Should we win the fight, a new era will be born. Even if we lose, the genie is out of the bottle and they are fighting a losing War already.

—Silk Road

I'm sitting here staring at an envelope that showed up in the mail. Even though it's from a totally bizarre return address, I know exactly what's inside: a quarter gram of East Coast powder heroin. I know what's in the envelope because I ordered it from a heroin dealer on the internet using Silk Road, the infamous "anonymous marketplace."

I'm definitely not the only person who pulled an envelope with "hard" drugs out of my mailbox like it's a letter from my grandma. Ever since NPR and Gawker gave Silk Road some unwanted media attention, new users have flooded the site. But it's not just media-sweetheart drugs like LSD and pot that people are buying. That shit's easy to get unless you're underage. Silk Road is a truly *free* market. That means people are buying and selling everything from weapons to meth to smack and they're doing it fairly easily.

Hackers, anarchists, and criminals have been dreaming about these days since forever. Where you can turn on your computer, browse the web anonymously, make an untraceable cash-like transaction, and have a product in your hands, regardless of what any government or authority decides. We're at a new point in history, where complicated, highly-technical systems have become freely available and pretty easy to use. But before you can join in on the party, you gotta understand what makes all of this possible. Welcome to Tor (a network for anonymous web browsing), Bitcoin (a new cash-like digital currency with anonymous properties), and strong encryption.

Tracking Us Through The System

Tracing people through electronic networks has been embedded on the minds of all TV and movie viewers since at least the '80s:

Clever criminal: "You know you'll never find the bomb … you stupid fucking pig!"

One FBI agent to another: "Keep him on the line! *We've almost got a trace!*"

The criminal hangs up abruptly.

FBI Agent: "Damn it! We didn't get the trace!"

Since the beginning of computer "crime," hackers have gone through many elaborate steps to hide where they're connecting from. This generally meant routing your connection through so many computers that it'd be very hard and time-consuming to find where you are actually coming from. Over the years, non-criminals decided they needed a way to hide their traffic from "Big Brother" type governments, even for day-to-day internet browsing. Today, there is a pre-packaged and simple way to route our internet traffic in a fairly anonymous way: the Tor Project.

Tor, short for “the onion router,” is a network of volunteer-ran computer systems (nodes) that accept internet traffic and send it to other nodes. After going through a few nodes, your internet data gets spit out onto the internet, to its destination, by an exit node.

In order to make sure that your internet traffic is anonymous while traveling *through* the Tor network, data is encrypted in layers.

A good analogy, one that the Tor project uses, is an onion. Let’s say that I’m connecting to Facebook, and I don’t want Facebook to know where I’m connecting from. I’d load up Tor (you can find it at www.torproject.org) and connect to Facebook using the Tor browser. What happens under the hood is basically this: my internet traffic would be encrypted several times, in layers like an onion. Then my data would get sent into the Tor network. Each node that got my traffic would decrypt one layer, peeling off one layer of the onion, and send it to the next node. This would happen a few more times until all the layers of the onion were peeled and the original message was left. At that point an “exit” node would send it onto the regular internet to Facebook.

All Facebook would see is a connection coming from some random computer. Further searching might show that my connection came through the Tor network, but little else.

Don’t think this means that Tor automatically makes you totally anonymous. Internet traffic exits the Tor network the same way it goes in, so if you’re not encrypting your traffic yourself, and especially if you’re including personal information about yourself (like logging into *your* Facebook account), it would be easy to figure out that *you*connected through the Tor network. Also, if an attacker controls or monitors both the Tor entry and exit nodes, it would be possible to link your traffic to you.

If something like Silk Road was just a regular website, where you could connect to it normally through a bone-headed internet connection, it would be easy for the government (or anyone else) to track down the server, confiscate it, throw everyone involved in prison, and*throw away the key*. One Tor feature that makes locating servers difficult, making Silk Road even possible, is hidden services.

