School of Law

University of California, Davis

400 Mrak Hall Drive

Davis, CA 95616

530.752.0243

http://www.law.ucdavis.edu

UC Davis Legal Studies Research Paper Series

Research Paper No. 462

October 2015

The Challenge of Bitcoin Psuedo-Anonymity To Computer Forensics

Jason Luu and Edward J. Imwinkelried

THE CHALLENGE OF BITCOIN PSEUDO-ANONYMITY TO COMPUTER FORENSICS

Jason Luu*

Edward J. Imwinkelried**

*J.D. University of California, Davis School of Law, 2015.

**Edward L. Barrett, Jr. Professor of Law Emeritus; University of California, Davis School of Law; coauthor, Giannelli, Imwinkelried, Roth & Campbell Moriarty, Scientific Evidence (5th ed. 2015).

This article is based largely on Mr. Luu's research paper in Professor Imwinkelried's Spring 2015 Scientific Evidence seminar.

As computer technology advances, digital forensics experts regularly encounter new challenges. One of the latest challenges is Bitcoin pseudo-anonymity. Fiat currencies such as American bills and coins are issued by national governments. In contrast, Bitcoin is an open-source, decentralized, peer-to-peer digital currency.[1] Bitcoin offers many legitimate benefits such as decentralization and pseudo-anonymity to participants in its economy. However, the same features that give rise to those benefits have attracted, or have the potential to attract, a variety of illegal activities such as money laundering and narcotics trafficking.[2] As criminal enterprises try to exploit the Bitcoin protocol, law enforcement authorities will turn to digital forensics experts to pierce Bitcoin's pseudo-anonymity.

To date, digital forensics experts have had few opportunities to deal with the challenges associated with Bitcoin. Due to the novelty of the currency and the difficulty of tracking Bitcoin transactions, there have been very few Bitcoin-related arrests. Nevertheless, a number of high-profile cases have focused digital forensics researchers' attention on the need to map Bitcoin transactions and identify suspects. In 2014, the head of a Bitcoin exchange was convicted of laundering money for Silk Road, an online black market that accepted bitcoin[3] payments.[4] In short order in 2015, the owner and operator

[1] Jerry Brito & Andrea Castillo, MERCATUS CENTER AT GEORGE MASON UNIVERSITY, *Bitcoin: A Primer for Policymakers* 3 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf. [hereinafter Brito & Castillo].
[2] FEDERAL BUREAU OF INVESTIGATION, *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity* 1 (April 24, 2012), http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf [hereinafter Federal Bureau of Investigation].
[3] Following convention, "Bitcoin" refers to the payment system and peer-to-peer network, whereas "bitcoin" refers to the unit of currency.
[4] James Cook, *'Bitcoin Millionaire' Charlie Shrem Sentenced to 2 Years in Prison*, BUSINESS INSIDER (Dec. 22, 2014, 5:06 AM), http://www.businessinsider.com/Bitcoin-millionaire-charlie-shrem-sentenced-to-2-years-in-prison-2014-12.

of Silk Road was sentenced as well.[5] These criminal cases have motivated researchers to investigate possible forensic methods to pierce the veil of pseudo-anonymity surrounding Bitcoin.

The first part of this article describes the advantages that Bitcoin offers to potential users. The second part identifies the primary dangers that Bitcoin poses. As the preceding paragraph suggests, one danger is that criminal elements will use Bitcoin to effect payments for illegal goods and services. Given that danger, digital forensics experts are attempting to develop techniques to identify the persons using Bitcoin. The third and fourth parts of the article describe those attempts. The third part dissects the Bitcoin protocol to set the stage for the fourth part of the article, a description of the new forensic techniques that have been proposed to identify Bitcoin users. The fifth and final part of the article evaluates the admissibility of testimony based on these new techniques under the *Frye* general acceptance standard and the *Daubert* empirical validation test. The article predicts that in the current state of the art, it will be difficult to justify admitting testimony resting on these novel techniques.

