general you should create new accounts for any given service as often as you can get away with doing so, when

your chief concern is anonymity. You should abandon old accounts and not check them again, in case an **investigator** has set some manner of digital tripwire.

Without a doubt, avoid contamination by never using the same **anonymous Bitcoin session** for checking the balance of a Bitcoin address, and then logging in to your personal e-mail or Facebook accounts. To learn more about this concern, read the [“Warning”](#) by Tails Linux, and in particular, [“Tails doesn't magically separate your different contextual identities”](#).

Anonymous Bitcoin Session Discipline

In addition to creating new service accounts as frequently as possible, you should be rigorous about creating fresh **anonymous Bitcoin sessions** when supplying or accessing information about the bitcoins you own anonymously. When in doubt, follow the instructions in this book to create a fresh session. If you rely on your judgment about which actions can be done in the same session, you'll need to be correct 100% of the time. If you make a habit of creating a fresh session for each basic action, this will be more time consuming, but it will require far less stringent judgment. Actions that require a fresh **anonymous Bitcoin session** – that might take place after mixing, but before selling or spending – include, but are not limited to:

- Checking the balance of a single Bitcoin address
- Logging into any account on a single Bitcoin service

Selling and Spending Anonymously

What are the challenges associated with selling and spending bitcoins anonymously?

Which approaches fail, and which ones work well?

Important Considerations for Selling and Spending Anonymously

The Challenge

Selling bitcoins for another currency, or spending bitcoins on goods and services, is probably the most challenging phase of bitcoin ownership to perform anonymously. Unlike Bitcoin, most things of value are difficult to obtain without linking them to your identity. In this chapter, I'll explain important considerations and current best practices for exchanging your bitcoins for other items.

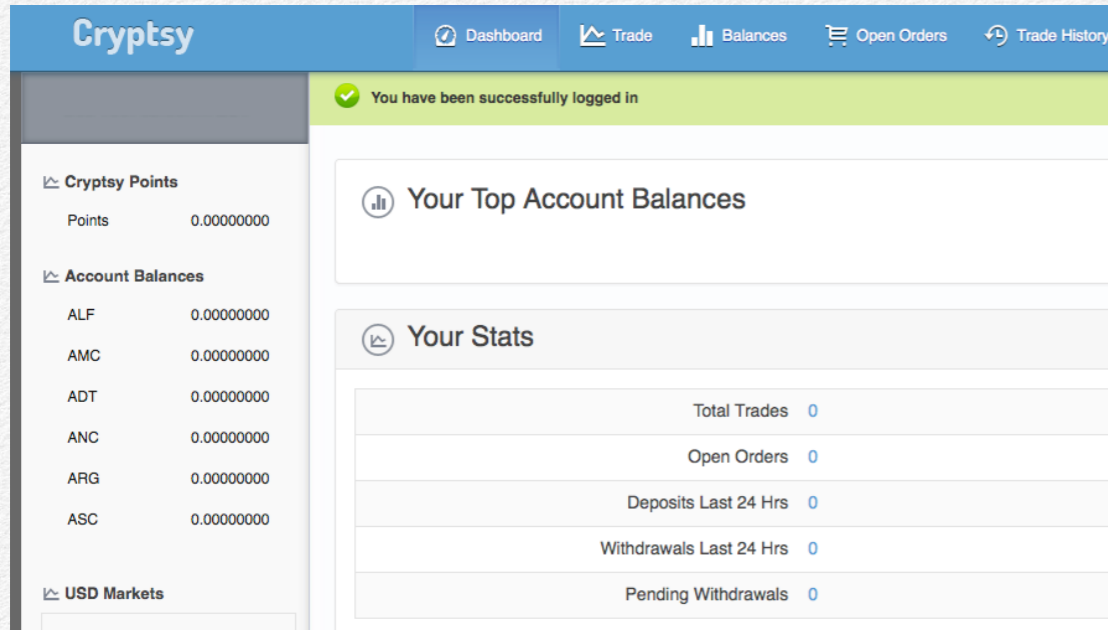
If you've made your bitcoin ownership anonymous to avoid theft, then exchanging your bitcoins for a non-anonymous item is particularly troublesome. If a local organized crime

syndicate believes that you do not own any bitcoins, but then observes that you receive something in the mail and determines that you purchased it with bitcoins, how will you justify this discrepancy? You can claim that it's an anonymous gift, but depending on how their shakedowns work, this may not be an acceptable explanation. Providing a legitimate-looking paper trail for transactions that were done anonymously remains an open problem in anonymous bitcoin ownership.