Using Tor, anyone can create a website (or any other web service) on their computer and allow people to connect to it using the Tor network through an *.onion* URL. (Example: the Silk Road forums’ URL is *http://dkn255hz262ypmii.onion*) These addresses look like a jumble of letters and numbers, because they’re generated using cryptography, not for readability or memorability. The Tor software understands this *.onion* address and will connect you, anonymously through the Tor network, to this hidden server without leaving the network. Finding where the server is located can be extremely difficult. And trust me. They’re trying.

Silk Road is a Tor hidden service and can be found at the address *silkroadvb5piz3r.onion*, but only through Tor. If you put that into your normal web browser, it will just shoot you back an error, telling you it can’t find what you’re looking for.

There are a lot of useful Tor hidden services, a major one being Tor mail, an anonymous decentralized e-mail provider. You can find it at *jhiwjjlqpyawmpjx.onion*.

But Tor alone isn’t enough to make a site like Silk Road secure, or even remotely safe. Payment, shipment, and government eavesdroppers are still a problem. This is where Bitcoin and public-key encryption come in.

Leaderless Currency

Bitcoin is the first successful decentralized digital currency that we’ve ever seen. The idea of digital cash has been around for almost as long as the internet, but every form relied on some company or authority to regulate and control things. According to the creator, Satoshi Nakamoto, this has been the root of all previous digital currencies’ failures.

In order to get around what Nakamoto called “trusted third-parties,” Bitcoin uses a peer-to-peer network of computer systems that work together to automatically control transactions and the currency. Anyone who wants to use Bitcoins can connect to the network and be a part of it. Tasks that the U.S. Mint and the Federal Reserve would normally do with the dollar are spread out across the huge network of users. Decentralization is what makes this different from any other currency.

There is no central authority. Monetary policy is controlled by the majority. No single group or person can force the network to do anything or follow any rules.

“Satoshi Nakamoto” posted the first version of Bitcoin onto a cryptography mailing list in January 2009. Nobody on the list knew who he was.

Most people agree that Satoshi is a fake name. He e-mailed other Bitcoin developers using an anonymous mailing service and gave out zero personal information about himself. After a few years, Nakamoto stopped working on the project and people who’d been there since the beginning took over.

A lot of articles go into depth about who Nakamoto might have been. But what’s the point? It’s not like he invented Bitcoin from nothing. The technical document, bitcoin.pdf, references and builds on some other related projects and ideas. The closest is B-Money, written by crypto-thinker / computer programmer Wei Dei in 1998. In the article, Dei describes a theoretical system for people to send and receive money in anonymous and untraceable ways. Even though there were problems with the technical side of B-Money, the philosophy behind it is similar to what’s behind Bitcoin. Wei Dei wrote:

“In a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.”

In that way, it makes sense that whoever created Bitcoin didn’t want their real name(s) linked in real life. It would be too easy to attack (or corrupt) the world’s first popular decentralized currency if there was a spokesman or leader. *Cut off the head, kill the body*.

"So what the hell is Bitcoin?"

There's a lot of bullshit going around about *what* Bitcoin is. Some people are calling it a "Ponzi scheme." Another popular myth is that it's a scam because the people who were involved in the beginning (back when a Bitcoin was worth less than a penny) now control millions of dollars worth. That sounds exactly like every successful business deal ever made to me. The developers and supporters make it clear that this is experimental and that it's an extremely high-risk investment. They only hope that people will find it useful.

For every skeptic, there's someone calling Bitcoin the beginning of a revolution where the U.S. Mint, Federal Reserve, Visa, MasterCard, and PayPal are challenged and eventually made *obsolete*.

Enough opinion. Let's get down to what makes this new and exciting. The next bit will be a little technical, but I've tried to break it down into small, simplified sections that should be easy enough to understand.

Bitcoin is made up of two main parts: a system for non-reversible spending and a way to prevent "double spending."

With cash, as a seller, you don't have to worry about someone not having the money. It's right there. Straight cash. But with credit, payment is handled by companies like Visa and PayPal, who transfer money from one person's account to the other's. Up until Bitcoin, using one of these companies has been *the* way to do business, especially since most online transactions happen between total strangers and the chance of getting burned is high.

In a perfect world, all these companies do is take money from A and give it to B and try to make sure that a product gets from B to A.