I. THE BENEFITS OF BITCOIN

In 2009, an unknown developer (or group of developers) named Satoshi Nakamoto[6] created Bitcoin as a response to one of the primary weaknesses of Internet commerce. More specifically, "[c]ommerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic

[5] Andy Greenberg, *Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges*, WIRED (Feb. 4, 2015, 3:57 PM), http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict [hereinafter Greenberg].
[6] The actual identity of "Satoshi Nakamoto" has never been confirmed. *See Who Is Satoshi Nakamoto?*, COINDESK (Mar. 20, 2015), http://www.coindesk.com/information/who-is-satoshi-nakamoto.

payments."[7] These trusted third parties are subject to government regulation, and the intervention of these third parties increases transaction costs between payer and payee. Third parties, such as PayPal, banks, or credit card networks, act as middlemen between payer and payee. Before Bitcoin, for any exchange to occur over the Internet, a payer had to go through a third-party in order to transfer money to a payee.

Moreover, prior to the advent of Bitcoin, the intervention of third parties was necessary to "keep a ledger of account holders' balances . . . Without such intermediaries, digital money could be spent twice."[8] For instance, if there were no third party intermediaries, Al could send $100 online to Beth--without a trusted ledger record of a debit from his account or a credit to Beth's account. Al could then send the same $100 amount to Claire--resulting in a double-spending problem.[9]

To address this double spending problem, the Bitcoin protocol eliminated the need for trusted third parties in Internet commerce. Instead of utilizing a centralized ledger maintained by a third party, the Bitcoin protocol decentralizes the ledger. In this new protocol, all Bitcoin participants have a complete copy of the same ledger to track debits and credits to ensure double spending does not occur. This ledger is called the *block chain*. Utilizing Bitcoin, a payer may transfer money directly to a payee without using an intermediary to track the debits and credits. The accounting function formerly handled by intermediaries is now performed by peers in the Bitcoin economy.

There are a number of important advantages to removing third party intermediaries from payment transactions by utilizing the Bitcoin protocol instead. These

[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 1 (2008), https://Bitcoin.org/Bitcoin.pdf.
[8] Brito & Castillo, supra note 1.
[9] Brito & Castillo, supra note 1.

advantages can be classified as financial benefits, political benefits, and pseudo-anonymity benefits.

A. Financial Benefits

Bitcoin lowers the transaction costs between businesses and consumers. Credit card transactions impose a number of fees on businesses, which are then passed on to consumers.[10] These fees include "authorization fees, transaction fees, statement fees, interchange fees, and customer-service fees" as well as fees associated with charge-backs.[11] Since transactional third parties are unnecessary in the Bitcoin economy, those associated fees are lessened or eliminated.[12] Businesses have lower overhead cost and can pass those savings on to consumers. Lower transaction fees may also make money transfers quicker and more affordable, particularly remittances between developed and developing countries.[13]

Bitcoin has the potential to bring banking services to the unbanked and underbanked populations of developed and developing countries. Unbanked populations lack checking, savings, or money market accounts.[14] In contrast, underbanked populations technically have access to checking, savings, or money market accounts but for a variety of practical reasons extensively use alternative financial services, such as

[10] Brito & Castillo, supra note 1, at 10-11.
[11] Brito & Castillo, supra note 1, at 10-12.
[12] Brito & Castillo, supra note 1.
[13] Brito & Castillo, supra note 1, at 13; *see also* Michael J. Casey & Paul Vigna, *Bitcoin For the Unbanked*, FOREIGN AFFAIRS (Feb. 26, 2015), http://www.foreignaffairs.com/articles/143162/paul-vigna-and-michael-j-casey/Bitcoin-for-the-unbanked [hereinafter Casey & Vigna].
[14] Matthew B. Gross, Jeanne M. Hogarth & Maximilian D. Schmeiser, BD. OF GOVERNORS OF THE FED. RESERVE SYS., *Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption* 3 (Sept. 2012), http://www.federalreserve.gov/pubs/bulletin/2012/pdf/mobile_financial_services_201209.pdf [hereinafter Gross, Hogarth & Schmeiser].