Scalability And Decentralization

Earlier in the book, I discussed the importance of the scalability of **investigation** methods for Bitcoin de-anonymization. Scalability measures how many Bitcoin users an **investigator** can de-anonymize at once, and how much will it cost her. To reduce the scalability of **investigative** methods, we want to increase the amount of work and expense for the **investigator**. We can decrease scalability by minimizing the amount of information about our Bitcoin addresses that we supply to any website or service that we use.

One way to accomplish this is by using decentralized, peer-to-peer services. Rather than selling bitcoins to a centralized exchange such as Coinbase.com, we can sell them to other people through websites like LocalBitcoins.com. Rather than purchasing a product with bitcoins directly from a vendor, we can have other people



Cryptsy supports a large range of altcoins, but it requires JavaScript – an anonymity drawback – for some pages to work, and it has a [history of significant security issues](#).



BTC-e has been around longer, but it has a [spotty record of keeping track of customer funds](#), supports fewer altcoins, and requires JavaScript for all of its pages.

To date, a crypto-currency exchange with a positive business reputation and anonymity-friendly features has not risen to compete.

Chapter 8: The Future of Bitcoin Anonymity

8

In a few short years, the Bitcoin ecosystem has grown rapidly. What's coming next to bring anonymity to digital money?

Decentralized Mixers

Introduction

In chapter five, I discussed how users must be able to trust centralized mixing services not to steal bitcoins, and not to store logs recording relationships between input and output addresses. Decentralized mixers are proposed software protocols that can potentially deal with both of these issues by making mixing a peer-to-peer process.

CoinJoin

CoinJoin is a decentralized protocol for mixing that was [proposed](#) by [Gregory Maxwell](#), a Bitcoin developer. CoinJoin helps mixed coins hide in the Blockchain by taking advantage of the way that Bitcoin transactions appear on the Blockchain. Consider the following two transactions taken at random from the Blockchain:

Transaction

Short link: <http://blockexplorer.com/8bzyS4ner5>

Hash²: c8a46766993abf04a909036ab91b50c2bfe80ffa0e8ee2578215c633f6fec6e0

Appeared in [block 272584](#) (2013-12-02 01:17:13)

Number of inputs²: 7 ([Jump to inputs](#))

Total BTC in²: 10.0003

Number of outputs²: 1 ([Jump to outputs](#))

Total BTC out²: 10

Size²: 1.083 kilobytes

Fee²: 0.0003

[Raw transaction](#)²

Inputs²

Previous output (index) ²	Amount ²	From address ²	Type ²	ScriptSig ²
439db4310d4a...0	0.73	1GCy8NYzgwNmBdBLo1w2TUgD4gf2HLpD1D	Address	304502210090e3887b20742791a168835f03092386d8f102ae685e9feb6356065fafb1
d777ba22f5a3...0	1.3	1JiMCK5W81A1rEmn6FRZ967CEhR2bVOSgd	Address	3046022100ad51a4c5ae7e3ec49d5dca26102016df73a00d60aa8e8ef7ac421f9ac5a
b4d582822906...0	0.28	1GLvJq4APsFXeSjTaAh2o4pefNN3QtZaG	Address	3046022100b532f07be684340423ee73230220dbe11ee7cf7ee38ce92cf6208e45718
22436f46c368...0	0.03	19YwF6G8964Z68agwwwv1MiauxmNRXwbTi	Address	3045022100de611fdffb706798e85b05a7033cecfac7e557cd53bb875849897978e65
7464d8783d22...0	2.8606	17x3zUeuqHhW4eEM47RHZGwucHz5noRhXv	Address	3046022100a0c009956d5bb0545da4db8802da437d3caaf77e93620d06a734e75c3378
e28526c396c8...0	1.8	1xpthfmeqnLGNDFjTAmmsHHQicqSbJP4	Address	304502207cc4494eca3e76f945e2e50fb72i03d8a98bb5dde72b013f3dd555bf69c5c6e
e7fc43fd403...0	2.9997	14kfe44GirM7vzUGRSJZf9hRSgwwvbaFe6	Address	304502210091367b89eb82243d8d44430i023e6c91b57a07ae1994926370f239cb5d1

Outputs²

Index ²	Redeemed at input ²	Amount ²	To address ²	Type ²	ScriptPubKey ²
0	Not yet redeemed	10	18GvJoEbz1csN84dCHJoswq7hJginE3dA	Address	OP_DUP OP_HASH160 4fcb9e4439d007152065273668aea39a70f OP_EQUALVERIFY OP_CHECKSIG

The above transaction involves pooling 10.0003 BTC from seven different Bitcoin addresses (inputs), and sending the combined total to one receiving address (output). This will typically occur when someone needs to send bitcoins, but they don't have enough to cover the transaction in any one of the addresses in their Bitcoin wallet; the client will automatically pool the balance of several addresses together. Based on this fact, we can easily infer that all of

Protocol-Level Mixers

Introduction

We can improve the ability of Bitcoin services and software clients to provide decentralized exchanges and mixing, but the holy grail of increased anonymity in Bitcoin involves implementing a mixing protocol within the Bitcoin protocol itself. This would mean that the moment that bitcoins are sent from one address to another, the record of transactions currently publicly documented by the Blockchain would instead be obscured. This would give Bitcoin users the option to use the currency anonymously, if they should so choose.

