ROCIC SPECIAL RESEARCH REPORT

Penetrating the Darknet

Silk Road, Bitcoins, and the Onion Router

© ROCIC 2013

ROCIC is a RISS Center
A Proven Resource for Law Enforcement®

SILK ROAD BLACK MARKET WEBSITE SHUT DOWN BY FEDERAL AGENTS

He had eluded law enforcement authorities for years, hiding on the Darknet, operating the most sophisticated and extensive hidden website where vendors could anonymously sell illegal goods and services ranging from Purple Haze pot to Fentanyl lollipops to a kit for converting rifles into machine guns.

Calling himself Dread Pirate Roberts or DPR, the 29-year-old white male had amassed at least $80 million in transaction commissions, all hidden in the crypto world of virtual currency. Over 36 months of operation, the site had been used by hundreds of thousands of customers throughout the world to purchase $1.2 billion in illicit goods and services. Displayed on the massive site, similar to amazon or eBay, were 13,000 listings for cannabis, Ecstasy, opioids, psychedelics, and stimulants. Service listings included computer hacking, malicious software, pirated media, fake driver's licenses, and bogus passports.

All customers were required to use Tor (The Onion Router) software, which concealed their Internet Protocol addresses by bouncing them around a worldwide network of servers, and to pay with Bitcoins, a decentralized form of digital currency consisting of numbers and letters. The website was not even visible to the average Internet user.

The black-market website also used a so-called tumbler, which sent all payments through a complex, semi-random series of dummy transactions, making it nearly impossible to link payments with any Bitcoins leaving the site. Buyers and sellers were operating in the shadows.

DPR maintained the computer infrastructure and programming code underlying the website; he determined vendor and customer policies, including deciding what can be sold on the site; he managed a small staff of online administrators who assisted with the day-to-day operation of the site; and he controlled the enormous profits generated from the operation of the site (commissions averaging 10 percent).

Reportedly, DPR attempted to have one vendor named FriendlyChemist murdered after the vendor demanded half a million dollars not to reveal a long list of website users.

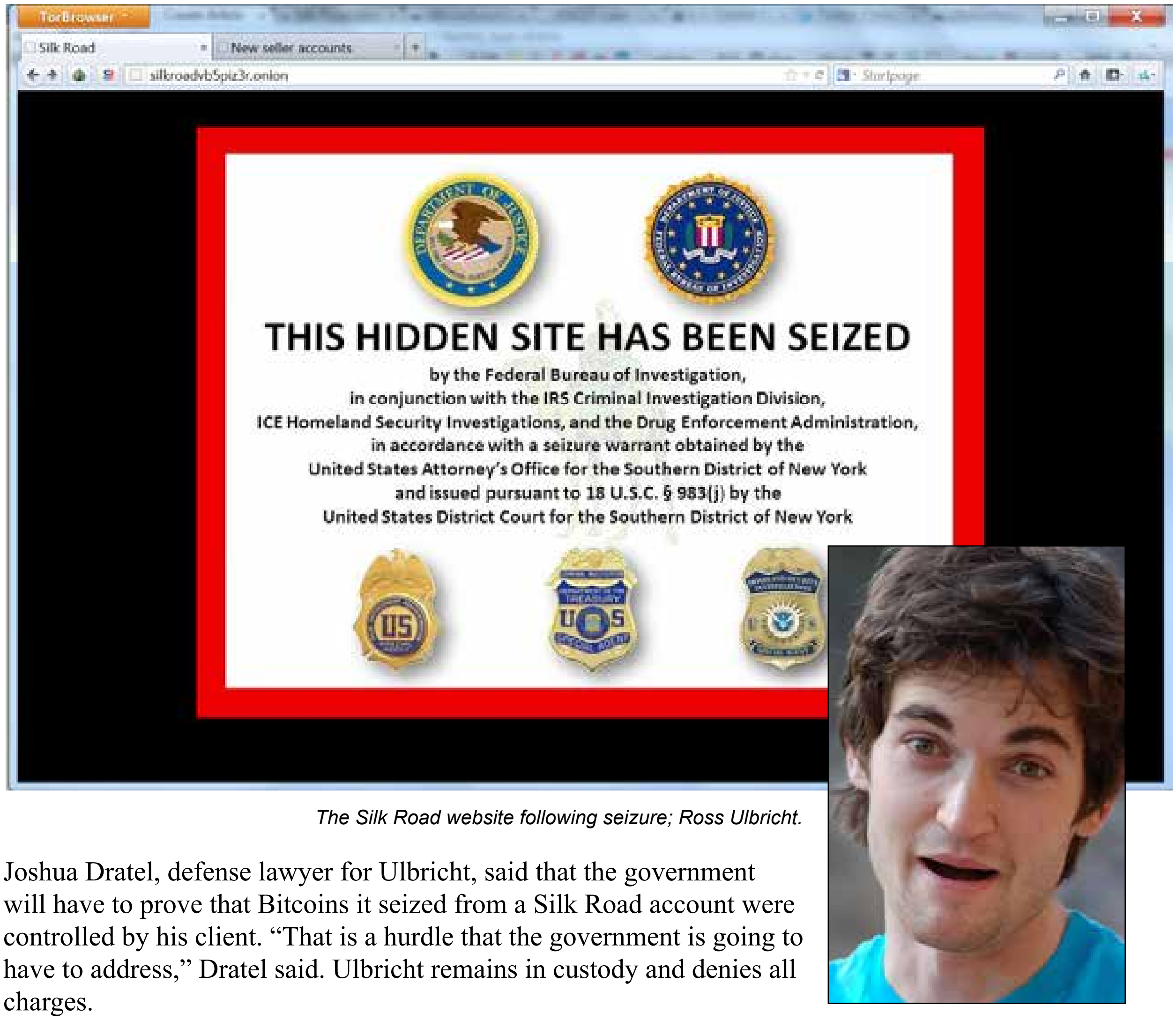
"The highest levels of government are hunting me," he told an online journalist from the safety of encrypted communications while claiming to have defeated the government's "war on drugs." Business was so lucrative that competing encrypted websites were beginning to steal the spotlight.

Federal agents catch their man

It all came crashing down on Oct. 1, 2013, when federal agents found the man they were looking for in the science fiction section of a San Francisco branch library working on his laptop.

Ross William Ulbricht, aka DPR, the alleged mastermind of the notorious Silk Road black-market website, was arrested and charged with criminal narcotics conspiracy, computer hacking, and money laundering. The charges could land him in prison for life. In a separate indictment in Baltimore, Md., he was accused of attempted murder for hire. There is no evidence, however, that the murder-for-hire scheme was accomplished.

Silk Road was shut down. The Feds eventually confiscated 174,000 Bitcoins worth $33.6 million at market value in connection with a civil action.



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

The Silk Road website following seizure; Ross Ulbricht.

Joshua Dratel, defense lawyer for Ulbricht, said that the government will have to prove that Bitcoins it seized from a Silk Road account were controlled by his client. “That is a hurdle that the government is going to have to address,” Dratel said. Ulbricht remains in custody and denies all charges.

The investigation is ongoing. The seizure of six of Silk Road’s servers in places such as Latvia and Romania allowed authorities to surveil the buying and selling of illegal drugs on the site. During the actual investigation of Silk Road, investigators made approximately 100 purchases of illegal drugs themselves. Four drug dealers have been arrested in Great Britain.

Although Silk Road was not involved in large kilo-levels of drug trafficking, DEA spokesman Rusty Payne told ROCIC that “not only are we interested in getting drugs off the streets, we want to know where these drug proceeds are going—follow the money.” Darknet sites are being

This Publication was supported by Grant No. 2011-RS-CX-K007, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Office of Justice Programs also coordinates the activities of the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position of ROCIC or the United States Department of Justice.

used to launder criminal proceeds. Some online drug funds have been traced to foreign criminal and terrorist organizations that threaten our national security.