payday loans, title loans, or check-cashing services.[15] Hence, both unbanked and underbanked communities are underserved. Policymakers have recognized the need to improve access to mainstream financial services as a means to encourage savings and asset building, particularly in underserved communities both here and abroad.[16] Lacking effective access to mainstream financial services, both unbanked and underbanked populations are subject to greater cash-only transaction costs, higher interest rates on alternative financial services, and less statutory consumer protection.[17]

This lack of effective access is a major problem even in developed countries. In the United States, approximately 11 percent of consumers are unbanked; and another 11 percent are underbanked.[18] Among the most frequently cited reasons why these Americans are unbanked is their dislike of dealing with banks and being charged fees and service charges.[19] The magnitude of the problem is much larger in developing countries. 64 percent of adults in developing countries are estimated to be unbanked.[20]

Bitcoin may advance the policy goals of encouraging savings and asset building for underserved communities.[21] By circumventing banks and providing lower transaction costs, Bitcoin addresses many of the concerns voiced by unbanked Americans. If Bitcoin becomes more commonly accepted among merchants, unbanked Americans may find Bitcoin to be a more attractive alternative to traditional banking channels.

---

[15] Gross, Hogarth & Schmeiser, supra note 15.
[16] Casey & Vigna, supra note 13, at 2.
[17] Gross, Hogarth & Schmeiser, supra note 14.
[18] Gross, Hogarth & Schmeiser, supra note 14, at 1.
[19] Gross, Hogarth & Schmeiser, supra note 14, at 5.
[20] Oya Pinar Ardic, Maximilien Heimann & Nataliya Mylenko, THE WORLD BANK, *Access to Financial Services and the Financial Inclusion Agenda Around the World* 3 (Jan. 2011), https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf.
[21] For a discussion of challenges to bringing Bitcoin to unbanked populations, see Jason Tyra, *Can Bitcoin Deliver on Its Promise to the World's Unbanked?*, COINDESK (Aug. 2, 2014, 5:45 PM), http://www.coindesk.com/can-Bitcoin-deliver-promise-worlds-unbanked.

The advent of Bitcoin holds out even more promise to the underserved populations in developing countries. Developing countries must contend with numerous barriers that make the development of traditional branch banking expensive.[22] Bitcoin has the potential to altogether eliminate the need for branch banking and to extend banking services to these currently unbanked populations.[23]

B. Political Benefits

Although there are obvious financial advantages to the Bitcoin protocol, much of the rhetoric touting Bitcoin has been political in nature. In a statement before the United States Senate, the general counsel of the Bitcoin Foundation noted the "potential for Bitcoin to improve people's enjoyment of autonomy, liberty, and dignity everywhere in the world."[24] As noted security researcher, Dan Kaminsky, wrote, "Bitcoin . . . turns nerd forums into libertarian forums."[25]

Created in the aftermath of the Great Recession and a series of controversies regarding government surveillance, Bitcoin emerged at a time when distrust of government ran high.[26] To many, Bitcoin represents a way to avoid many of the problems associated with government and financial authorities. Because Bitcoin is an open-source economic system that participants choose to engage in, it has attracted people concerned about the effects of centralized financial control and surveillance. Bitcoin has the ability

---

[22] *See* Michael J. Casey & Paul Vigna, *Bitcoin For the Unbanked*, FOREIGN AFFAIRS (Feb. 26, 2015), http://www.foreignaffairs.com/articles/143162/paul-vigna-and-michael-j-casey/Bitcoin-for-the-unbanked [hereinafter Casey & Vigna].
[23] Casey & Vigna, supra note 22.
[24] Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the S. Comm. on Homeland Security and Government Affairs, 113th Cong. 6 (Nov. 18, 2013) [hereinafter *Hearing*] (statement of Patrick Murck, General Counsel, Bitcoin Foundation), *available at* http://www.hsgac.senate.gov/download/?id=4cd1ff12-312d-429f-aa41-1d77034ec5a8.
[25] Dan Kaminsky, *Plain Old Money Has Gotten Buggy*, CATO UNBOUND (July 11, 2013), http://www.cato-unbound.org/2013/07/10/dan-kaminsky/money-has-gotten-buggy.
[26] *See Public Trust in Government: 1958-2014*, PEW RESEARCH CENTER (Nov. 13, 2014), http://www.people-press.org/2014/11/13/public-trust-in-government.

to bypass the conventional government controls imposed on third party intermediaries such as banks and payment processors. By eliminating intermediaries in financial transactions, Bitcoin can circumvent the government oversight, regulations, or controls that normally restrict third party intermediaries.