Side-channel attacks based on IP address tracing and other surveillance schemes could still remove this anonymity, so a protocol-level mixer would not be a panacea. That said, it would go a long way in providing a consistent, trustworthy, and simple-to-use mechanism for anonymous Bitcoin use.

Zerocoin

The most popular and realistic proposal for incorporating greater anonymity directly into Bitcoin is called [Zerocoin](#). A research project headed by computer science professor Matthew Green at John Hopkins University, Zerocoin is a proposed protocol that could be implemented within Bitcoin to provide Blockchain anonymity.

The Zerocoin protocol is somewhat complicated, but the following analogy will help explain how it would work. Imagine that you can only perform financial transactions by paying with paper bills that are marked with serial numbers. These easily tracked, numbered bills are the bitcoins in this scenario. Now imagine that someone offers you a coin that can be traded, dollar for dollar, for the paper bills. The coins are completely non-descript, and thus cannot be tracked. You can trade the coin back in return for paper bills, but you will not receive the same bills that you originally traded in. This is the kind of functionality that Zerocoin would provide, allowing people to trade trackable bitcoins for anonymous zerocoins.

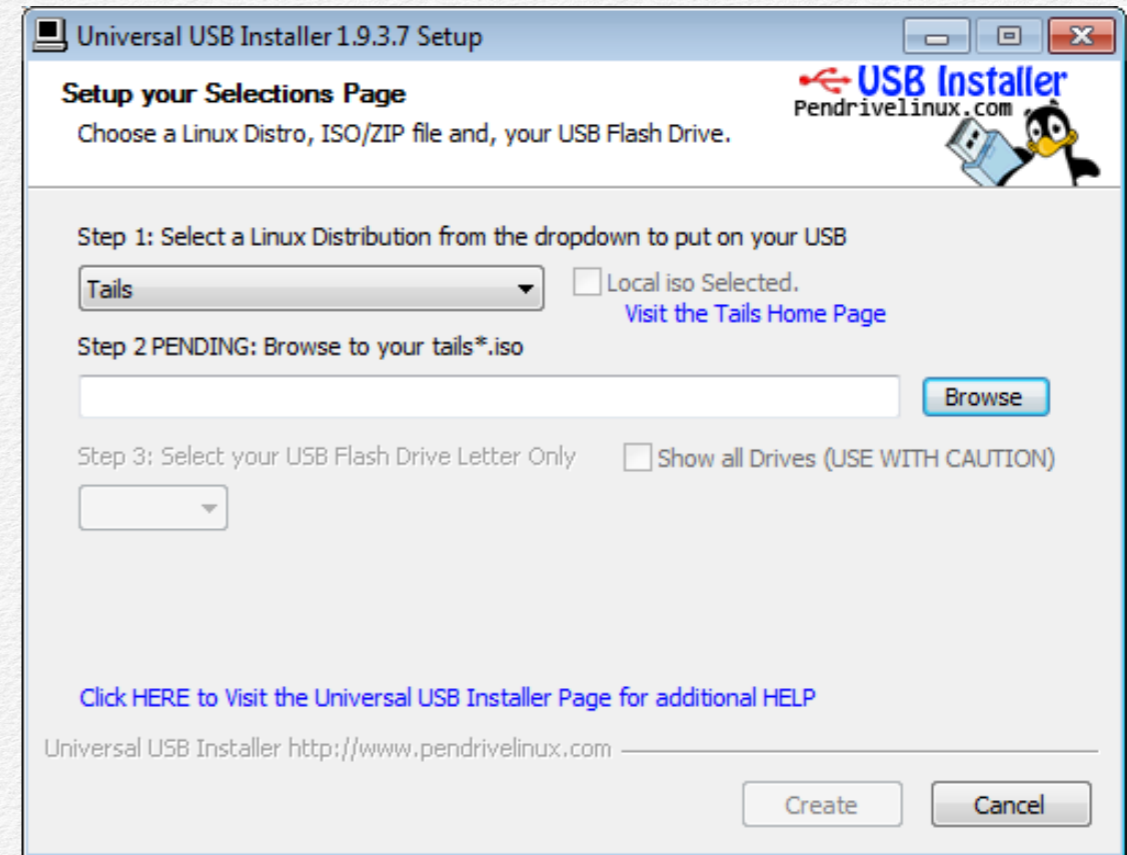
Zerocoins would exist alongside bitcoins, and would not be counted differently from the currency itself. Since there will only ever be about 21 million bitcoins in existence, Zerocoin would not add to this total, or otherwise devalue bitcoins. Most likely, this technology would exist purely in the background and be hidden from Bitcoin users entirely.

