A Brief Introduction to the Dark Web and Cryptocurrency

by Rahul Gupta and Josef Saar

The dark web and cryptocurrency are providing criminals with new ways to commit old crimes. When we think of traditional crime such as drug dealing, we envision a scene similar to one depicted in the HBO series, "The Wire." Drug dealers standing on a street corner conducting hand-to-hand transactions of drugs for cash while the police conduct surveillance, listen in on a wire, and wait to take down the dealers. In this scenario, the police have a physical location with live suspects, hard cash to seize, and a telecommunications provider upon whom they have served a wiretap order.

Now imagine a completely digital, criminal marketplace where any type of illegal good or service is available anonymously to anyone online at any time, and the contraband can be delivered by mail anywhere in the world. A specialized, free software allows the buyer and seller to remain anonymous so they never physically meet or even speak on the phone, and payments are made using digital cash making them difficult to trace. In this scenario, the police have no physical location or suspects to observe; there is no tangible money; and there is no telecommunications provider to serve

Rahul Gupta is a senior deputy district attorney in Orange County's Major Fraud–Cyber Crime Unit. He is also co-chair of CDAA's High-Tech Crimes Committee.

Josef Saar is a detective in the Costa Mesa Police Department's Special Investigations Unit.

legal process. This latter scenario is no longer imaginary, it is reality and it is happening on the dark web.

In 2017, the FBI and Europol "shut down Alphabay and Hansa, two of the largest dark web marketplaces responsible for the trading of over 350,000 illicit goods like drugs, firearms and cybercrime tools, such as malware."[1] In May 2019, the FBI shut down the Wall Street Market (WSM) on the dark web, which allowed approximately 5,400 vendors to sell illegal drugs, counterfeit goods, and malware to approximately 1.15 million customers around the world.[2]

Ironically, the driving force behind the development of the dark web and cryptocurrency was protecting individual privacy and anonymity on the web. Privacy and anonymity online are like two sides of the same digital coin. When the twin technologies of the dark web and cryptocurrency are combined, they significantly decrease the ability to track a person's online activity, thus increasing the privacy and anonymity of any online transaction. As a result, these digital privacy tools have encouraged digital criminal markets to flourish on the dark web, making it harder for law enforcement to stop illegal activity.

This article provides prosecutors with a brief introduction about the origins, terminology, and technology behind the dark web and cryptocurrency to promote a basic understanding of an emerging global criminal trend.

The Internet Versus the World Wide Web

To understand the dark web, it is important to first explain the distinction between the Internet and the World Wide Web (web). The terms "Internet" and "web" are often used interchangeably, but they are actually very different.

The Internet

The Internet is the backbone over which we transfer almost all of the digital data we consume online and use every day. It is the actual hardware infrastructure "in which any computer can communicate with any other computer as long as they are both connected to the internet."[3] The Internet is a public network that any computer can join or exit at any time. This ease of access comes at a cost of privacy and anonymity. An Internet Protocol (IP) address is a unique number assigned to a computer or server to access the

Internet and communicate with other computers. IP addresses can either be dynamic or static.

> An IP address is "dynamic" if a user's internet service provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. An IP address is "static" if a user's ISP assigns a particular IP address to the user's computer which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.[4]

The uniqueness of an IP address allows businesses and law enforcement to identify a particular computer's online activity or a specific server on a network. A marketing company can use IP address information for location-based advertising, while law enforcement can use it as a basis to serve a search warrant to the ISP to reveal the subscriber information associated with the IP address. When data travels over the Internet, the IP address is generally not private or anonymous and can identify a computer on the network.

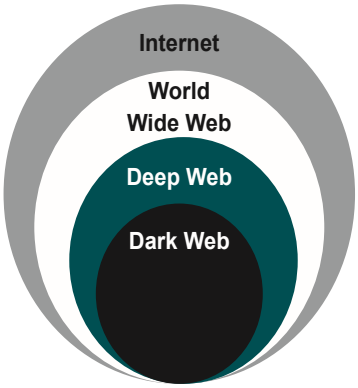
> ***Practice Tip***: A valid surface web (see below) IP address will always resolve back to an ISP and is the primary tool used by law enforcement to identify a computer used in traditional crimes. It does not put your suspect "behind the keyboard," but assists you with identifying a location associated with a potential suspect.