But since they’re forced to settle problems between buyers and sellers, the processors require us to hand over all kinds of personal information. Their services aren’t cheap, either. Credit companies take flat fees and percentages from every transaction processed. They also have total control over what types of transactions or products are allowed.

Like cash, Bitcoin lets its users make non-reversible payments to anywhere in the world. To understand how this can be done digitally, you need to understand “public-key cryptography.”

There are two parts to public key encryption: a public key and a private key. You can think about a key like you would one that goes into a doorknob. One key, the public one, can lock a private door, but not unlock it. With the private key, you’d be able to unlock the door that was locked by the public key and take whatever was in the room. In public-key cryptography the process works in one direction. So you wouldn’t be able to unlock the private door with the public key once it was locked.

The keys are generated in pairs. The public key is created from the private key. Standard encryption goes like this: a message is encrypted with a public key and decrypted with a private key.

Let’s say that someone wants to send me an encrypted message that only I can read. First, I would use a program like GnuPG (this is a free public-key encryption program, based on the “OpenPGP standard”) to generate my public and private encryption keys. Then I’d give the sender my public key. I’d hide my private key somewhere secret where only I could get to it. The sender would take my public key and use it to encrypt a message. Only someone with my private key would be able to decrypt that message.

“Signing” a message is a similar, but almost-reverse process. With my private key, I can run a set of mathematical operations on a digested version of my message (called a “hash”). This would create a digital signature, which I would attach to the end of the message that I am signing. Anyone who wanted to see if I’d written the message, or if it’d been changed since they got it, would create their own hash of it, and then use my public key to decrypt the signature, revealing my version of the hash. If both are the same, it means that whoever signed the message had my public key and that the message hasn’t been changed since its signing.

Bitcoin uses this as the base for transactions.

So, let’s say that I have 10 Bitcoins and I want to send them to Bob. Let’s also say that I got them from Liz. I would create digital a message that basically says: “I will pay Bob 10 Bitcoins I got from Liz.” I will take my private key and sign the message. To prove that I sent the Bitcoins, anyone could use my public key to prove that I signed the message. In other words, proving that I spentmy 10 Bitcoins to Bob.

Your digital “wallet” is basically your private key. So, whoever has your private key controls your wallet and can spend your Bitcoins.

But if there’s no middleman like Visa or PayPal, I could easily sign the transaction above and then sign another transaction that says: “I will pay Matt 10 Bitcoins I got from Liz.” Matt and Bob wouldn’t know that I spent my Bitcoins twice. This is what was known as the “double spend.”

The Bitcoin P2P Network

The real innovation about Bitcoin is its relatively simple method for eliminating double spending *and* powerful "trusted" third parties: the peer-to-peer network.

Peer-to-peer (P2P) networking is something that almost everyone has used by now. BitTorrent is probably the most popular use for this type of network. When you download a torrent, all you're doing is loading a link to a few computers who share the same goal as you (downloading a file). The hope is that those users will link you to some others who link you to others. All of them will send you small parts of the file you want until you have the whole thing. If another computer pops up on the network that needs a piece of the file that you have, you can send it. Unlike Napster, chopping the head off of one or even one hundred of those systems will do almost nothing to stop you from downloading the file, as long as there are enough computers left connecting to each other and that they are physically spread apart. (Like in different countries with different laws.)

Bitcoin takes this idea and makes the file that everyone is sharing the Bitcoin ledger, or the history of all transactions. This makes private organizations like banks and credit companies unnecessary. In Bitcoin, everyone is the bank.

In the above examples I used "Bob" and other generic names to make a point about Bitcoin transactions. But really, no names are used. Instead, money is transferred between cryptographic aliases, which are based on someone's Bitcoin wallet (private key). These aliases are known as addresses. The above "Bob" example, would actually look more like this in the ledger: "29ac41a will pay 0ab55af 10 Bitcoins I got from ffab7ab," with the random numbers being Bitcoin addresses.

Unless you accidentally let people know which address is yours, it is possible to make fairly anonymous transactions.