Appendices

Appendix I:	Online Services and JavaScript Requirements	152
Appendix II:	Copying Linux to a USB Drive in Windows	153
Appendix III:	Copying Linux to a USB Drive in OS X	155
Appendix IV:	Creating a Fresh Anonymous Bitcoin Session	158
Appendix V:	Opening TrueCrypt in Tails Linux	160
Appendix VI:	Opening Bitcoin-Qt in Offline Mode	165
Appendix VII:	Safely Shutting Down Tails Linux	169
Appendix VIII:	Retrieving Bitcoins from Cold Storage Using Bitcoin-Qt	170
Appendix IX:	Formatting a USB Drive in Windows 7	181
Appendix X:	Formatting a USB Drive in OS X	182

Appendix II: Copying Linux to a USB Drive in Windows

1. In your normal Windows operating system (**Operating System A**), download the latest Tails Linux ISO file from the Tails “Download” page: <https://tails.boum.org/download/index.en.html>. To make the file easy to find later, save it to your Downloads folder.
2. (Optional.) Follow the directions on the “Download” page in order to verify that the file you downloaded has not been tampered with. Follow the directions for “[Verify] using other operating systems”.
3. Download the Universal USB Installer: <http://pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/>.
4. Insert the USB drive to which you want to copy Tails Linux. If it’s a write-protected drive, disable the write protection before inserting the drive into your computer.



5. Open the Universal USB Installer executable that you downloaded, named “Universal-USB-Installer-1.9.3.7.exe”, or something similar. After agreeing to the terms and conditions, select “Tails” under the Linux Distribution drop-down menu, and browse to find the Tails Linux ISO file that you downloaded.


```
bash-3.2$ diskutil list
/dev/disk0
#:#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *200.0 GB disk0
1: EFI 209.7 MB disk0s1
2: Apple_HFS Local Drive 168.5 GB disk0s2
3: Apple_Boot Recovery HD 650.0 MB disk0s3
4: Microsoft Basic Data BOOTCAMP 30.7 GB disk0s4
bash-3.2$
```

4. Start **without** the USB drive to which you'll be copying Tails Linux plugged into your computer. Inside the Terminal window, run the command

```
diskutil list
```

in order to list the drives currently connected to your machine.

```
bash-3.2$ diskutil list
/dev/disk0
#:#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *200.0 GB disk0
1: EFI 209.7 MB disk0s1
2: Apple_HFS Local Drive 168.5 GB disk0s2
3: Apple_Boot Recovery HD 650.0 MB disk0s3
4: Microsoft Basic Data BOOTCAMP 30.7 GB disk0s4
bash-3.2$ diskutil list
/dev/disk0
#:#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *200.0 GB disk0
1: EFI 209.7 MB disk0s1
2: Apple_HFS Local Drive 168.5 GB disk0s2
3: Apple_Boot Recovery HD 650.0 MB disk0s3
4: Microsoft Basic Data BOOTCAMP 30.7 GB disk0s4
/dev/disk1
#:#: TYPE NAME SIZE IDENTIFIER
0: MYUSBDRIVE *8.1 GB disk1
bash-3.2$
```