Other online black markets seek to fill the void

Silk Road isn't the only online illicit goods market in town, so to speak.

Deepbay, Sheep Marketplace, and Black Market Reloaded (BMR) are trying to pick up where Silk Road left off, according to an article on The Verge. BMR has the most drug listings with 3,567. BMR has no qualms about selling weapons or child pornography, unlike Silk Road. Deepbay has dropped commission fees to 3 percent. All three darknet sites require the use of Tor software and Bitcoins, so it's likely that they will also end up seized by federal authorities.

Another market, Atlantis, was gaining popularity until it shut down and absconded with customer deposits a week before the Silk Road shutdown, despite a concerted marketing campaign with a YouTube video posted on how to use the site.

Users of illicit online drug bazaars can discuss their experiences on sites like Reddit, which has dedicated "subreddits" for both Black Market Reloaded and The Sheep Marketplace.

Darknet users consider government regulation as oppression

Although the chief motive for these sites is profit, there is a philosophical side to them also.

One of Silk Road's enablers was quoted upon its shutdown, "We have the power to fight these agents of oppression, to fight the governments that task them with that oppression, and with the fires that Silk Road has stoked in our hearts and minds we must do just that."

The quote illustrates the attitudes of many in the online community, who consider the darknet as a utopian way of challenging "government oppression and surveillance." For many, virtual currencies such as Bitcoin are viewed as a mission or even a secular religion. Others who claim no

Buying Drugs Online

"The age of narcotics e-commerce has arrived," declared a recent *Forbes* article.

The *Forbes* author used Tor and Bitcoins to purchase gram quantities of marijuana from three online illicit drug markets (this was before Silk Road was busted). The survey was not scientific and the purchased drugs were not tested for purity.

On Silk Road, it cost $24 in Bitcoins to buy one gram of Grape God marijuana. It arrived in a double-vacuum seal in six business days. The vendor insisted that customers release their payment escrow before the product arrived, contrary to website rules.

On Atlantis, one gram of Snow White Kush purchased for $23 in Bitcoins arrived triple vacuum sealed in two business days.

On Black Market Reloaded, a half-gram of pre-rolled Joints of Haze purchased for $9 in Bitcoins never arrived. The vendor was based in the Netherlands and was the only vendor found listing small quantities of marijuana.

The article warned: don't try this at home. It also noted that the magazine's attorney demanded that the drugs be destroyed immediately and a video posted of the cannabis being flushed down the toilet.

criminal intent whatsoever trumpet markets without governmental regulation or supervision, citing the Austrian model of economics, and calling their network The Clearnet.

Both Tor and Bitcoin reacted to the closing of Silk Road. "We've been watching carefully to try to learn if there are any flaws with Tor that we need to correct," stated the Tor Project. "So far, nothing about this case makes us think that there are new ways to compromise Tor (the software or the network). The FBI said their suspect made mistakes in operational security, and was found through actual detective work."

The Bitcoin Foundation stated, "It is important to note that the sanctity of the Bitcoin protocol remains intact and it was not a weakness of the core protocol that led to the apprehension of Mr. Ulbricht. Although Bitcoin is not anonymous by default, Bitcoin addresses were not a factor in solving the case. The FBI was able to capture an alleged criminal without any new investigative methodologies being needed and without having to get into changing the nature of the Bitcoin protocol. They caught him the same way they would catch somebody using cash."

Multi-jurisdictional Effort

Credited with catching Dread Pirate Roberts were the FBI's New York Special Operations and Cyber Division, the DEA's New York Organized Crime Drug Enforcement Strike Force, which is comprised of agents and officers of the DEA, the IRS, the New York City Police Department, U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Secret Service, the U.S. Marshals Service, Office of Foreign Assets Control, and NY Department of Taxation. Also cited were the Chicago field office of ICE-HSI, as well as the Department of Justice's Computer Crime and Intellectual Property Section. Foreign law enforcement partners included the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight against Crime Linked to Information Technology and Communication. The prosecution is being handled by the Office of U.S. Attorney Preet Bharara, Southern District of New York, Complex Frauds Unit. Assistant U.S. Attorney Serrin Turner is in charge of the prosecution, and Assistant U.S. Attorney Christine Magdo is in charge of the forfeiture aspects.

Perpetrator slipped up early in the process

According to a *TIME* magazine article: "Indeed, according to its complaint, the FBI eventually found Ulbricht by scouring the "surface web" for hints of Ulbricht's identity—as opposed to the deep web, which is not indexed by search engines. Ulbricht slipped up early in the process when he first began to promote Silk Road on a surface website forum dedicated to illegal drugs using the handle "Altoid." Months later, according to the complaint, Ulbricht appeared on another forum under the same handle asking for information about Bitcoin and asking other readers to email him. He then listed his personal email address. These slip ups, among others, eventually allowed the FBI to close in on Ulbricht's identity and the location of Silk Road's servers. One of the reasons Ulbricht was caught was that he purchased several fake IDs in order to rent servers to grow Silk Road's capacity. Ulbricht had these IDs shipped from Canada, and they were discovered during a routine customs inspection."

Ross Ulbricht grew up in Austin, Texas, and graduated from the University of Texas-Dallas, earning a degree in physics. He attended grad school at Penn State. He started Silk Road on Jan. 27, 2011 and moved to San Francisco in September 2012. He lived in a room for $1,000 a month cash. He was known as Josh. His moniker Dread Pirate Roberts, a "ruthless pirate who takes no prisoners," comes from the novel and movie *The Princess Bride.*

Investigators stalk Altoid and Frosty

The following scenario is derived from a *USA Today* article by Donna Leger, based on information from court records:

A simple search by an FBI agent turned up postings on forums back in 2011 from a person known as Altoid, publicizing the advantages of a hidden service known as Silk Road. Altoid instructed potential candidates to reply to his Gmail address, rossulbricht@gmail.com. A photo subpoenaed from Google from the email address matched the photo listed by Ulbricht on his LinkedIn profile. The Google records showed every IP address used to access Ulbricht's Gmail account in 2013 from Jan. 13 to June 20, court papers said. The IP address associated with the Gmail account led to a computer in an apartment on Hickory Street in San Francisco (Ulbricht's residence). The logs indicated Ulbricht accessed his Gmail account from a café on Laguna Street, less than 500 feet from the apartment, court papers say.

Ultimately, the FBI linked the computer at the Hickory Street apartment and its IP address to code on the Silk Road server that allowed the computer access, court papers say.

On March 5, 2012, Ulbricht opened an account under his own name on stackoverflow.com, posted 12 lines of computer code, and sought advice for fixing a coding problem. He quickly deleted his real name and changed his user name to "frosty" and his e-mail to frosty@frosty.com.

Forensic analysts found a revised version of the same code on the Silk Road website, court papers say. The analysis also found encryption keys that end with frosty@frosty.com.

Investigators go undercover

An FBI agent went undercover in 2012 posing as a drug dealer. The agent emailed "Dread Pirate Roberts," directly seeking help finding a buyer for a kilo of cocaine. Ulbricht allegedly instructed one of his employees to help. The alleged buyer, who turned out to be the employee, deposited $27,000 in Bitcoins in a Silk Road account and arranged a shipment to his home. Federal agents arrested the employee, who has not been identified.

On Jan. 26, the FBI says in court papers, Ulbricht emailed the undercover agent to say the employee had been arrested and had stolen funds from other Silk Road users. He allegedly asked the agent to have the employee beaten up and forced to return the money.

The next day, Ulbricht allegedly asked the FBI agent to have the employee killed because "now that he's been arrested, I'm afraid he'll give up info." The FBI says Ulbricht agreed to pay $80,000 for the hit and on Feb. 4 wired $40,000 from Technocash Limited in Australia to a bank account at Capital One in Washington. Ulbricht deposited another $40,000 after the undercover agent emailed him staged photographs of the killing, court papers say.