For instance, the Bitcoin protocol is not subject to capital controls, the whims of central banks, or manipulation by humans, since the computer protocol itself is settled.[27] These qualities have made Bitcoin an attractive option in the aftermath of high-profile bank failures. By way of example, in 2013 investors lost confidence in the Cypriot banking system after an unprecedented bailout.[28] The Cypriot government then instituted strict capital controls to limit the movement of money outside the country.[29] Seeking security, Cypriot investors flooded into the Bitcoin economy to bypass these government controls.[30] As a result, the price of Bitcoin surged by 87%.[31]

Bitcoin can also be used to support politically unpopular causes. After WikiLeaks released a trove of secret U.S. diplomatic cables, donations to the organization slowed.[32] Third party intermediaries, notably the Bank of America, MasterCard, PayPal, VISA, and Western Union, started refusing to process payments to WikiLeaks.[33] Some commentators suggested that the U.S. government had exerted pressure on these private

[27] Brito & Castillo, supra note 1, at 17.
[28] Maureen Farrell, *Bitcoin Prices Surge Post-Cyprus bailout*, CNN (Mar. 28, 2013, 6:25 AM), http://money.cnn.com/2013/03/28/investing/Bitcoin-cyprus/index.html [hereinafter Farrell].
[29] Farrell, supra note 28.
[30] Farrell, supra note 28.; *see also* Jon Matonis, *Bitcoin's Promise in Argentina*, FORBES (Apr. 27, 2013, 12:57 PM), http://www.forbes.com/sites/jonmatonis/2013/04/27/Bitcoins-promise-in-argentina [hereinafter Matonis].
[31] Farrell, supra note 28.
[32] Jon Matonis, *WikiLeaks Bypasses Financial Blockade with Bitcoin*, FORBES (Aug. 20, 2012, 9:47 AM), http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-Bitcoin [hereinafter Matonis].
[33] Matonis, supra note 32.

payment processors to in effect impose a financial blockade of WikiLeaks.[34] In response, WikiLeaks began accepting Bitcoin donations to finance its continued operations.[35] By eliminating third parties, the Bitcoin protocol allowed a near-direct transaction line between payer and payee to bypass the blockade.

C. Pseudo-Anonymity Benefits

One of the most frequently mentioned features of Bitcoin is the pseudo-anonymity it provides participants. Contrary to popular misconception, Bitcoin is not a truly anonymous currency.[36] Rather, Bitcoin is partially, or pseudo, anonymous.[37] "Bitcoin has the unintuitive property that while the ownership of money is implicitly anonymous, its flow is globally visible."[38] To understand Bitcoin's pseudo-anonymity, we must distinguish among three models for financial transactions:

· *Parties-unknown/transaction-unknown.* For instance, in a cash transaction, there is no ledger recording the transaction. If the payer and payee do not know each other's identities, the entire transaction is completely anonymous. In other words, this type of exchange follows a parties-unknown/transaction-unknown model.[39]

· *Parties-known/transaction-known.* At the polar extreme, an online transaction involving a third party intermediary, such as PayPal, is recorded by the intermediary.