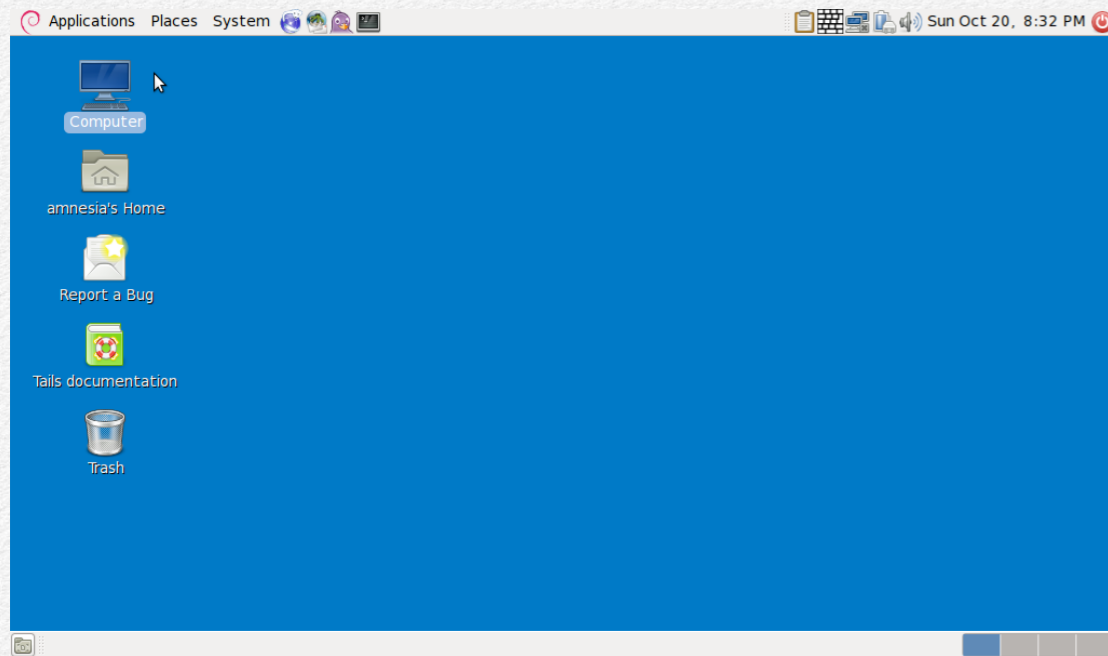
5. Next, plug in the USB drive to which you'll be copying. Run the

```
diskutil list
```

command once more. After running it the second time, you should see another drive that was not previously listed, which corresponds to the USB drive you just plugged in. Take note of the disk number corresponding to that drive. In the screenshot above, the USB drive corresponds to "/dev/disk1".

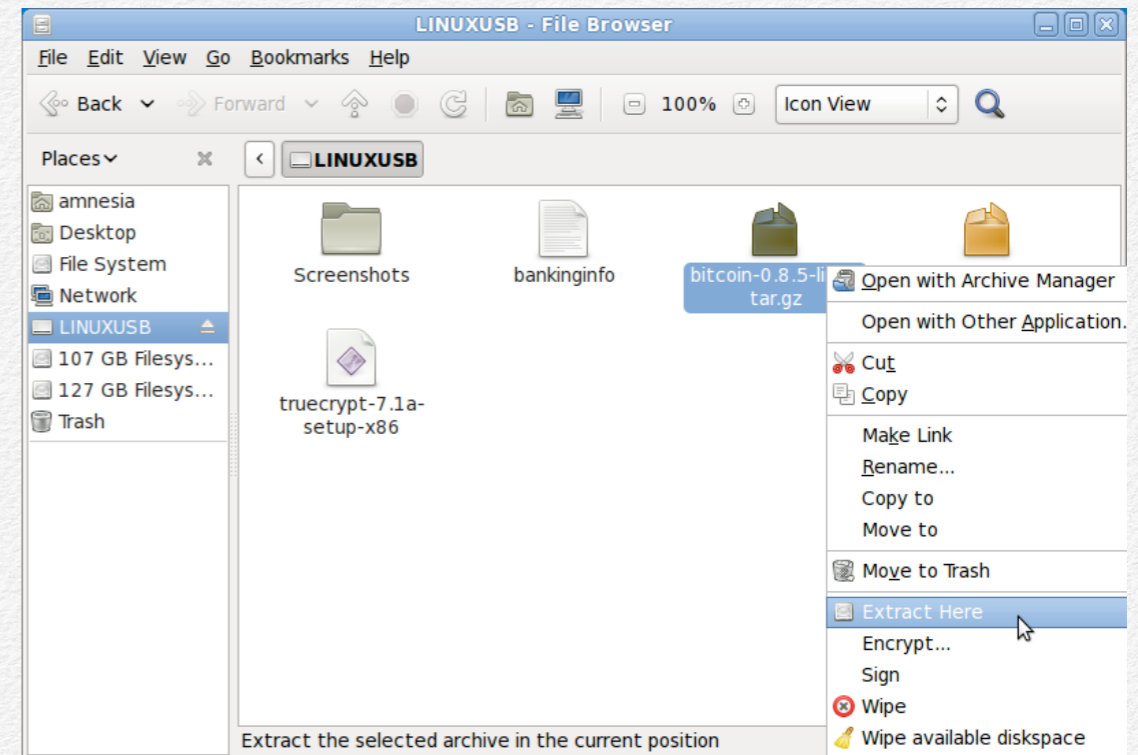
6. Download a copy of the syslinux archive from here: http://ftp.debian.org/debian/pool/main/s/syslinux/syslinux_4.02+dfsg.orig.tar.gz. Once you've downloaded it, double click it to extract the archive to a folder. Open the folder to locate the "isohybrid.pl" file