By July 23, investigators had located at least one of Silk Road's servers in an unnamed foreign country. The FBI executed a Mutual Legal Assistance Treaty request that allowed law enforcement in that country to make a copy of the Silk Road server and give it to the FBI. The snapshot gave the FBI records of 1.2 million transactions from February to July and all of the site operator's email exchanges.

How the FBI located the Silk Road server remains a mystery.

Manhunt closes in on likely suspect

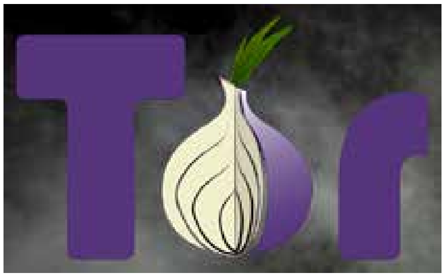
On July 10, as part of a routine search at the Canadian border, customs agents intercepted a package of nine fake IDs, each with a different name but all with a photo of Ulbricht. Email exchanges found on the Silk Road server indicate Dread Pirate Roberts had sought IDs in June from several Silk Road vendors so he could rent servers under an assumed name.

On July 26, three days after federal investigators located one of Silk Road's servers, investigators paid Ulbricht a visit to ask about the IDs. Ulbricht said he didn't know anything except that there were sites on the Internet where people could buy fake identification.

On Oct. 1, federal agents waited until Ulbricht logged into his computer before sweeping in to the Glen Park branch of the San Francisco Public Library to arrest him, making it easier for agents to simply plug in a thumb drive and download everything on the computer without having to break his passwords.

Criminals Use Anonymity of Darknet to Profit While Eluding Authorities

Criminals on the Internet often resort to a hidden place called the Darknet. Darknet sites are hosted on regular Internet servers, but to access them you need special software, usually utilities that encrypt all users' traffic and allows them relative anonymity. We're talking about pedophiles, hitmen, and drug and weapons traffickers.



Many Darknet patrons use Tor software to move around anonymously. The notorious Silk Road black-market site used Tor, which is short for The Onion Router. According to an extensive article in USA Today, the U.S. Naval Research Lab developed onion routing, the concept behind Tor, as a way to protect naval communication so an enemy could not trace computer messages and detect a ship's position.

Every computer on the Internet has an Internet Protocol, or IP, address that can be used to find its physical location. Tor, which is totally legal, ensures privacy by randomly routing computer messages through several places on the Internet, wrapped in layers of encryption, so no single point can link the source to the destination.

The routing system is public and maintained by a non-profit organization that runs on donations from a variety of organizations, including Human Rights Watch, Radio Free Asia, the National Science Foundation, and Google.

Dissidents in countries that restrict Internet access use Tor to publish protests out of government reach. Journalists use Tor to communicate with confidential sources. WikiLeaks used Tor to collect documents from whistleblowers who wanted to remain anonymous. Law enforcement agents use Tor to visit websites without leaving a record of a government computer or IP address in the web's log. It is also used by undercover officers in sting operations and can be used for anonymous tips.

Tor is available as a download on Torproject.org for PC, Mac, and Linux. It will block browser plugins such as Flash, RealPlayer, Quicktime, among other things, so it might not be the optimal choice for all web users.

Child pornography conspiracy alleged

The FBI is seeking the extradition from Ireland of Eric E. Marquis, 28, owner of a computer services and web hosting company and, according to the FBI, "the largest facilitator of child porn on the planet." He is allegedly the operator of Freedom Hosting, the largest web hosting company on the Darknet. The FBI alleges that Marquis, who holds dual US-Irish citizenship, advertised and distributed child pornography from 2008 to 2013.

Darknet retagged as the Clearnet

Citizens concerned about online government surveillance by agencies such as the NSA are turning to the Darknet. Because they are not using it for criminal purposes, they call it the Clearnet.

The *New Yorker* ran a Tor-hidden service built by the hacker Aaron Swartz and *Wired* magazine's investigations editor, Kevin Poulsen, so whistleblowers can securely leave documents or messages. DuckDuckGo, a privacy-minded search engine, also runs a Tor-hidden service so users can search the web in complete anonymity. Hyperboria is an encrypted network where users connect peer-to-peer. Nobody can intercept a connection. It only has 500 users—you can join only by asking an existing user's consent. Hyperboria has a Twitter-like clone called Social-node, a Reddit-powered voting-and-sharing service called Uppit, spaces for file-sharing, blogs, and lively IRC channels.

Email may morph into Darkmail

Ladar Levison, founder of Lavabit, the now-closed encrypted-email service used by former National Security Agency contractor and leaker Edward Snowden, is working with encryption company Silent Circle to create a new kind of messaging called Darkmail, set to launch next year.

The trick to the new system is software where only users, and not email providers, have the keys to private messages. In Darkmail, users would encrypt messages with private keys kept only on their computers or mobile devices before sending them. It means that if the government asks a Darkmail company for user data, the company would only be able to offer garble.

This past summer, Levison received a request from the FBI to hand over encryption keys to Lavabit. Sharing the keys would have allowed the FBI theoretically to monitor all of Lavabit's 400,000 users. He complied with the FBI request but then shut down Lavabit, making future access impossible.

In short order, Silent Circle closed its own encrypted-email service, Silent Mail, out of fear it could be forced to provide similar information to the government.

Email was never meant to be anonymous. Even though some technology now allows users to encrypt the bodies of their messages, email still requires certain data—including the subject line, the sender and the recipient—to be left in unencrypted text. Prying eyes can see who is sending emails to whom although they can't read the body of the message itself.

Gadget would create anonymous wireless networks

A $100 gadget called D-Central will allow users to create small local-area wireless networks where people can communicate anonymously, according to its inventor, eccentric playboy John McAfee, 68, the creator of McAfee Antivirus (he no longer owns the company). He said the revolutionary technology, which will reportedly ship about mid-2014, "will reclaim our lost privacy."

The device adds a "lower layer" to the Internet and will have a range of only three blocks. Uplinks and downloads are made anonymously as the network constantly changes users. D-Central will communicate with Android or iPhone smartphones, tablets, and laptop computers.

McAfee claims his unique encryption method has never been seen by the NSA and any other surveillance agency. He added that D-Central will protect against not only government surveillance but malicious hackers.

The Tax Man Cometh!

Revenues derived from transactions involving virtual currencies are most likely taxable by the Internal Revenue Service, according to a study released in June 2013 by the Government Accountability Office (GOA). Currently, however, the IRS does "a poor job of tracking" such transactions and educating buyers and sellers.

GAO said that strict virtual (or "closed flow") transactions in which virtual currency is used only within a game or virtual environment to purchase virtual goods and services were not taxable. However, so called "hybrid" and "open flow" virtual currency systems, in which real world currency is used to buy virtual currency, which is then used to buy or sell virtual- or real world goods and services are subject to U.S. taxes.

Some virtual economies in massively multiplayer online role-playing games (MMORPG) like World of Warcraft are "hybrid" systems in which in-game economic activity can spill into the real world via third-party transactions in which virtual goods are exchanged for real money, GAO said.

Bitcoin miners, who earn Bitcoins by processing Bitcoin transactions over the network with their computers, are most likley liable for paying taxes on their "virtual" earnings.

In August 2013, Judge Amos Mazzart of the U.S. District Court of Eastern Texas ruled that virtual currencies such as Bitcoin are actually money, especially since it can be exchanged for real-world money. Trenton Shavers of Bitcoin Savings and Trust has been accused by the Securities and Exchange Commission of running a virtual currency Ponzi scheme. He allegedly raised more than $4.5 million worth of Bitcoin from investors who were promised a weekly interest rate of seven percent.