But sharing the ledger using a peer-to-peer network, and using that ledger to believe a transaction, means that the ledger must be trusted. And that goes against the foundation of Bitcoin, which basically says trust nothing and demand proof of *everything*. This is known as the "proof-of-work" system.

Instead of the Bitcoin network just sharing random transactions and trusting all of them, the computers in the network are doing something called "mining." The process of mining is complicated, and a little outside of what I want to be talking about, but it basically comes down to a few things. Transactions are sent out over the network and are collected by other people's systems that are set up for mining. The mining systems ("miners") group up the transactions into "blocks."

Every block has a reference to the block before it, so they build what's called a "block chain."

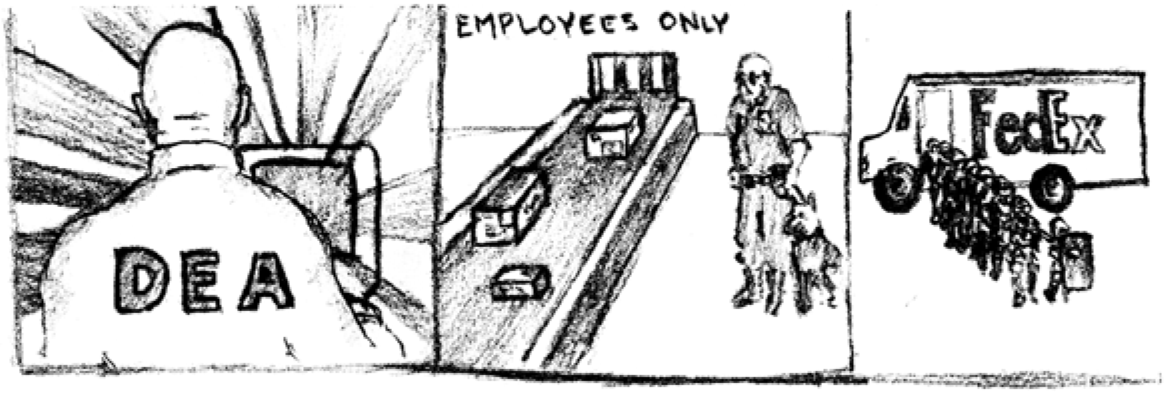
The miners take these blocks and run sets of intensely mathematical operations on them until they find a specific result. This result is agreed upon by the network based on how much time (and processing power, a.k.a. work) it takes to find, averaging to once every ten minutes. Right now (Dec. 2011), the estimated number of tries it would take to find the answer to the next block takes somewhere around 4.68 quadrillion computations.

While it's extremely difficult to find the correct answer to the next block, it only takes a second to check and make sure that it's the correct answer. As the blocks build on each other, transactions in blocks deeper down are more trusted than ones in brand new blocks. (Because more "work" has been done on top of that block.)

The block chain is what is being shared on the Bitcoin P2P network. Anyone who receives a transaction can check back through the block chain to make sure that those Bitcoins haven't already been spent. If they have, then the transaction is rejected and it shouldn't end up in the block chain. Otherwise, miners will continue to spread that transaction to other miners who'll include it in the block they're working on.

There's a 50 Bitcoin bonus (or "bounty") given to the person who finds the correct result to, or mines, the next block. Every four years or so, the amount of Bitcoins awarded to a miner gets cut in half, meaning that the total number of Bitcoins will max out at 21 million, sometime in 2140. This was chosen to make the supply of Bitcoins more like that of people crawling into caves digging up gold or silver. It also gets rid of the need for a mint.

In order to run the Bitcoin software (you can find it at bitcoin.org) you have to be connected to the internet. *Theoretically*, someone might be able to trace your IP address to some sort of Bitcoin activity, so a lot of people configure their Bitcoin client to run through Tor. Luckily, the official Bitcoin software makes connecting through Tor as easy as one click.



Getting Bitcoin

There are a ton of places to buy Bitcoins online. Most of them accept bank account transfers, checks, prepaid debit gift cards, money orders, and even cash. Credit companies and other online payment processors like PayPal have been "unfriendly" to Bitcoin-related companies (suspending accounts, freezing money), so it's not quite as easy as swiping that plastic, yet.