---

[34] Matonis, supra note 32.; *see also* Dan Gillmor, *WikiLeaks Payments Blockade Sets Dangerous Precedent*, THE GUARDIAN (Oct. 27, 2011, 12:09 PM), http://www.theguardian.com/commentisfree/cifamerica/2011/oct/27/wikileaks-payments-blockade-dangerous-precedent.
[35] Matonis, supra note 32.
[36] Kate Knibbs, *A Friendly Reminder: Bitcoin Is Not Anonymous*, GIZMODO (Jan. 31, 2015, 3:00 PM), http://gizmodo.com/a-friendly-reminder-Bitcoin-is-not-anonymous-1682885318.
[37] Brito & Castillo, supra note 1, at 7-9 ("Although Bitcoin is frequently referred to as an 'anonymous' currency, in reality, it is very difficult to stay anonymous in the Bitcoin network."); *Hearing*, supra note 24, at 11 ("Bitcoin is not a magic cloak for illicit transactions.").
[38] Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, *in* PROCEEDINGS OF THE 2013 INTERNET MEASUREMENT CONFERENCE 127 (Oct. 23, 2013), *available at* https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf [hereinafter Meiklejohn].
[39] *See Hearing*, supra note 24, at 11.

Additionally, the payer and payee's banks accounts are linked to the intermediary. That link facilitates the subsequent discovery of their identities. This transaction is not anonymous in any sense because the transaction follows a parties-known/transaction-known model.

· *Parties-unknown/transaction-known.* Bitcoin is a hybrid of the previous two models—a parties-unknown/transaction-known model.[40] The block chain, serving as the public ledger, records every Bitcoin transaction that has been made or will be made. However, while the Bitcoin addresses associated with each transaction are recorded in the block chain, the addresses are not tied expressly to anyone's identity. "[W]hile Bitcoin is very similar to cash in that parties can transact without disclosing their identities to a third party or to each other, it is unlike cash in that all the transaction to and from a particular Bitcoin address can be traced."[41] Every transaction made by using that Bitcoin address can be traced on the public block chain. Therefore, Bitcoin is only pseudo-anonymous. If a Bitcoin address could somehow be associated with a specific identity, the pseudo-anonymity would be penetrated.

However, so long as Bitcoin's pseudo-anonymity is maintained, participants enjoy limited financial privacy. Transactions conducted through third party intermediaries are more vulnerable to surveillance.[42] There are many legitimate reasons why people may desire the financial privacy that Bitcoin provides. "Privacy is many things to many people. Among other things, it is the individual's bulwark against objectification by governments, corporations and other individuals."[43] For instance,

[40] Brito & Castillo, supra note 1, at 8. *See Hearing*, supra note 24, at 11.
[41] Brito & Castillo, supra note 1, at 8.
[42] *Hearing*, supra note 24, at 7.
[43] *Hearing,* supra note 24, at 7.

victims of domestic violence can spend money discreetly without being tracked by their abusers. Similarly, charitable benefactors can freely donate money to politically unpopular organizations without fear of reprisal.[44]

II. THE DANGERS POSED BY BITCOIN

Although the Bitcoin protocol offers the significant advantages detailed in Part I, the protocol also poses countervailing dangers. The two most prominent dangers are its doubtful long-term viability as a currency and its possible criminal misuse.

A. Currency Viability

Commentators have noted Bitcoin's price volatility over the past few years, as illustrated by Figure 1.[45] After a steep rise in price due to currency speculation, Bitcoin recently lost much of its value.[46] A year and a half after hitting an all-time high above $1,100, Bitcoin is currently trading near $200.[47] This price volatility and unpredictable swings may deter investors and participants.[48] Investors and participants may be tempted to sell the bitcoins they already own and further depress prices.[49] The depressed price may drive away miners, the individuals responsible for verifying Bitcoin transactions and incorporating them in the block chain. The cost of their computational mining

[44] *See* Brito & Castillo, supra note 1, at 17.
[45] Paul R. La Monica, *Will Bitcoin Ever Rebound?*, CNN (Jan. 15, 2015, 10:56 AM), http://money.cnn.com/2015/01/15/investing/Bitcoin-prices/index.html [hereinafter LaMonica]. *See also* Bitcoin Obituaries: Following Bitcoin While It Dies and Goes Up in Price, http://Bitcoinobituaries.com (last visited Apr. 14, 2015).
[46] La Monica, supra note 45.
[47] LaMonica, supra note 45.
[48] LaMonica, supra note 45.
[49] Nermin Hajdarbegovic & Jon Southurst, *Bitcoin Price Continues to Fall, Breaks $200 Mark*, COINDESK (Jan. 14, 2015, 9:58 AM), http://www.coindesk.com/Bitcoin-price-continues-fall-breaks-200-mark [hereinafter Hajdarbegovic & Southurst].

operations might exceed the fees garnered from mining.[50] It remains to be seen whether Bitcoin will remain a viable currency.