Virtual Currencies Becoming More Popular Online

Money Not Backed By Any Bank or Government

Virtual currencies are those money systems that exist only on the Internet. Some examples are Bitcoin, Litecoin, Linden Dollars used in the Second Life virtual environment; Simoleons used in the virtual game The Sims, and WoW Gold used in the World of Warcraft gaming world.

Some currencies are closed and can only be used online. BitCoin and Linden Dollars are open-flow systems which can be used to purchase both real and virtual goods and services and can be exchanged for real-world currencies such as the U.S. dollar. Hybrid systems such as WoW Gold allow virtual currency to be converted into U.S. dollars via third-party transactions.

PayPal and other similar systems are not virtual currency. They are global e-commerce businesses allowing payments and money transfers to be made over the Internet.

“The idea of digital money—convenient and untraceable, liberated from the oversight of governments and banks—has been a hot topic since the birth of the Internet,” according to Wired magazine. “Cypherpunks, the 1990s movement of libertarian cryptographers, dedicated themselves to the project. Yet every effort to create virtual cash had foundered. Ecash, an anonymous system launched in the early 1990s by cryptographer David Chaum, failed in part because it depended on the existing infrastructures of government and credit card companies. Other proposals followed—bit gold, RPOW, b-money—but none got off the ground.”

Bitcoin emerges on the scene

Bitcoin was founded in 2008 by a man named Satoshi Nakamoto, who claimed to live in Japan. Very little information is actually known about Bitcoin’s creator or even that he actually exists. Some suspect it’s an alias. Others claim the name was composed from four companies–SAmsung, TOSHIba, NAKAmichi, and MOTOrola. Some say it was a team at Google or the NSA.

Bitcoin substituted a centralized clearinghouse with a computer network that solves mathematical puzzles to verify transactions and create new Bitcoins (see article and charts in this report for a more technical explanation). It was estimated that in the year 2140 the currency will reach its preordained limit of 21 million Bitcoins. Nakamoto himself mined the first 50 Bitcoins – which came to be called the genesis block – on Jan. 3, 2009. Virtually a recluse, Nakamoto posted his final message to the Bitcoin forum in December 2010.

Supporters see Bitcoin as a religion

All of this came at the time of the 2008 financial

FBI assesses Bitcoin

Bitcoin will likely continue to attract cyber criminals who view it as a means to transfer, launder, or steal funds as well as a means of making donations to groups participating in illegal activities, such as hactivists. As long as there is a means of converting bitcoins into real money, criminal actors will have an incentive to steal them. Since maintaining anonymity while using Bitcoin requires that users not exchange or transfer their bitcoins using third-party bitcoins services that require real world account information, the use of bitcoins to make donations to disreputable groups (which can be done within the Bitcoin P2P system) will likely remain one of the most popular uses for the virtual currency.

If Bitcoin stabilizes and grows in popularity, it will become an increasingly useful tool for various illegal activities beyond the cyber realm. For instance, child pornography and Internet gambling are illegal activities already taking place on the Internet which require simple payment transfers. Bitcoin might logically attract money launderers, human traffickers, terrorists, and other criminals who avoid traditional financial systems by using the Internet to conduct global monetary transfers.

Although Bitcoin does not have a centralized authority, the FBI assesses with medium confidence that law enforcement can discover more information about, and in some cases identify, malicious actors, if the actors convert their bitcoins into a fiat currency. Third-party bitcoin services may require customers to submit valid identification or bank information to complete transactions. Furthermore, any third-party service that qualifies as a money transmitter, and therefore a MSB, must register with the FinCEN and implement an anti-money laundering program.

Excerpt from FBI Intelligence Assessment, "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," April 24, 2012

crisis, the beginning of the so-called Great Recession, and now ever-increasing concerns over computer hackers and government-sponsored online surveillance.

"Bitcoin enthusiasts are almost evangelists," said Bruce Wagner, who hosts *The Bitcoin Show,* a program on OnlyOneTV. "They see the beauty of the technology. It's a huge movement. It's almost like a religion. On the forum, you'll see the spirit. It's not just me, me, me. It's what's for the betterment of Bitcoin."

Although owners see value in Bitcoin's decentralization, Bitcoin values can fluctuate wildly.

In the beginning, Bitcoins had no value at all. Once they started trading in April 2010 a Bitcoin was worth about 14 cents. By a year later it had topped $1 before settling in at 87 cents. In April-May 2011, due to media publicity, it soared to $8.89. When it was revealed that drug dealers used it online, the value of a Bitcoin tripled within a week, to $27. A Tennessean dubbed KnightMB, who held 371,000 Bitcoins, became worth more than $10 million, the richest man in the Bitcoin realm.

A Norwegian who on a whim bought 5,000 Bitcoins worth $24 in 2009 just recently remembered his earlier investment. After a frantic day of trying to recall his password, he discovered the Bitcoins were valued at $690,000. He cashed in a fifth of his stash and bought an apartment in Oslo.

Reportedly the value of Bitcoins fell 20 percent after the seizure of Silk Road but has since rebounded. As of Nov. 8, 2013, the value of a single Bitcoin was $313.55.

Law enforcement seeks answers

Law enforcement agencies are concerned that virtual currencies can be used by criminal organizations and individuals to anonymously launder money and to buy or sell illegal goods such as drugs and weapons, all without regulation or paying taxes to government authorities.

"In addition to getting drugs off the streets we want to know where these drug proceeds are going," said DEA-Washington spokesman Rusty Payne. Some drug proceeds going overseas are used for terrorist activities, he noted. "Bitcoins seek to be virtually untraceable, leaving the buyers and sellers of drugs seemingly hidden from law enforcement. As for investigations, law enforcement is keeping up with every new method criminals are using to evade authorities."

In March 2013, the U.S. Treasury Department's Financial Crimes Enforcement Network moved to clarify that existing money-transmitter rules that apply to businesses such as Western Union Co. and MoneyGram International Inc. also apply to sellers and exchanges of virtual currencies.

Some state banking regulators have also pressured Bitcoin-related companies to obtain licenses to operate as money transmitters. States typically require companies to post a bond that in some cases can cost several million dollars for such licenses.

In August 2013, members of the Bitcoin Foundation met with the U.S. Treasury's Financial Crimes Enforcement Network and several other federal agencies for an informational presentation. A lot of questions were asked. Government regulators are investigating whether new rules should be adopted as the popularity of virtual currencies increases.

Libertarianism and Austrian school of economics

The previous month, 350 enthusiasts met in midtown Manhattan for "Inside Bitcoins," a one-day seminar and gathering of the faithful. Many consider the advent of digital currency systems, which are not tied to governmental regulation or supervision, as revolutionary, utopian, and even religious in nature.

"The Bitcoin movement has a strong element of a counterculture about it, and in that sense it looks less like the dot-com boom or gold rush, to which it's often compared, and more like the 60s hippie culture," according to an article in the Wall Street Journal. "There's a strong feeling among its followers that they're actually creating a new world, a digital world in this case, that will sweep away

THE WORLD'S FIRST BITCOIN ATM went live on Oct. 28, 2013 at a coffee shop in Vancouver, British Columbia, Canada. In less than a minute, a customer received a tenth of a Bitcoin in exchange for his $20 bill and ordered a steamed milk with vanilla. It was "super-convenient and easy to use," said the user, who happens to handle real-world currency as a bank account manager.

Robocoin takes only cash and gives you numbers. If you already own Bitcoins, the ATM can scan a QR code on your smartphone and dispense cash.

It takes a scan of your palm and matches that to a database to ensure that you're not buying more than $3,000 per day — means of deterring money launderers — and then the machine connects to a back-end Bitcoin exchange to buy and sell your coins in real time.

You don't need a bank account to use Robocoin and, at least in Canada, you don't need any identification. The U.S. version of the machine will have more stringent identification requirements.

Canadian authorities don't consider Bitcoin as "funds or the currency of a country," and therefore the machine is not subject to regulation.

The ATM is owned by three men who are already trading Bitcoins at a storefront called Bitcoiniacs.