Appendix VI: Opening Bitcoin-Qt in Offline Mode

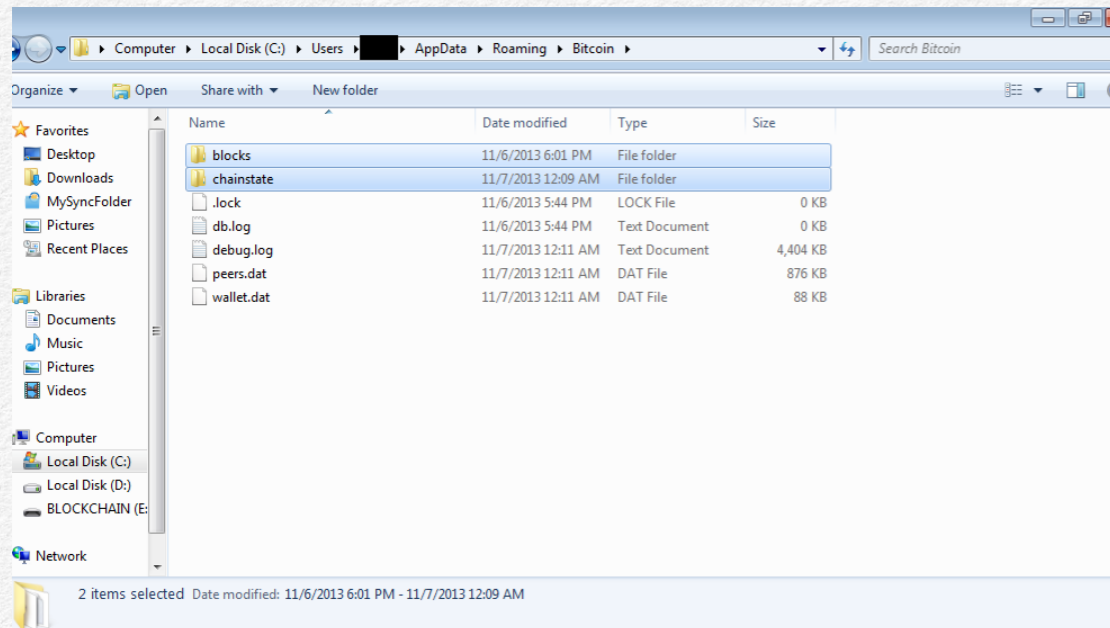


1. While in **offline mode**, double click the **Computer** icon on the Tails Linux desktop. (Note that if you have already entered **online mode** during this session, you

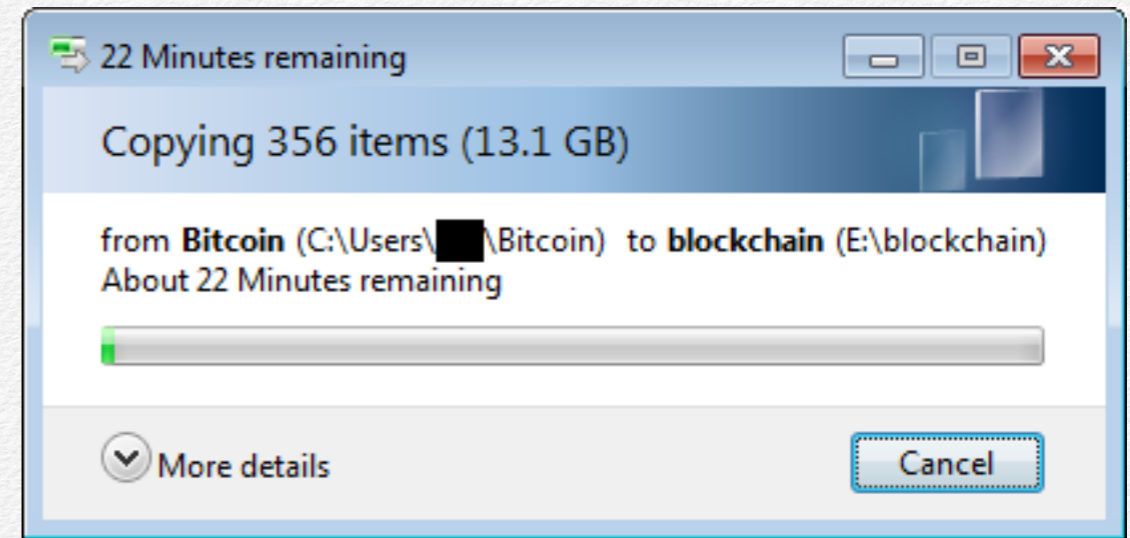
need to start a fresh anonymous Bitcoin session to return to **offline mode**.)