Even though *within* the block chain, transactions are only made between random-seeming addresses, it's not that hard for an investigator to trace a Bitcoin purchase to a person. Bitcoin was never intended to be used to launder money, to totally hide the fact that someone ever bought them, or to keep secret how many they have. It was just meant to make the transactions not directly linked to *names*; the rest is up to us.

The easiest and quickest way to buy Bitcoins is to transfer money from your bank account to an exchange company, who will buy Bitcoins for you at market price plus a small fee. But a lot of the payment methods, especially a bank transfer, leave an ugly paper trail leading right back to you.

"Tumbling" is a way for people to mix up the trail of transactions by swapping their Bitcoins with each other. There are a few ways to do this, but a popular way is to send your Bitcoins to what's called an e-wallet, which is basically an address and wallet stored on a website somewhere. Assuming the site operator isn't a scammer, and that a hacker doesn't steal all the wallets stored on the site while your Bitcoins are there (these things have happened in the past), you can send your Bitcoins to an e-wallet and then to another address that you create. (The Bitcoin software also makes this as easy as a click. The official recommendation is to create a new address for every transaction.) Doing this a few times, through different sites or exchanges, can make tracing where your Bitcoins went or came from harder.

I bought Bitcoins using a popular exchange service called GetBitcoin. They have accounts at Chase Bank and Bank of America, and you can make an anonymous cash deposit into their account to pay for your Bitcoins. This is how I got them. No ID required.

Teller: "GetBitcoin, LLC? What kind of company is that?"

Customer: "It's an internet thing. I just need a receipt, please!"

I took a photo of my receipt, and e-mailed it to GetBitcoin using an anonymous address I created using Tor mail. Within a day, I had Bitcoins in my wallet. Besides getting me on Chase Bank's security camera making a cash deposit, there was no trail proving that I ever bought Bitcoins. I got rid of the receipt, and securely deleted the picture of it.

For the hell of it, I transferred my Bitcoins to a couple e-wallet services and then back to a newly created address. I was happy with the number of steps I'd taken to hide the tiny trail that might have existed, and I figured it was time to spend my Bitcoins on Silk Road.

Cruising Silk Road and Buying Smack

Visiting Silk Road for the first time is strange. The first thing you see is an extremely minimalistic login box and a message warning you to double check the URL. I guess there are a ton of people out there setting up fake Silk Road sites that steal your password.

I took a page from Philip K. Dick's *The Three Stigmata of Palmer Eldritch,* and turned it into a ridiculously long and complicated password. Then I was in. Silk Road is a culture shock compared to modern websites. It's rugged. Nothing but green text and photos of products: pharmaceuticals, psychedelics, weed, and every illegal powder you could dream of.

Even though the extreme majority of products sold on Silk Road are drugs, you can get anything from e-books on "anarchy" type topics, to GPS tracking devices, to downloads of popular porn sites. There are even Silk Road T-shirts going for about thirty bucks.

Almost everything on Silk Road is a little overpriced. The site administrators take a cut of the sales and since the Bitcoin fluctuates in value so quickly, dealers often add a small percentage to try and compensate.

It's easy to get the picture that Silk Road is some kind of a free-for-all where you're constantly one step away from getting your digital cash stolen by scammers and your identity revealed to the cops. But really, Silk Road makes buying shit that can get you thrown in a prison cell for a decade or so, incredibly smooth and simple.

Drugs are divided by type: "opioids," "stimulants," "marijuana," etc. Individual listings are sorted by top-selling items. You can see the username of the seller and their rating: a 0 – 100 scale, based on the seller's past customer reviews. There is also a Silk Road forum (a separate Tor hidden service) where Silk Road users get together and talk. Vendor ratings can also be found on here.

For each group of drugs, there are a couple veteran sellers who are basically Silk Road drug dealing professionals. These people ship quick, package carefully, sell at fair prices, and have generally awesome reviews.