Of course, high technology is prone to glitches. The ATM went offline for awhile and it took three hours to prep the machine for its first transaction.

Bitcoin ATMs are expected to appear in the U.S. soon.

existing financial structures, which are either outdated and archaic, or ominously close to totalitarianism. (To Bitcoiners, what happened in Cyprus – where private bank deposits were seized to help pay off a bailout – is less an outlier and more a foreshadowing).”

Advocates of virtual currencies often identify themselves as libertarians, those who emphasis individual liberty, free markets, and fewer government regulations. They also cite the Austrian school of economics, which is closely linked to libertarianism. The two leading Austrian economists of the 20th century were Ludwig von Mises and Friedrich A. Hayek. Mises (in the 1920s) and Hayek (in the 1940s) both showed that a complex economy cannot be rationally planned because true market prices are absent. As a result, the information critical for centralized planning cannot be obtained, according to this theory.

Criminal cases involving Bitcoins

In June 2013, Michael M. Brown, 24, of Franklin, Tenn. was charged in District Court with demanding that $1 million worth of Bitcoins be deposited into his account to prevent the release of computerized tax returns allegedly stolen from an accounting firm. The tax returns were supposedly those of former Presidential candidate Mitt Romney and his wife. The alleged extortion scheme was perpetrated during the 2012 Presidential election campaign.

On Nov. 1, 2013, Vladimir Kats of Brooklyn, N.Y. pled guilty to money laundering charges in connection with the operation of Liberty Reserve, a Costa Rican digital currency service created in 2006. It is estimated that Liberty Reserve laundered more than $6 billion in criminal proceeds.

“Vladimir Kats, by his own admission, helped to create and operate an anonymous digital currency system that provided cybercriminals and others with the means to launder criminal proceeds on an unprecedented scale,” stated the acting assistant attorney general.

For years, it operated one of the world’s most widely used digital currencies, touted as “instant

Homeless Geeks

There are beneficiaries of the computer age and virtual currencies such as Bitcoin who wouldn’t readily come to mind—the homeless. Panhandling isn’t what it used to be.

According to an article in *Wired* magazine, Jesse Angle, 42, is a homeless man in Pensacola, Fla. who lives off food stamps. He spends time in a city park, which offers free wireless access, working his laptop computer, earning Bitcoins that can be converted into gift cards with an app called Gyft. The gift cards can be used to buy food or order pizza, which is delivered to Jesse and his friends in the park.

When he needs to charge his laptop or smartphone he can do that at a nearby public library.

It’s not exactly a get-rich-quick scheme, however, but it’s legal and beats the heck out of hassling people for donations. It’s a lot less embarrassing, he added.

For every YouTube video he watches on his laptop, Jesse earns 0.00004 Bitcoins (about half a cent). He can watch up to 12 videos a day. A mobile app called Bitcoin Tapper gives him 0.000133 Bitcoins a day for tapping on an icon over and over. Since obtaining a Bitcoin wallet three months ago, he has earned four to five Bitcoins, worth about $600 (the value of Bitcoins fluctuates wildly).

Being paid in Bitcoins, he doesn’t have to worry about being beaten and robbed. And he didn’t need an ID or street address to obtain a Bitcoin wallet.

Angle learned about Bitcoin through Sean’s Outpost, a Pensacola charity that has raised about $32,000 through a program that solicits donations in Bitcoins rather than dollars. So far, it has received donations from 25 different countries, and this has bought almost 16,000 meals for Pensacola homeless.

Angle said, “We’re kind of the homeless geeks. We all got laptops and smartphones.”

real-time currency for international commerce."

The company described itself as the Internet's largest payment processor and offered its services to people across the globe, including an estimated 200,000 in the U.S. However, it failed to register with the U.S. Treasury Department as a money-transmitting business and was operating without even the basic anti-money laundering controls, such as know-your-customer procedures.

The online criminal activity included credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking. The company processed more than 12 million financial transactions per year. The currency users of Liberty Reserve included traffickers of stolen credit card data and personal identity information; peddlers of various types of online Ponzi and get-rich-quick schemes; computer hackers for hire; unregulated gambling enterprises; and underground drug-dealing websites.

Kats left Liberty Reserve in 2009 in a dispute with the co-founder. The site was shut down in May 2013 when Kats was arrested and charged. Kats could face 75 years in prison. Charges against Kats' co-defendants are pending as of November 2013.

In response to the Kats case, supporters of Bitcoin declared that decentralized digital currencies such as Bitcoin are much more open to public compliance and investigation than centralized convertible digital currency systems such as Liberty Reserve. Bitcoin proponents also state that the seizure of the Silk Road online black market, which used Bitcoins for transactions, will now focus attention on the legal, legitimate uses of the Bitcoin virtual currency.

Litecoin emerges as alternative

Bitcoin gets the lion's share of attention in the virtual currency world but another similar system has emerged called Litecoin. Litecoin was created in 2011 by developer Charles Lee, who had noticed that Bitcoin mining was becoming more and more the providence of the few miners who could afford the most powerful computing rigs, a process which is tending to centralize the currency into the hands of a few. Bitcoin rigs now require application-specific integrated circuits, or ASICs. The ASICs in these computers are specifically hardwired to compute the Bitcoin SHA-256 hash.

Lee modified Bitcoin by replacing the hashing function with a more memory-intensive cryptographic algorithm called Scrypt. Because Litecoin requires more memory-intensive computing it is resistent to the ever more powerful ASIC chips devoted entirely to Bitcoin. Bottom line, Litecoin reverses the economic incentive to upgrade computing power.

"After ASICs came out, the Bitcoin difficulty shot up so high that it became less profitable to mine Bitcoins when compared to Litecoins. So they all switched over," says Lee. "For example, right now you can make more than six times as much money mining Litecoins as Bitcoins with GPUs. So pretty much every single GPU [mining rig] is mining Litecoins now."

None of the major online currency exchanges such as Bitstamp and Mt. Gox support Litecoin but that may soon change. The Litecoin network is scheduled to produce a total of 84 million currency units, four times as many as Bitcoin.

According to the Litecoin website, the Litecoin blockchain is capable of handling higher transaction volume than its Bitcoin counterpart. Due to more frequent block generation, the network supports more transactions without a need to modify the software in the future. As a result, merchants get faster confirmation times, while still having the ability to wait for more confirmations when selling bigger ticket items.

How Does Bitcoin Virtual Currency Work?

What is the future of Bitcoin and other virtual currencies? By just about any measure–the price listed by online exchanges, the number of new merchants accepting the cryptocurrency for goods and services, the transaction volume across the Bitcoin network–the system is gaining popularity.

People can use Bitcoins to buy goods and services online. At online exchanges, they can buy Bitcoins with U.S. dollars and convert Bitcoins into cash.

But how does Bitcoin work?

Bitcoin was invented in 2008 by a computer developer as a virtual currency controlled by mathematical equations and formulas. The integrity of the Bitcoin system and the means by which new Bitcoins are introduced into circulation is accomplished by "mining." Owners of powerful computers on the Bitcoin network use Bitcoin software to solve complicated mathematical equations which are used to verify merchandise transactions involving Bitcoins. The computer owner who solves the equation is awarded 25 Bitcoins.

According to the original Bitcoin equation, the number of Bitcoins that can be produced will end at 21 million. It is estimated that there are almost 12 million now in circulation.

The computing power needed to make a profit from Bitcoin mining is quickly accelerating, which is tending to push out the smaller miners. In recent months, this computing power doubled in a matter of weeks from what it had taken four years to amass. First-generation machines that once brought in a profit now fail to mine enough Bitcoins to pay for the electricity running them.

At least one Bitcoin miner has stated that local law enforcement mistakenly raided his residence, believing that the huge increase in his electric bills was due to an indoor marijuana grow rather than Bitcoin mining.