The World Wide Web

The web "is a way of accessing information over the medium of the internet."[5] The web uses browsers, "such as Internet Explorer or Firefox, to access ... web pages that are linked to each other via hyperlinks."[6] The web is built on top of the Internet to move data, pictures, videos, and text. Email, instant messaging, and voice over IP (VOIP) phone calls are distinct applications from the web also built on top of the Internet to transfer data from one computer to another.[7] Regardless of whether data travels over the Internet as part of the web, email, or VOIP, each computer connected to the Internet is assigned a unique IP address.

Layers of the Web

The earlier distinction between the Internet and the web was important because the dark web is just one of three distinct layers of the web: The top layer is the surface or clear web; the middle layer is the deep web, and inside the deep web is the dark web. Each layer of the web has varying levels of protection for a user's online privacy and anonymity.



Source: Kristen Finklea, *Dark Web* (Mar. 10, 2017) Congressional Research Service, p. 3 <*https://fas.org/sgp/crs/misc/R44101.pdf*> (accessed Sep. 20, 2019).

Practice Tip: Think of the World Wide Web as a series of concentric circles. Imagine a large circle representing the surface web, which contains a mid-sized circle that represents the deep web, which in turn contains an even smaller circle that represents the dark web.

The Surface Web

The surface or clear web is what most people around the world use every day when typing a simple Google search. The surface web is the collection of web pages publicly accessible and indexed by a search engine. Indexing means sites such as Google have specifically searched the entire web to identify and catalog specific web pages so they will appear as relevant search results on their search engine. These web pages can be viewed by anyone using a web browser. Even though a Google search may return millions of search results, the surface web actually comprises the smallest part of the web at less than four percent.[8]

The surface web typically provides the least amount of privacy and anonymity. When using the surface web, your ISP can see your IP address, view your web traffic content, record the websites you visit, and the type of computer and browser you use. Additionally, your web browser may also record websites you visit and retain passwords and items you searched. Lastly, the search engine or websites you visit may track all of the above information, in addition to any cookies that allow them to extract even more

personal data you are willing to share. The default setting of a typical web browser or search engine usually provides very little privacy and anonymity. This can be beneficial for law enforcement but detrimental for privacy advocates or criminals.

The Deep Web

The next layer of the web is the deep web, which is the opposite of the surface web. The deep web is the largest portion of the web, comprising almost 90%.[9] It consists of web pages not indexed by any search engine. Most of the data stored on the Internet is part of the deep web.

For example, think of all the private information accessed using the web that cannot be found using a Google search—a person's bank records, medical records, personal emails, work emails, private intranets at corporations, databases at government agencies or universities, or any commercial databases like Lexis Nexis or Westlaw.[10] The surface web can be used to locate the main website or web page of data stored on the deep web, but not the data behind the password or login needed to view the data.

The Dark Web

For many, just the term dark web conjures up images of a destination rife with danger. The dark web is considered "dark" because the web pages cannot be indexed or accessed without a special software and therefore are hidden from Google and standard web browsers. However, as previously discussed, we are just exploring the different layers of the web people use every day. Thus, the dark web is a very small subset of the deep web, estimated to be less than .01%.[11]

There is nothing inherently illegal or dangerous about the dark web, it is just another way to access and transfer data over the Internet. Similar to the deep web, web pages on the dark web are not indexed by any search engine and thus not publicly accessible to the average user like the surface web. In fact, the key attribute of the dark web is that it can only be "accessed through special network-routing software, which is designed to provide anonymity for both visitors to websites and publishers of these sites."[12] The most common specialized network software used to access the dark web is The Onion Router (TOR).[13]

> ***Practice Tip***: A key indicator that you are on the dark web is if the webpage ends in .onion.

The Onion Router (TOR)

The TOR software was originally developed by the U.S. Naval Research Laboratory in the mid-1990s to provide privacy and anonymity to U.S. military operatives communicating from abroad.[14] The TOR software is completely legal and can be downloaded by anyone for free.[15] The software is comprised of two components: the TOR browser and the TOR network. The TOR network allows users to build websites on the network known as "hidden services" that reside on the dark web.

Privacy and Anonymity

TOR is an open source software built on top of Mozilla's popular Firefox browser.[16] The software runs on a network of computers provided by volunteers around the world. Therefore, there is no central authority controlling the network or available to serve legal process.