The guy who I bought heroin from was one of these people, and is basically the go-to guy for the stuff. He had a ton of reviews. One guy was excited enough to write: "Just pulled the needle out of my arm and all I can say is 'ahhhhhhhhhh.' This dope is among the best and cleanest I've had. The shipping was fast as all hell too. This Silk Road heroin dealer is the real deal. Thanks a ton, bro!"

Buying anything on Silk Road is extremely easy. Once you have the Bitcoins, you send them to an address that is connected to your Silk Road account. (Silk Road tumbles your Bitcoins with other users' as an added precaution, but that's basically trading drug money for drug money.) Once the Bitcoins are transferred, you can buy a product just like you would on any site using the Silk Road shopping cart. Once you buy the product, Silk Road holds your money and asks you for your address.

Here's how Silk Road escrow works: you buy a product using the site and Silk Road holds onto your Bitcoins; you enter the shipping address and it is sent to the seller, your order is now in "processing." Once the seller ships the product they mark the order as "in transit." (The seller has three days to do this, or else the order can be cancelled.) Once the package arrives, the seller marks the order as "finalized," the Bitcoins are given to the seller, and the buyer can leave feedback and a 0-5 rating. Finalization cannot be undone and escrow is over. Some dealers demand that buyers with less than five or so transactions finalize before shipment, but not all do. If there's a problem between buyer and seller, the Silk Road administrators will help resolve it. A common result is 50% refund to the buyer if the seller reships 50% of the product.

In my and a lot of other people's opinions, sending the address is the sketchiest part of the whole deal (for the buyer, at least). You have to trust that your dealer isn't a cop, and that your address isn't going to get leaked out. Most vendors put their public encryption key on their information pages and urge you to encrypt your address before sending it to them. On the same page, sellers usually go into some detail about their operation, some precautions to take, and how good their packaging methods are.

One respected seller warned users to never check a tracking number using Tor. According to this particular seller, postal companies watch for connections from the Tor network and confiscate the tracked packages. Silk Road has a few suggestions of their own for receiving products. Never ship directly to where the package will end up. Ship to a real name, or a *very* similar looking name, so the mail actually gets delivered by the mailman. And never sign for a package.

The precautions are there to make the mail blend in and the transaction go smoothly, with as little interference from authorities as possible. As far as I can tell, it works. A regular looking envelope showed up in the mail three days after ordering. The return address was for some nerdy shop on the East Coast. Imagine what kind of a mind-blow it would be for the owner of a shop that sells Pokémon shit to find out that their business is being printed as the return address for heroin filled envelopes.

There was a hilarious post on the Silk Road forums by two people arguing about some kind of a botched deal. One guy said he got ripped off (someone finalized their order on accident, from what I can tell) and was threatening another, more respected, user IN ALL CAPS. He went on and on about how *nobody* disrespects him and how in real life he fucks up anyone who tries. People on the forum made fun of him and told him to shut the hell up. It showed how successful Silk Road really is. It makes drug buying and selling so smooth that it's easy to forget what kinds of violent fuckers drug dealers can be.

That's the whole point of Silk Road. It totally takes evil pieces of shit out of the drug equation. Whether they're vicious drug dealers or bloodthirsty narcotics cops, both sides of that coin suck and end pretty much the same way. Death, despair, madness, prison, etc. Thanks to decentralization and powerful encryption, we're able to operate in a digital world that is almost free from prohibition and the violence it causes.

Senators Joe Manchin and Charles Schumer declared war on Silk Road and Bitcoin in June this year. In a highly-publicized press conference, Schumer called Silk Road a "brazen attempt to peddle drugs online" and dumbed Bitcoin down into a high-tech money laundering tool. Anyone who agrees with them isn't just cheapening what's happening, but is missing the whole point.

This goes beyond people trying to get around laws and use the internet to commit crime. This goes beyond that nasty scar on the face of human history, the "war on drugs." This is about *real* freedom. Freedom from violence, from arbitrary morals and law, from corrupt centralized authorities, and from centralization altogether. While Silk Road and Bitcoin may fade or be crushed by their enemies, we've seen what free, leaderless systems can do. You can only chop off so many heads.

This is the future.