This centralizing trend may leave the stability and security of Bitcoin in the hands of fewer people and threaten the reputation of a currency that was designed to distribute power among the masses.

The increase came as mining rigs based on application-specific integrated circuits, or ASICs, hit the market. The ASICs in these computers are specifically hardwired to compute the Bitcoin SHA-256 hash. The big manufacturers are GlobalFoundries, Intel, and Taiwan Semiconductor Manufacturing Co.

Flaw found with Bitcoin?

There may be a flaw to Bitcoin, discovered by two computer science researchers at Cornell University, according to *Business Insider.* It has become so difficult and time consuming for a computer to create new Bitcoins, they reported, that some miners have banded together in pools, using multiple computers that work together. This can lead to a monopoly over the whole system. "… a minority group of miners can obtain revenues in excess of their fair share, and grow in number until they reach a majority. When this point is reached, the Bitcoin … the currency … is no longer decentralized; the controlling entity can determine who participates in mining and which transactions are committed, and can even roll back transactions at will.

The solution, the researchers said, is to change how Bitcoin mining works so that a single pool of miners can never control more than 25 percent of the available mining power.

Inside the code

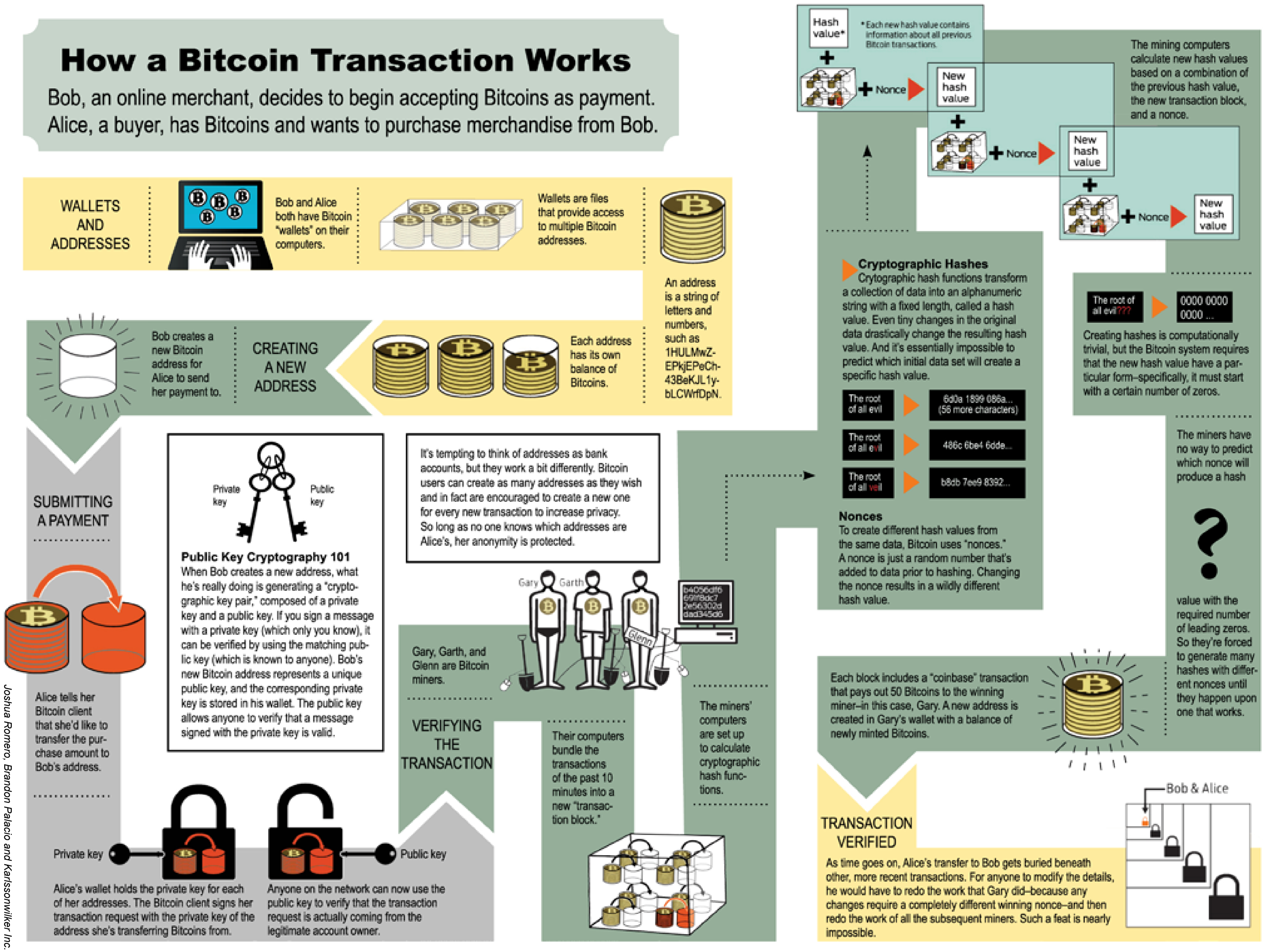
According to the CoinDesk online reference website, this is how Bitcoin mining works (also see explanatory charts on next two pages):

People are sending Bitcoins to each other over the Bitcoin network all the time, but unless someone keeps a record of all these transactions, nobody would be able to keep track of who had paid what. The Bitcoin network deals with this by collecting

Continued on page 17

How a Bitcoin Transaction Works

Bob, an online merchant, decides to begin accepting Bitcoins as payment. Alice, a buyer, has Bitcoins and wants to purchase merchandise from Bob.



WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZ-EPkjEPeCh-43BeKJL1y-bLCWrfDpN.

Each address has its own balance of Bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring Bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

Cryptographic Hashes
Crytographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil ▶ 6d0a 1899 086a... (56 more characters)

The root of all evil ▶ 486c 6be4 6dde...

The root of all veil ▶ b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

The root of all evil??? ▶ 0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form–specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 Bitcoins to the winning miner–in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted Bitcoins.