> The TOR software permits a user to access the TOR network, a network of computers that obscures the identity of users by rerouting a user's IP address through "layers" of relay points, so that the IP address at which a signal exits (the "exit node") is not the IP address at which the signal originated. This process makes it impossible to "peel back the layers of the onion" to discover the originating IP address, which in turn marks the user's geographic location and can be used to identify the user.[17]

The TOR software does not collect any information that a typical browser or ISP may collect on a user's online activity, such as IP addresses, web content, or websites visited. Thus, TOR provides much higher privacy and anonymity than using a standard browser on the surface web.

The TOR Browser

The TOR browser is unique in that it can be used to visit websites on the surface web as well as on the dark web. Based on the TOR software that encrypts the user data and masks the user's true IP address, a user can visit websites on the surface web or dark web without fear of being tracked or identified. The TOR browser can be used for legal or illegal activity. A person using TOR is not indicative of any nefarious behavior. Many activists, journalists,

and privacy advocates who do not want their web activities tracked by corporations or the government may legitimately use the TOR browser to protect their privacy and anonymity.

These privacy features of the TOR browser also benefit those engaged in illegal activity, however. Unlike a typical web browser on the surface web that exposes digital user details, like an IP address, law enforcement cannot obtain a user's IP address when a suspect is using the TOR browser. Additionally, the user's own ISP would not even be able to track the IP address, the websites visited, or the contents of the user's web traffic.[18] Therefore, a search warrant to the ISP would not yield the crucial digital evidence to link the suspect to criminal activity on either the surface web or dark web.

Practice Tip: A TOR browser:

1. Encrypts a user's web traffic and data.
2. Masks a user's true IP address.
3. Allows users to visit surface websites and avoid being tracked.
4. Creates anonymity between the visitor to a website and the website provider.
5. Has no centralized authority controlling the network to serve with a search warrant.

TOR's Hidden Services

Websites accessible only on the TOR network, termed "hidden services," are not searchable through Google or other search engines. Rather, a user must employ the TOR software and know the exact address of a particular hidden service to access it.[19] Websites on the surface web have domain names that end in .com or .org. Dark web pages on the TOR network will have unique randomized alphanumeric addresses that will always end in the ".onion" domain. Finding a website on the dark web can be challenging, but there are many regular websites that will list the most recent .onion website listings. The most popular is *https://thehiddenwiki.org/*. Otherwise, you must know the exact hidden service to access it on the dark web.

The TOR network can be used for both legal and illegal purposes. Many legitimate businesses from Facebook to the *New York Times* operate .onion websites on the TOR network.

However, just as the TOR browser protects the anonymity of the user, the TOR network also protects the anonymity of .onion website operators, and this combination of website operator and user anonymity is what makes the dark web ideal for criminal activity.[20]

> ***Practice Tip***: There are many types of legitimate TOR users, including:
>
> 1. government agents
> 2. journalists
> 3. citizens under repressive regimes
> 4. whistleblowers
> 5. privacy advocates
> 6. anonymous web surfing

Dark Web Markets

The dark web created a perfect way for criminals to find each other and engage in illegal activity while remaining anonymous. To conduct illegal online transactions, however, a medium of exchange was still needed. Using traditional currency, credit cards, or any centralized payment system would create a financial trail that would defeat all the benefits of privacy and anonymity of the dark web. The missing link to allow dark web markets to flourish was cryptocurrency.

Cryptocurrency

Cryptocurrency, especially bitcoin, has come to the public's attention for two reasons: extreme price volatility and association with criminal activity on the dark web. Because bitcoin is the most commonly used cryptocurrency on the dark web,[21] this article highlights its unique features, which in many ways are similar to other types of cryptocurrencies available. Bitcoin itself is not illegal or criminal in any way. Much like TOR, bitcoin is a new technology prized by advocates of digital privacy and anonymity. Before we can fully understand bitcoin and cryptocurrency, however, we must explain the distinction between tangible and intangible currency.