2. Go to your USB drive in the file explorer, and right click the Bitcoin Client file that you downloaded previously. Select the **Extract Here** option. This will extract the archived file.



9. Go to the Bitcoin-Qt data directory, and copy the “blocks” and “chainstate” directories. These two directories contain all of the Blockchain data that the Bitcoin-Qt client needs to download.

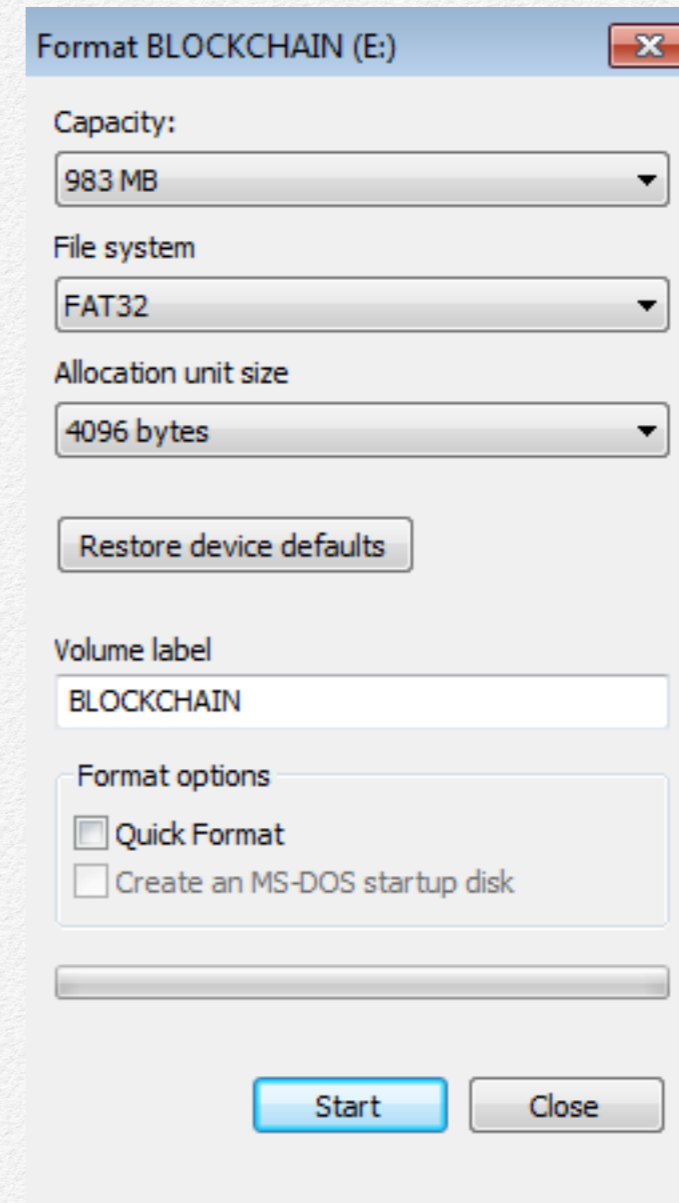


10. Create a new folder named “datadir” on your USB drive designated for copying the Blockchain, and paste the “blocks” and “chainstate” folders into it. This operation might take 30 to 60 minutes, depending upon your machine, since the Blockchain is so large.
11. Eject and unplug the USB drive to which you copied the Blockchain files.
12. Open Bitcoin-Qt again and let it synchronize with the Bitcoin network for a while longer. This will help thwart any **investigator** who tries to correlate the amount of the Blockchain that you downloaded in **Operating System A** with the amount that you will need to download when you use it again in **Operating System B**. You never have to delete the Blockchain files from **Operating System A**. This way, the next time you need to copy those files from **Operating System A**, you only need to catch it up from wherever you left off previously, rather than downloading the whole thing over again.

Appendix IX: Formatting a USB Drive in Windows 7

I recommend using FAT32 format for all of your USB drives for anonymizing bitcoins, because of its compatibility with Windows, OS X, and Linux. This appendix explains how to format a USB drive in Windows 7. The directions should only be slightly different for older or newer versions of Windows.