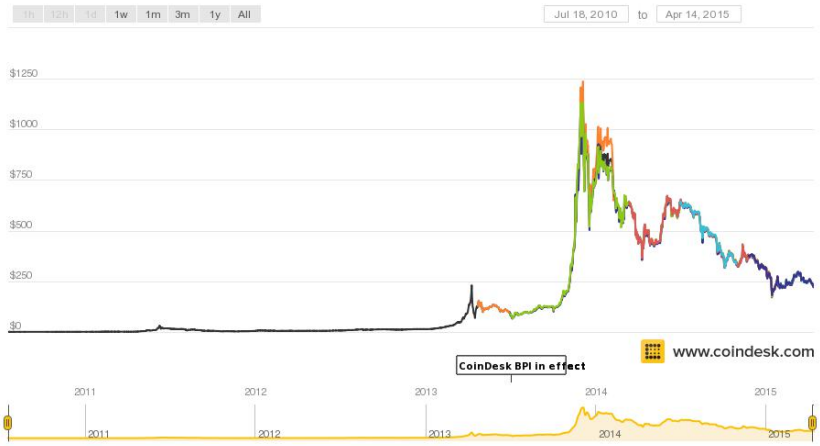


Figure 1. Bitcoin price index chart. *Bitcoin Price Index*, COINDESK, http://www.coindesk.com/price (last visited Apr. 14, 2015).

B. Illegitimate Uses

Another challenge to Bitcoin's legitimacy is its possible criminal misuse. Many commentators in the public, media, and policy circles are aware of Bitcoin only from the notorious examples of its misuse by criminals, notably the two Silk Road prosecutions.[51] These commentators are impressed by the danger arising from Bitcoin's pseudo-anonymity, which makes it difficult to track financial transactions.[52] In a widely distributed intelligence assessment, the Federal Bureau of Investigation declared that Bitcoin "provides a venue for individuals to generate, transfer, launder, and steal illicit funds with some anonymity."[53] The assessment added that "[s]ince Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious

[50] Hajdarbegovic & Southurst, supra note 49.
[51] *See* Yessi Bello Perez, *Bitcoin in the Headlines: Political Spin and Kidnapped Data*, COINDESK (Apr. 11, 2015, 1:00 PM), http://www.coindesk.com/Bitcoin-in-the-headlines-political-spin-kidnapped-data. *See also* Jim Edwards, *CLAIM: Bitcoin Is Basically for Criminals*, BUSINESS INSIDER (Nov. 27, 2013, 12:30 PM), http://www.businessinsider.com/claim-Bitcoin-is-basically-for-criminals-2013-11.
[52] FEDERAL BUREAU OF INVESTIGATION, supra note 2, at 1.
[53] Federal Bureau of Investigation, supra note 2.

activity, identifying users, and obtaining transaction records—problems that might attract malicious actors to Bitcoin."[54]

The most notorious example of such malicious action is the now-defunct Silk Road online black market. Launched in early 2011, Silk Road was confiscated and shut down by U.S. federal authorities in October 2013.[55] Silk Road was created, owned, and operated by Ross Ulbricht, working under a pseudonym, the Dread Pirate Roberts.[56] He was convicted of all seven charges lodged against him, including narcotics and money laundering conspiracies.[57]

During its operation, Silk Road provided a marketplace for vendors to sell illegal narcotics, forged identifications, and other illicit goods and services.[58] Silk Road operated in the deep web, parts of the Internet unreachable by indexing search engines such as Google.[59] Instead, Silk Road operated in the Tor network, a collection of websites reachable only by specialized software that can mask participants' activities.[60] Silk Road relied upon Bitcoin as its primary payment method.[61] "The pseudonymous nature of Bitcoin enabled buyers to purchase illegal goods online in the same way that cash has been traditionally used to facilitate illicit purchases in person."[62]