The Federal Reserve

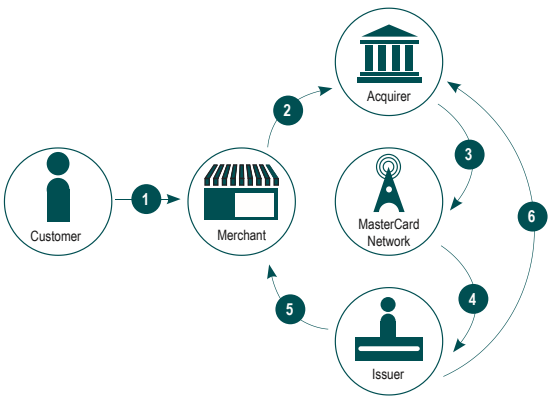
In most developed countries, including the United States, currency is tangible and issued by the government. In the United States, the Federal Reserve is the governing authority for banks

and the U.S. dollar. After the financial crises of 2008, the Federal Reserve helped the economy recover by printing more money to bail out big banks. Many, including a group of people known as "Cypherpunks,"[22] believed this gave the government too much control over our financial system and could lead to unchecked currency debasement. The Cypherpunks wanted to create a digital currency that was independent of any government control and in which the identity of the buyer and seller could remain anonymous. Thus, privacy and anonymity were key elements behind the digital cash movement.

Physical Cash Versus Digital Cash

When two individuals conduct a financial transaction using cash, cash from person A goes to person B. The unit of value is simply transferred from one entity to another without the need for a third party to verify the transaction. The downside of using cash, however, is that each individual involved must be physically present at the time of the transaction.

The use of electronic payment methods enable us to conduct financial transactions without being physically present. In order to complete these transactions, however, a third party is required in order to verify them. This third party, or central authority, can be a bank or another entity such as Visa or Mastercard. Centralized systems require *trust* in the third party. Centralization, however, leaves the system vulnerable to technical issues, hacks, and corruption, among other things. As an example of the electronic payment system, take a look at Mastercard's process:



Step 1: The customer pays with MasterCard
The customer purchased goods/services from a merchant.

Step 2: The payment is authenticated
The merchant point-of-sale system captures the customer's account information and securely sends it to the acquirer.

Step 3: The transaction is submitted
The merchant acquirer asks MasterCard to get an authorization from the customer's issuing bank.

Step 4: Authorization is requester
MasterCard submits the transaction to the issuer for authorization.

Step 5: Authorization response
The issuing bank authorizes the transaction and routes the response back to the merchant.

Step 6: The payment is authenticated
The issuing bank routes the payment to the merchant's acquirer who deposits the payment into the merchant's account.

Source: <*https://www.mastercard.us/en-us/merchants/start-accepting/payment-process.html*> (accessed Sept. 20, 2019).

Keep in mind that third parties do not work free, and the cost of payment processing is passed down the chain. While the customer and merchant will not see the processing fees upfront, the fees are paid nonetheless.

Bitcoin: *A Peer-to-Peer Electronic Cash System*

On October 31, 2008, Satoshi Nakamoto published a nine-page white paper titled, "Peer-to-Peer Electronic Cash System."[23] Nakamoto, who has never been positively identified, began the paper by explaining the problems with the legacy financial system. He went on to proclaim, "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[24]

In the paper, Nakamoto laid out the vision for his electronic cash system, which he named "Bitcoin." Nakamoto cited previous attempts at creating electronic payment systems and explained how Bitcoin solved the issues preventing their success/adoption. The first bitcoins were generated through a process called "mining" on January 3, 2009.

Nathaniel Popper of the *New York Times* explained:

> Rather than relying on a central bank or company to issue and keep track of the money—as the existing financial system… did—this system was set up so that every Bitcoin transaction, and the holdings of every user, would be tracked and recorded by the computers of all the people using the digital money, on a communally maintained database that would come to be known as the blockchain.[25]

Note: Merriam-Webster defines blockchain as "a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network."

What Makes Bitcoin Different?

In simplified terms, Bitcoin allows a user to send and receive electronic currency without the use of a central authority. This may not seem like a big deal for those of us fortunate to live/work in developed countries like the United States, but for people living in developing countries, cryptocurrencies like Bitcoin can be a

game-changer. Consider what is required to open a bank account in the United States: multiple forms of identification, a social security number, proof of residency, etc. Individuals in a developing country may not have the ability to open a bank account, which precludes them from participating in the global financial system. Because bitcoin has no such requirements, anyone in the world can send and receive bitcoin at any time.