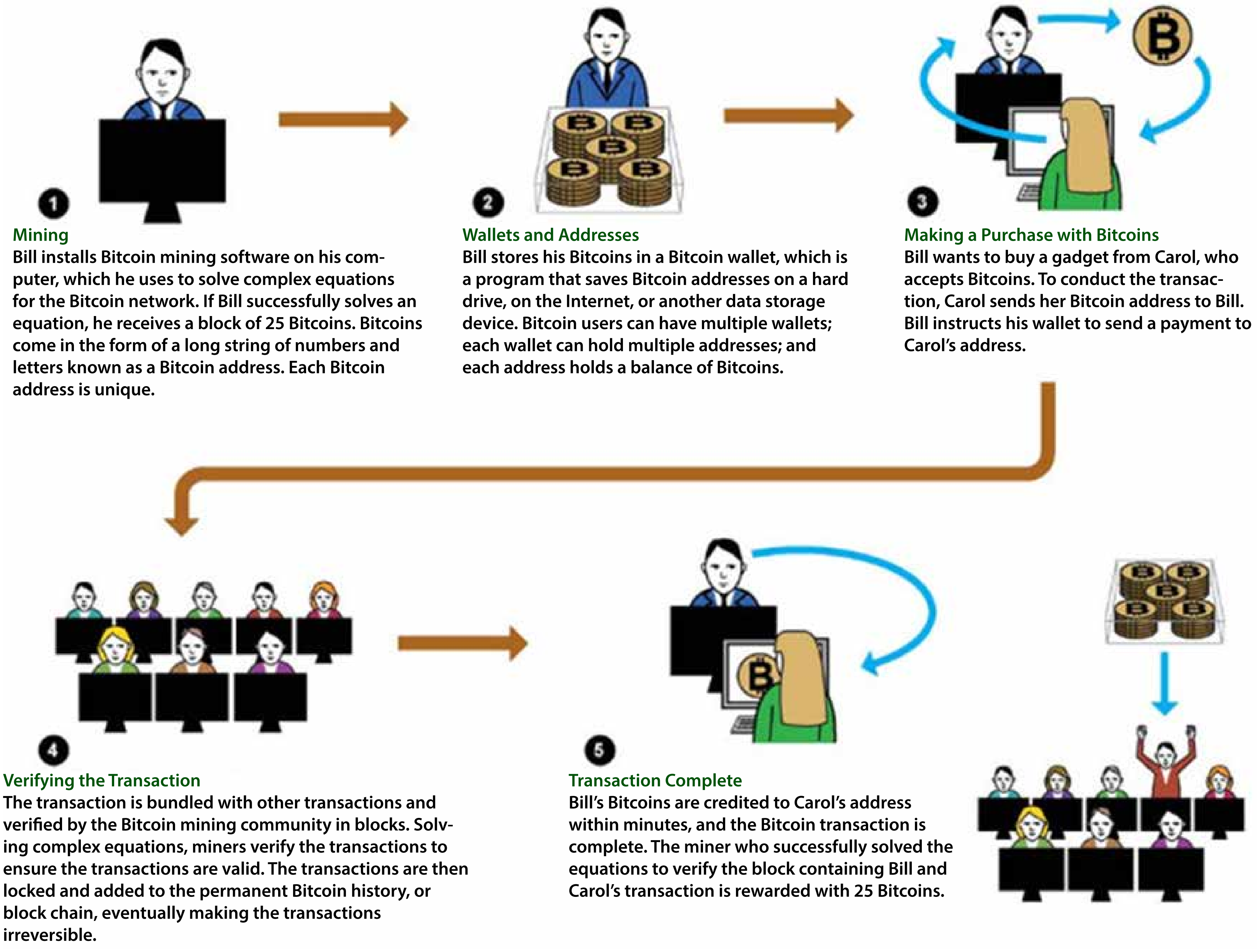
TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did–because any changes require a completely different winning nonce–and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

Joshua Romero, Brandon Palacio and Karlssonwilker Inc.

Bitcoins enter into circulation through a process known as mining.

A BITCOIN ADDRESS comprises a paired private key and a public key. The private key is stored in a wallet and known only to the bitcoin address owner, who uses the private key to conduct a transaction. The public key associated with the bitcoin address is public information. Bitcoin miners use the public key to verify a transaction is valid, which avoids double spending of a Bitcoin.



1 Mining

Bill installs Bitcoin mining software on his computer, which he uses to solve complex equations for the Bitcoin network. If Bill successfully solves an equation, he receives a block of 25 Bitcoins. Bitcoins come in the form of a long string of numbers and letters known as a Bitcoin address. Each Bitcoin address is unique.

2 Wallets and Addresses

Bill stores his Bitcoins in a Bitcoin wallet, which is a program that saves Bitcoin addresses on a hard drive, on the Internet, or another data storage device. Bitcoin users can have multiple wallets; each wallet can hold multiple addresses; and each address holds a balance of Bitcoins.

3 Making a Purchase with Bitcoins

Bill wants to buy a gadget from Carol, who accepts Bitcoins. To conduct the transaction, Carol sends her Bitcoin address to Bill. Bill instructs his wallet to send a payment to Carol's address.

4 Verifying the Transaction

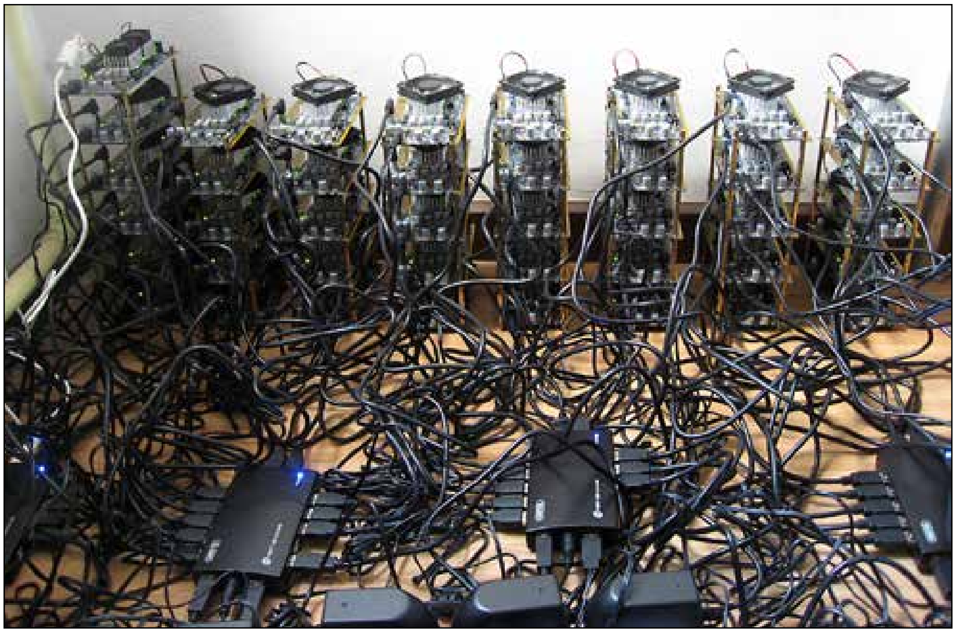
The transaction is bundled with other transactions and verified by the Bitcoin mining community in blocks. Solving complex equations, miners verify the transactions to ensure the transactions are valid. The transactions are then locked and added to the permanent Bitcoin history, or block chain, eventually making the transactions irreversible.

5 Transaction Complete

Bill's Bitcoins are credited to Carol's address within minutes, and the Bitcoin transaction is complete. The miner who successfully solved the equations to verify the block containing Bill and Carol's transaction is rewarded with 25 Bitcoins.

all of the transactions made during a set time period into a list, called a block. It's the miners' job to confirm those transactions, and write them into a general ledger.

This general ledger is a long list of blocks, known as the block chain. It can be used to explore any transaction made between any Bitcoin addresses, at any point on the network. Whenever a new block of transactions is created, it is added to the block chain, creating an increasingly lengthy list of all the transactions that ever took place on the Bitcoin network. A constantly updated copy of the block is given to everyone who participates, so that they all know what is going on.



Bitcoin mining rig

But a general ledger has to be trusted, and all of this is conducted and stored digitally. How can everyone be sure that the block chain stays intact, and is never tampered with? This is where the miners come in.

When a block of transactions is created, miners put it through a process. They take the information in the block, and apply a mathematical formula to it, turning it into something else. That something else is a far shorter, seemingly random sequence of letters and numbers known as a hash. This hash is stored along with the block, at the end of the block chain.

Hashes have some interesting properties. It's easy to produce a hash from a collection of data like a Bitcoin block, but it's practically impossible to figure out what the original data was just by looking at the hash. And while it is easy to produce a hash from a large amount of data, each hash is unique. If you change just one character in a Bitcoin block, its hash will change completely.

Miners don't just use the transactions in a block to generate a hash. Some other pieces of data are used too. One of these pieces of data is the hash of the last block stored in the block chain.

Because each block's hash is produced using the hash of the block before it, the hash becomes the digital version of a wax seal. It confirms that this block – and every block after it – is legitimate, because if you tampered with it, everyone would know.

If you tried to fake a transaction by changing a block that had already been stored in the block chain, this would change that block's hash. If someone checked the block's authenticity by running the hashing function on it, they'd find that the hash was different from the one already stored along with that block in the block chain.

Because each block's hash is used to help produce the hash of the next block in the chain, tampering with a block would also change the next block's hash. So tampering with a block would make the subsequent block's hash wrong, too. That would continue all the way down the chain, throwing everything out of whack.

Glossary of Terms

Bitcoin: A decentralized virtual currency created in 2008 which ensures a high degree of anonymity to users.