In the public mind, Bitcoin has become associated with Silk Road and, by extension, other illicit activities. Silk Road has been held up as "an example of how

---

[54] Federal Bureau of Investigation, supra note 2.
[55] Sealed Complaint at 5-6, United States v. Ross William Ulbricht, No. 1:14-cr-00068-KBF (S.D.N.Y. Sept. 27, 2013)[hereinafter Complaint].
[56] Complaint, supra note 55.
[57] Greenberg, supra note 5.
[58] Brito & Castillo, supra note 1, at 23-24.
[59] Jose Pagliery, *The Deep Web You Don't Know About*, CNN (Mar. 10, 2014, 9:18 AM), http://money.cnn.com/2014/03/10/technology/deep-web/index.html [hereinafter Pagliery].
[60] Pagliery, supra note 59.
[61] Brito & Castillo, supra note 1, at 24.
[62] Brito & Castillo, supra note 1, at 24.

[Bitcoin] enabled an online marketplace that could scoff at the oppressive totalitarian attention of law enforcement or the tax man."[63] Bitcoin's association with Silk Road has tarnished Bitcoin's reputation.[64] Today many commentators and casual observers dismiss the supposed benefits of Bitcoin and cynically view Bitcoin as nothing more than a vehicle for illicit transactions.[65]

The simple truth is that "like cash, [Bitcoin] can be used for ill as well as for good."[66] The Bitcoin payment mechanism confers a level of anonymity that makes financial transactions difficult to trace. Given the extensive media coverage of the two Silk Road prosecutions, Bitcoin supporters fear that the government may reflexively react to Bitcoin's negative reputation by overregulating it.[67] The general counsel for the Bitcoin Foundation cautioned the U.S. Senate that "[n]imble and sensible interaction with the Bitcoin community will permit law enforcement to protect the public without stifling innovation and economic growth."[68] He noted that Bitcoin "certainly may provide new challenges to law enforcement, . . . [b]ut we expect the law enforcement challenge to be different, not necessarily harder, in the Bitcoin environment."[69]

To meet this challenge, law enforcement authorities are turning to digital forensics investigators. Those investigators are now tasked to develop new tools and

---

[63] Andrew Leonard, *A Bitcoin Libertarian Disaster: The Silk Road Gets Busted*, SALON (Oct. 2, 2013, 1:05 PM), http://www.salon.com/2013/10/02/a_Bitcoin_libertarian_disaster_the_silk_road_gets_busted.
[64] *See* Brito & Castillo, *supra* note 1, at 24. *See also* Joshua Brustein, *The End of the Internet's Biggest Black Market Is Good for Bitcoin*, BLOOMBERG (Oct. 2, 2013), http://www.bloomberg.com/bw/articles/2013-10-02/silk-roads-demise-sinks-Bitcoin-value-and-saves-Bitcoins-reputation; Samantha Sim & Kazi Stastna, *Bitcoin Will Bounce Back from Silk Road Scandal, Users Say*, CBC NEWS (Oct. 4, 2013, 9:29 PM), http://www.cbc.ca/news/business/Bitcoin-will-bounce-back-from-silk-road-scandal-users-say-1.1913243.
[65] *See* Jim Edwards, *CLAIM: Bitcoin Is Basically for Criminals*, BUSINESS INSIDER (Nov. 27, 2013, 12:30 PM), http://www.businessinsider.com/claim-Bitcoin-is-basically-for-criminals-2013-11.
[66] Brito & Castillo, supra note 1, at 23. *See also Hearing*, supra note 24, at 9.
[67] Brito & Castillo, supra note 1, at 26-27.
[68] *Hearing*, supra note 24, at 11.
[69] *Hearing,* supra note 24, at 11.

methods to de-anonymize participants using Bitcoin illegitimately. The ensuing parts of this article describe some of those new tools and methods.