Characteristics of Bitcoin

1. Bitcoin is a digital cash. There is no physical representation of bitcoin. It is all based on computer software, which is known as the Bitcoin network or protocol.
2. Bitcoin is peer-to-peer. The transactions are conducted without involvement of a third party. Furthermore, the Bitcoin network is decentralized, meaning that anyone in the world is capable of running a node. So long as one node is in operation, Bitcoin will continue to function. Therefore, it is nearly impossible to stop Bitcoin without spending an astronomical amount of money in order to take control of more than 51% of the nodes on the Bitcoin network.
3. Transactions are immutable. The underlying technology that powers bitcoin is called the blockchain. The blockchain is a distributed ledger that records each transaction. Once confirmed on the blockchain, a transaction cannot be altered, which greatly reduces chances of fraud. Additionally, the blockchain is public, which allows anyone in the world to view the entire history of recorded bitcoin transactions. For prosecutors and investigators, this can be extremely valuable.
4. Bitcoin is pseudo-anonymous. While the transactions are publicly visible on the blockchain, there is not necessarily anything tying a specific user to a specific transaction.
5. There is a fixed supply of bitcoins. Only 21 million bitcoins will ever be created, i.e.,"mining." The last bitcoin will be mined around the year 2140.
6. A single bitcoin (BTC) is divisible up to 100 million units (e.g., 0.01190634 BTC). The smallest unit of bitcoin measurement is known as a "Satoshi." This is important to understand because an individual can own a small fraction of a bitcoin.

7. The Bitcoin network relies upon public key cryptography. Unlike classic banking in which an institution holds your money, Bitcoin allows the user to be in control of his or her own money.

Ways to Obtain Bitcoins

1. Purchase them from a cryptocurrency exchange such as Coinbase or Gemini. A cryptocurrency exchange functions somewhat like a bank: They can store your cryptocurrency (i.e., your private keys) for you. *Note*: Major cryptocurrency exchanges, including U.S.-based exchanges, are required to be in compliance with bank security laws, including Know Your Customer (KYC). This means they will have information about their clients that can be obtained via subpoena or search warrant.
2. Mine them. Cryptocurrency mining companies operate high-powered computer farms which run the Bitcoin protocol. Because of the advanced computing power currently required to mine bitcoins, this option is not really feasible for an individual person simply looking to obtain bitcoins.
3. Conduct a peer-to-peer exchange. In California, it is easy to trade cash for bitcoin. This is currently being done on a regular basis in order to avoid the bank security laws (as well as tax filings) that would come into play when an individual uses one of the bitcoin exchanges mentioned earlier. Technically, an individual who trades bitcoin for cash without filing with the Financial Crimes Enforcement Network (FinCEN) is operating as an illegal money services business and is in violation of title 18 United States Code section 1960.
4. Find a cryptocurrency ATM. Deposit cash and have your bitcoin sent directly to your mobile wallet. Visit *coinatmradar.com* to find an ATM location near you.

Bitcoins will be sent to you and stored on a bitcoin address. The address is a string of 25–36 alphanumeric characters (e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa). Addresses are considered pseudo-anonymous and do not store personally identifying information (PII). Addresses are stored on bitcoin wallets. Wallets can be used on various platforms including mobile

phones (e.g., MyCelium), desktops (e.g., Electrum), or cloud (e.g., Blockchain).

Note: *Consumer Reports* released a detailed primer on Bitcoin and its characteristics, further detailing the cryptocurrency's origin and how to obtain them.[26]

To be clear, Bitcoin and its underlying technology has many legitimate and lawful uses. Because of the public nature of the Bitcoin blockchain, Bitcoin payments can easily be tracked using some type of blockchain analysis. As such, in terms of anonymity for nefarious transactions, cash is still king. There are, however, five common criminal activity uses of bitcoin to be aware of:

1. dark web markets
2. money laundering
3. blackmail/extortion
4. ransomware
5. hacking (bitcoins are usually the targets of hacks and scams)

Case Study: *The Silk Road*

In 2011, Ross William Ulbricht[27] launched a hidden service on the TOR network named the Silk Road. By the time it was seized by federal law enforcement in October 2013, it was estimated that the Silk Road was generating $100 million a year in revenue.[28] The investigation led to indictments of drug vendors throughout the world, as well as the arrests of two federal law enforcement agents. This case is important for prosecutors and law enforcement to be aware of for several reasons:

1. The Silk Road was the first drug market of its kind.
2. New (active) markets are similar in design and use to the Silk Road.
3. The Silk Road is a litigated case.[29] It can be read, cited, and used for training/experience.
4. Bitcoin was seized and forfeited by the federal government.