Bitcoin wallet: A data file that stores bitcoin currency. A user downloads software to a personal computer or may use an online, third-party provider to create a wallet (often called an eWallet) to store bitcoins.

Botnets: Any group of two or more computers and/or mobile devices that are controlled and/or updated remotely for an illegal purpose. Botnets can be used to perform denial-of-service attacks, send spam email, host illegal content, and may aid in other types of online criminal behavior.

Carding: The act of trafficking and/or fraudulent use of stolen credit card account information.

Decentralized: No central administration, issuing authority, or database.

Cyber underground: The extensive network of members engaged in cyber crime who have a unique language, an underground economy, a set of expectations about its members' conduct, and a social hierarchy based on knowledge, skill, and activities.

Electronic payment systems: Provide a secure means of transferring money among parties to facilitate e-commerce and operate using real money or virtual currency. Electronic payment systems either allow payment to be made between users, vendors, and other merchants, or they only allow payments to be made between users or accounts. There is both a regulated sector and a sector operating outside regulatory systems.

Exchangers: Online entities that, for a fee, convert cash, virtual currency, or digital gold currency into the type of currency requested. In general, individuals must use an exchanger to deposit money into an electronic payment system account, unless the electronic payment system has a physical location. Due to this fact, exchangers are a vital part of the money flow process for electronic payment systems and virtual currencies.

Fiat currency: Money that has value solely due to government regulation or law. Most modern currencies, such as the U.S. dollar and the Euro are fiat currencies.

Freenode: An open-source, software-focused Internet relay chat network.

Hacktivists: Individuals or groups who attack computer systems to draw attention to a particular issue, influence public opinion, or punish entities who oppose their ideological positions.

Internet Relay Chat (IRC): A form of real-time Internet chatting or synchronous conferencing. Mainly designed for group communication in discussion forums called channels, but also allowing one-to-one communication via private messages.

Malware or malicious software: Computer software that facilitates illicit activities, to include data exfiltration, denial-of-service

Glossary of Terms

attacks, fraud, and spam dissemination.

Mining, Bitcoin (also known as Bitcoin creation, Bitcoin generation, and Bitcoin manufacturing): The process of allowing the Bitcoin network to use a computer's resources in exchange for the possibility of earning bitcoins. The more computing power a user offers, the more likely they are to receive bitcoins.

Money Services Business (MSB): Any person doing business in one or more of the following capacities, wholly or in substantial part within the United States: 1) dealer in a foreign exchange; 2) check casher; 3) issuer or seller of traveler's checks or money orders; 4) issuer, seller, or redeemer of stored value; 5) money transmitter; 6) U.S. Postal Service (31 C.F.R 103.11).

Money transmitter: A person who provides money transmission services. Money transmission services means the acceptance of currency, funds, or other value that substitutes for currency and the transmission of currency, fund, or other value that substitutes for currency to another location or person by any means.

Peer-to-Peer (P2P): A type of network in which each workstation has equivalent capabilities and responsibilities. P2P is typically used for the transfer of data from one peer to another and are free programs that can be easily downloaded from the Internet. P2P file-sharing is the primary source for pirated software. Some popular examples include Limewire, Kazaa, and Gnutella.

Public Key Infrastructure (PKI): A framework for creating a secure method of exchanging information based on public key cryptography. PKI uses a certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet.

Real money: Coins or paper notes issued and backed by a government and used as a medium of exchange and measure of value.

Virtual currency: Something used on the Internet that is in circulation as a medium of exchange but is not backed by a government.

ZeuS Trojan: malicious software used by cyber criminals to steal online account credentials.

(Source: FBI)

Sources of Information

(All from Internet websites unless otherwise noted)

Bloomberg, “Bitcoin Foundation Meets With U.S. Regulators, Law Enforcement,” by Jesse Hamilton and Olga Kharif, Aug. 26, 2013

Business Insider, “Researchers say Bitcoin is broken and could collapse,” by Julie Bort, Nov. 4, 2013

CoinDesk, “Founder of Liberty Reserve admits guilt and faces 75 years in prison,” by Emily Spaven, Nov. 1, 2013

CoinDesk, “How Bitcoin mining works”

Criminal Complaint, U.S. v. Ross William Ulbricht, U.S. District Court, Southern District of New York, Sept. 27, 2013

DEA website, “Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of Silk Road Website,” Oct. 25, 2013

FBI Intelligence Assessment, “Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity,” April 24, 2012

Financial Crimes Enforcement Network, U.S. Treasury Dept., “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013

Forbes, “FBI Says It’s Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road,” by Andy Greenberg, Oct. 25, 2013

Forbes, “Meet the Dread Pirate Roberts, the man behind booming black market drug website Silk Road,” by Andy Greenberg, Aug. 14, 2013

Forbes, “What’s it like to buy drugs on three anonymous online black markets,” by Andy Greenberg, Aug. 14, 2013

IEEE Spectrum, “Bitcoin’s computing crisis,” by Morgen Peck, Oct. 31, 2013

New York Daily News, “So long, Silk Road,” by Winston Ross, Oct. 25, 2013

PCMag.com, “What was Silk Road and How Did It Work?” by Chloe Albanesuis, Oct. 3, 2013

Rusty Payne, DEA-Washington spokesman, phone interview, Nov. 6, 2013

Reuters, “Chip designers see dollar signs in Bitcoin miners,” by Noel Randewich, Nov. 3, 2013

The Security Ledger, “Beware Bitcoin users: the tax man cometh!” by Paul (NLN), June 18, 2013

The Verge, “After Silk Road’s demise, online drug dealing moves to new sites,” by Adrianne Jeffries, Oct. 4, 2013

Time magazine, “Online Drug Markets are alive and thriving,” by Christopher Matthews, Oct. 4, 2013

U.S. Department of Justice, “Tennessee Man Indicted in Romney Tax Return Fraud and Extortion Scheme,” June 26, 2013

U.S. Government Accountability Office, “Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks,” May 2013

USA Today, “Federal agents seize alleged Silk Road profits worth $35M,” by Donna L. Leger, Oct. 26, 2013

USA Today, “How FBI brought down cyber-underworld site Silk Road,” by Donna L. Leger, Oct. 22, 2013

Venturebeat.com, “John McAfee’s plan to build a million tiny darknets, foil the NSA, & give everyone free music,” by John Koetsier, Sept. 30, 2013

Wall Street Journal, “Bitcoin and the Rise of a Digital Counterculture,” by Paul Vigna, July 31, 2013

Wall Street Journal, “Bitcoin Equals Money, Says Judge,” by Robin Sidel, Aug. 7, 2013

Wall Street Journal, “Bitcoin Poses a Challenge for Law Enforcement: Rise of Virtual Currency Makes It Harder for Officials to Track Criminal Activity,” by Danny Yadron and Devlin Barrett, Oct. 22, 2013

Wall Street Journal, “Bitcoin Rebounds After Plunge on Silk Road Charges,” by Andrew R. Johnson, Oct. 3, 2013

Wall Street Journal, “Darkmail pushes privacy,” by Danny Yadron, Oct. 30, 2013

Wall Street Journal, “Feds Nab Alleged Leader of Silk Road Online Drug Market,” by Danny Yadron, Oct. 2, 2013

Washington Post with Bloomberg, “Silk Road ‘Pirate’ Accused of Running Online Drug Market,” by Bob Van Voris, Oct. 2, 2013

Wired magazine, “Homeless, Unemployed, and Surviving on Bitcoins,” by Daniela Hernandez, Sept. 20, 2013

Wired magazine, “Take a Tour of Robocoin, the World’s First Bitcoin ATM,” by Robert McMillan, Oct. 29, 2013

Wired magazine, “The Darkest Place on the Internet Isn’t Just for Criminals,” by Clive Thompson, Oct. 18, 2013

Wired magazine, “The Rise and Fall of Bitcoin,” by Benjamin Wallace, Nov. 23, 2011