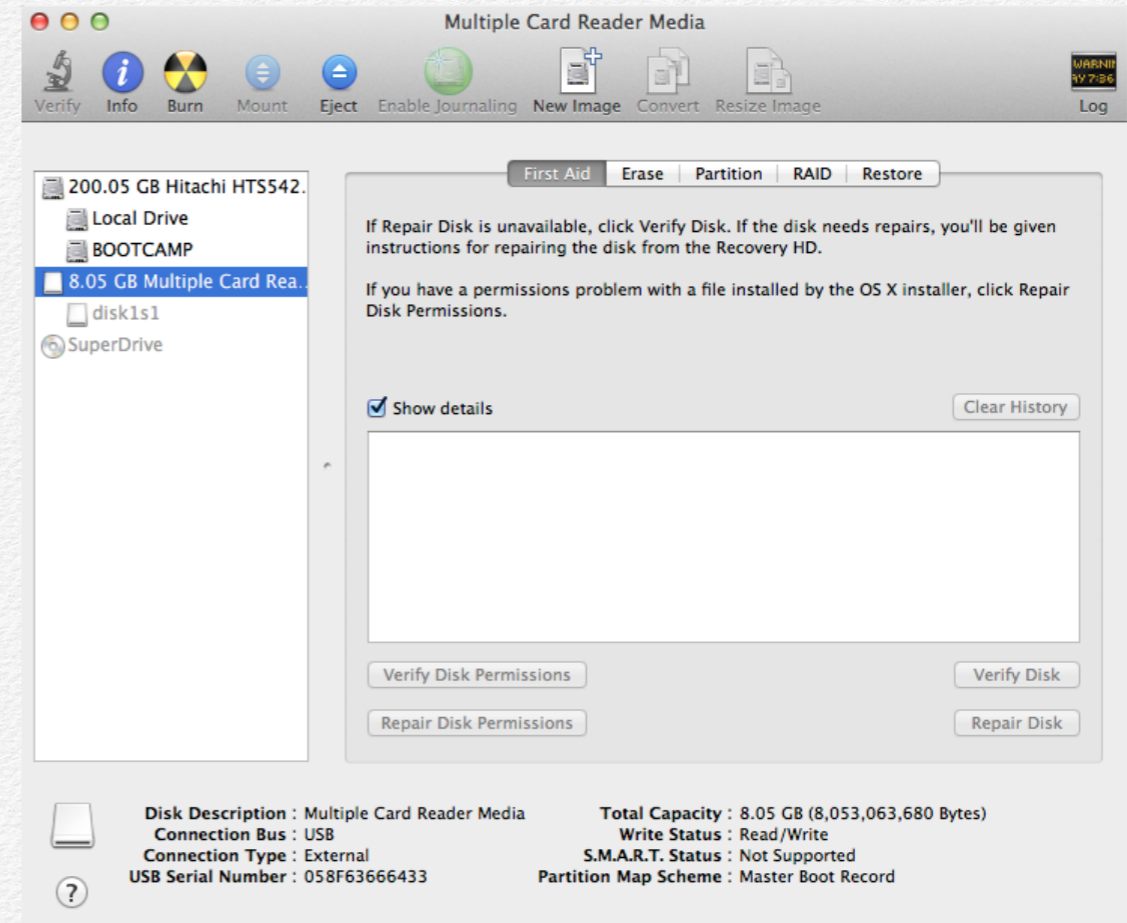
1. After inserting your USB drive into your Windows system (**Operating System A**), select **Start** → **Computer**.
2. Select the drive that represents your USB under **Devices with Removable Storage**, right click it, and select **Format**.



3. You will be presented with a Format window. In the **File system** section, select **FAT32**. In the **Format options** section toward the bottom, make sure that the **Quick Format** option is un-checked. Click the **Start** button.
4. Click **OK** on the warning pop-up. The drive will take a while to format.

Appendix X: Formatting a USB Drive in OS X

1. Insert the USB drive into your Mac running OS X.
2. Open the Disk Utility from **Applications** → **Utilities** → **Disk Utility**.



3. In Disk Utility, select your USB drive on the left-hand side of the application.

References

Images Used	185
Links	186
Citations	190

Citations

[1] “Black Ops Of TCP/IP 2011”. Dan Kaminsky, Black Hat 2011. <http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011>

[2] “Quantitative Analysis of the Full Bitcoin Transaction Graph”. Dorit Ron and Adi Shamir. January 2013. <https://www.google.com/search?q=Quantitative+Analysis+of+the+Full+Bitcoin+Transaction+Graph>

[3] “An Analysis of Anonymity in the Bitcoin System”. Fergal Reid and Martin Harrigan. May 2012. <http://arxiv.org/abs/1107.4524>

[4] “Robust De-anonymization of Large Sparse Datasets”. Arvind Narayanan and Vitaly Shmatikov. 2008. <https://www.google.com/search?q=Robust+De-anonymization+of+Large+Sparse+Datasets+Arvind+Narayanan+and+Vitaly+Shmatikov>