Ulbricht, who embraced libertarian philosophies, developed the concept for an online drug bazaar in part after reading *A Lodging of Wayfaring Men*, a novel about a group that creates an online society free from government control, which eventually grows so large that the government takes action to try and stop them. The issue, however, was that there was no way to conduct anonymous

The Anatomy of a Dark Web Market Transaction

1. Download and run the TOR browser.
2. Locate the URL (hidden service) for your desired dark web market.
3. Create an account with the dark web market.
4. Browse the listings for your desired contraband.
5. Once located, add the item to your cart just like you would with Amazon.
6. Load cryptocurrency (most commonly Bitcoin) onto your account's wallet.
7. Enter the shipping location. This information is commonly encrypted using PGP so that only the vendor will be able to view it.
8. Confirm the purchase. Your bitcoin will now be held in escrow for a period of time determined by the dark web market. This allows buyers to open a dispute and get their money back if their item never arrives due to seizure or scams.

Privacy and Anonymity

After completing the transaction, the buyer simply waits for the contraband to arrive through the mail. Often nothing arrives, because the seller executed a simple scam. Other times the contraband arrives as promised. Either way, on dark web markets buyers and sellers can leave ratings and comments about each other, the transaction process, and quality of the contraband.

If the vendor perpetuates a scam, a negative review will deter future sales. If the contraband is high quality, a positive review can generate more sales. Since privacy and anonymity of the buyer and seller is the primary concern throughout the transaction, the ability to read reviews of prior sales provides a means to make informed decisions about dark web market purchases. When buying illegal items in a criminal marketplace there is distrust on both sides of the transaction.

Much like on Amazon or eBay, buyer and seller ratings on a dark web market create an instant level of online trust. The combination of cryptocurrency and the dark web have created an anonymous and seamless digital platform for online criminal activity.

financial transactions online. This changed in 2010 when Ulbricht discovered Bitcoin. That summer, he began developing the Silk Road. It was officially launched in January 2011.

Ulbricht began growing psilocybin mushrooms and selling them on the site, which could be accessed by entering the URL "tydgccykixpbu6uz.onion" into the TOR browser. Ulbricht generated interest in the site by posting about it on online forums. By June 2011, the site had over 300 listings for various types of narcotics. In that month, an article was released in the online blog *Gawker*,[30] which covered Silk Road and even included a conversation the author had with the Silk Road administrator. The article was later updated with a statement from Jeff Garzik, a Bitcoin developer, which is of particular note to prosecutors and law enforcement:

> [B]ecause all Bitcoin transactions are recorded in a public log, though the identities of all the parties are anonymous, law enforcement could use sophisticated network analysis techniques to parse the transaction flow and track down individual Bitcoin users. 'Attempting major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb.'[31]

Within days of the *Gawker* article, Senator Chuck Schumer (D-NY) held a press conference calling for federal authorities to shut down the site. In the following months, the Marco Polo Task Force was formed with the intent to shut down the Silk Road. The task force consisted of the Drug Enforcement Administration (DEA), Homeland Security Investigations (HSI), the U.S. Postal Inspection Service (USPIS), the Secret Service, the Internal Revenue Service (IRS), and the Federal Bureau of Investigation (FBI).

Carl Force, a DEA agent, created an undercover account and began communicating directly with Ulbricht, who himself had begun using the moniker "Dread Pirate Roberts" from *The Princess Bride*. Force, using the moniker "Nob," built a rapport with Ulbricht over the span of several months. Eventually, Ulbricht brokered a deal for Force to purchase a kilogram of cocaine for $27,000. The cocaine would be shipped via USPS to a middleman by the name of Curtis Green (aka, "Flush") in Utah. In addition to selling drugs on the Silk Road, Green worked for Ulbricht as a moderator on the Silk Road.

Force and other federal agents, including Secret Service Agent Shaun Bridges arranged for a controlled delivery (CD) of the cocaine to Green. After accepting the parcel, the agents served a search warrant and took Green into custody. Green cooperated with the investigation, which allowed Bridges and Force to access Green's moderator account on the Silk Road.

Ulbricht, having known the true identities of his employees, discovered through public records that Green had been arrested.[32] Ulbricht also discovered that Green's Silk Road account had stolen approximately $350,000 worth of bitcoin from the site. In retribution, Ulbricht paid $80,000 (in bitcoin) to Nob (Force) in order to have Green killed. This was to be the first of five murders Ulbricht would ultimately sanction in relation to the Silk Road. A staged photograph was sent to Ulbricht once the (staged) murder-for-hire had been carried out.[33]

In reality, Green had not stolen anything from Ulbricht. The theft had been committed by Bridges, who then funneled the bitcoins into his own personal accounts. Force, meanwhile, began to extort Ulbricht using other online aliases that were not documented in his case files. In addition, he sold Ulbricht information about the Silk Road investigation.

In May 2013, IRS Agent Gary Alford located an email address tied to one of the first Silk Road advertisements that Ulbricht had posted in the online forums. The email address had been deleted from the forums, but it was still retained in their database. The address was *rossulbricht@gmail.com*. After months of surveillance, arrests, and Silk Road account takeovers, federal agents arrested Ulbricht on October 1, 2013, at the Glen Park Branch of the San Francisco Public Library. At the time of his arrest, Ulbricht had been using his laptop on the library's public Wi-Fi. The federal agents were able to grab the laptop before it was locked and encrypted. In doing so, they found that Ulbricht was logged on the Silk Road under the moniker Dread Pirate Roberts.[34]

At the time of Ulbricht's arrest, the Silk Road had more than 10,000 different items available for purchase on the site, at least 70 percent of which were drugs.[35]

Ulbricht was charged and later convicted by a federal jury for the following:

> (1) distribution and aiding and abetting distribution of narcotics ... (2) using the Internet to distribute

> narcotics ... (3) conspiracy to distribute narcotics ... (4) engaging in a continuing criminal enterprise ... (5) conspiring to obtain unauthorized access to a computer for purposes of commercial advantage and private financial gain and in furtherance of other criminal and tortious acts ... (6) conspiring to traffic in fraudulent identification documents ... and (7) conspiring to launder money.[36]

Ulbricht was sentenced to life in prison.

Bitcoin Seizure

The FBI seized 144,336 bitcoins from Ulbricht. They were later forfeited and auctioned off for $48 million.[37] In July 2019, bitcoin was trading above $10,000 per bitcoin. That would make the seizure of 144,336 bitcoins worth more than $1.4 billion.

Force and Bridges

Before trial, the government purged any evidence that could be traced back to Carl Force. Force and Bridges subsequently pled guilty after their own indictments. Force received a 78-month sentence in federal prison. Bridges was sentenced to 71 months.

The unsealed criminal complaint—*United States v. Carl Mark Force IV and Shaun W. Bridges*—provides insight into how blockchain analysis can be done to effectively "follow the money." The affiant includes multiple spreadsheets and transaction logs that catalog where and when the bitcoins were transferred from Ulbricht and the Silk Road into the accounts belonging to Force and Bridges.[38]

Conclusion

Most investigators and prosecutors pursue careers in law enforcement to catch criminals, not to search and seize computers. The sheer thought of trying to understand another new technology such as the dark web or cryptocurrency in an era of information overload may feel daunting. Digital privacy and anonymity are important issues for everyone, however, and these new twin technologies are here to stay.

It may be beneficial to download TOR or purchase a small amount of bitcoin at a local ATM to help better understand these new technologies. Additionally, just as law enforcement has adapted to collecting and understanding DNA evidence, cell tower pings, and using Facebook, the dark web and cryptocurrency can also become familiar and useful. ■

ENDNOTES

1. Europol, "Crime on the Dark Web: Law Enforcement Coordination Is the Only Cure" (May 2018) [press release] <*https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure*> (accessed Sep. 24, 2019).
2. Brian Krebs, "Feds Bust Up Dark Web Hub Wall Street Market" (May 19, 2019) *Krebs on Security* <*https://krebsonsecurity.com/2019/05/feds-bust-up-dark-web-hub-wall-street-market/*> (accessed Sep. 24, 2019).
3. <*https://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp*> (accessed Sep. 24, 2019).
4. *United States v. Scanlon* (2017) WL3974031 [citations].
5. <*https://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp*> (accessed Sep. 24, 2019).
6. *Id.*
7. *Id.*
8. Bruce Sussman, "Dark Web vs. Deep Web: What Is the Difference?" (Aug. 15, 2018) *SecureWorld* <*https://www.secureworldexpo.com/industry-news/dark-web-vs-deep-web*> (accessed Sep. 24, 2019).
9. *Id.*
10. Kristin Finklea, *Dark Web* (Mar. 10, 2017) Congressional Research Service <*https://fas.org/sgp/crs/misc/R44101.pdf*> (accessed Sep. 24, 2019).
11. Michael Chertoff and Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security* (Feb. 2015) Global Commission on Internet Governance <*https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf*> (accessed Sep. 24, 2019).
12. Robert Gehl, "Illuminating the Dark Web" (Oct. 31, 2018) *Scientific American* <*https://www.scientificamerican.com/article/illuminating-the-dark-web/*> (accessed Sep. 24, 2019).
13. Mohd Faizan and Raees Ahmad Khan, *Exploring and analyzing the dark Web: A new alchemy* (2019) 24 First Monday 5 <*https://firstmonday.org/ojs/index.php/fm/article/view/9473/7794*> (accessed Sep. 24, 2019).
14. Chertoff and Simon, *The Impact of the Dark Web, supra*, p. 3.
15. <*https://www.torproject.org/download*> (accessed Sep. 24, 2019).
16. Dan Patterson, "Dark Web: A cheat sheet for business professionals" (Oct. 26, 2018) *Tech Republic* <*https://www.techrepublic.com/article/dark-web-the-smart-persons-guide/*> (accessed Sep. 24, 2019).
17. *United States v. Taylor* (N.D. Ala. 2017) 250 F.Supp.3d 1215, 1220.
18. Dennis Anon, "Everything you wanted to know about Tor but were afraid to ask" (Aug. 21, 2018) *Privacy.net* <*https://privacy.net/what-is-tor/*> (accessed Sep. 24, 2019).
19. *Taylor, supra*, at 1220.
20. Anon, "Everything you wanted to know about Tor," *supra*.
21. Chertoff and Simon, *The Impact of the Dark Web, supra*.
22. <*https://en.wikipedia.org/wiki/Cypherpunk*> (accessed Sep. 24, 2019).
23. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008) <*https://bitcoin.org/bitcoin.pdf*> (accessed Sep. 24, 2019).
24. *Id.* at p. 1.
25. Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (2016) Harper Paperbacks, pp. 20–21.

26. Octavio Blanco, "Still Confused About Bitcoin?" (Dec. 21, 2017) *Consumer Reports* <*https://www.consumerreports.org/cryptocurrency/still-confused-about-bitcoin/*> (accessed Sep. 24, 2019).
27. Ulbricht has also been known as "Dread Pirate Roberts" (DPR) and "Silk Road Admin." He was born on March 27, 1984.
28. Nick Bilton, *American Kingpin* (May 29, 2018) Penguin Random House.
29. *United States v. Ulbricht* (2d Cir. 2017) 858 F.3d 71.
30. Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable" (Jun. 1, 2011) *Gawker* <*https:// gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160*> (accessed Sep. 24, 2019).
31. *Id.*
32. Bilton, *American Kingpin, supra.*
33. No bodies were ever recovered, and it is unknown if any murders were ever actually committed. It is likely that Ulbricht was scammed by other would-be hitmen.
34. Because of encryption methods, investigators may not be able to crack and image a computer or smartphone's hard drive. Therefore, it may be necessary for you to develop a plan to catch your suspect in the act of accessing the hidden service, as was done against Ulbricht.
35. James Ball, "Silk Road: the online drug marketplace that officials seem powerless to stop" (Mar. 22, 2013) *The Guardian* <*www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace*> (accessed Sep. 24, 2019).
36. *Ulbricht, supra*, at 82, fn. 1.
37. Jeff John Roberts, "The Feds Just Collected $48 Million from Seized Bitcoins" (Oct. 2, 2017) *Fortune* <*https://fortune.com/2017/10/02/bitcoin-sale-silk-road*> (accessed Sep. 24, 2019).
38. We strongly encourage reviewing the court documents pertaining to the Silk Road investigation. In addition to highlighting an incredible investigation, the story itself will enhance the reader's understanding and appreciation of the concepts discussed in this article.