III. THE MECHANICS OF THE BITCOIN PROTOCOL THAT CREATES PSEUDO-ANONYMITY

To appreciate the nature and magnitude of the challenge now facing digital forensic investigators, we must understand the basic mechanics of a Bitcoin transaction. To illustrate a Bitcoin transaction, assume that Al is the consumer-payer and that Beth is the merchant-payee. Al wants to pay Beth for goods and services by using Bitcoin. Subpart III.A examines a Bitcoin transaction from the end-user perspective—what Al and Beth see and experience when they engage in the transaction. Subpart III.B examines the same transaction at a deeper, protocol level—how the underlying processes work. Combined, both levels of explanation provide a foundation for discussing Bitcoin forensic techniques, described in Part IV.

A. Level #1: The End-User Perspective

Employing Bitcoin as an end-user resembles the use of other online payment mechanisms such as PayPal or Venmo. In order to transact, both payer and payee must have some way to send and receive bitcoins. This transfer is accomplished through the use of Bitcoin "clients." In this context, clients are not persons or even entities. Rather, "clients" are pieces of software or hardware designed to connect participants to the Bitcoin economy and network.[70] Clients come in many forms: desktop, mobile, online, and hardware, each with special power and limitations.[71] Bitcoin clients vary in their

[70] "Bitcoin clients" are also referred to as "bitcoin wallets." To minimize confusion in this section, "clients" will refer to the end-user interface, whereas "wallets" will refer to the wallet.dat file.
[71] For a comparison of clients, see *How to Store Your Bitcoins*, COINDESK (Dec. 22, 2014), http://www.coindesk.com/information/how-to-store-your-Bitcoins.

features and functionality. Some have increased network and file security, back-up options, and additional information about user accounts and network health.[72] Despite this variety, clients have one common denominator: All clients maintain a wallet file. The wallet file contains the information necessary to send bitcoins to Bitcoin addresses. A Bitcoin address is a string of 26-35 alphanumeric characters representing a destination for bitcoin payments. Each Bitcoin address has its own "balance" of bitcoins. There are three ways to start or increase a balance of bitcoins: 1) accept bitcoin as a payment, gift, or donation; 2) buy bitcoin from an exchange or local dealer; or 3) mine bitcoin.

To illustrate these concepts, assume Al would like to pay Beth 1.20 bitcoin (BTC).[73] To transact, they do not need to use the same client. Nor do their clients have to be in the same form.

In this hypothetical, Al uses MultiBit, a desktop client on his Windows PC. Al checks his balance and sees that he has 5 BTC. He had previously bought 5 BTC at the Bitstamp exchange by using U.S. dollars.

For her business, Beth employs CoinBase, an online client, to accept Bitcoin payments. Following good privacy practices, Beth uses her client to create a new Bitcoin address to receive Al's payment.[74] In her CoinBase client, Beth clicks on "Create New Address" to create a new Bitcoin address, namely, the alphanumeric string 3D73hgWqPR36MQatxnwsuktpEVkeFhPNjy.

---

[72] For a comparison of client features, see *Clients*, EN.BITCOIN.IT, https://en.Bitcoin.it/wiki/Clients (last visited Apr. 18, 2015).
[73] BTC is the most commonly used symbol to denote bitcoin. *Bitcoin*, WIKIPEDIA, http://en.wikipedia.org/wiki/Bitcoin (last accessed Apr. 18, 2015). Bloomberg, CNN, and CoinDesk use XBT. *Id.* The Bitcoin Foundation is trying to establish a Unicode symbol for bitcoin consisting of two vertical strokes at the top and bottom of the letter B. *Id.*
[74] *See Protect Your Privacy*, BITCOIN.ORG, https://Bitcoin.org/en/protect-your-privacy (last accessed Apr. 18, 2015).

She forwards this address to Al and instructs him to send 1.20 BTC there as payment. In his MultiBit client, Al clicks on "Send," enters Beth's Bitcoin address, specifies the amount he wants to send (in this case 1.20 BTC), and confirms the action. The 1.20 BTC transaction should show up near-instantaneously but stay pending for up to an hour while the miners in the Bitcoin network verify the transaction.

B. The Processes Underlying a Bitcoin Transaction

Subpart III.A provided an accurate, but superficial description of a Bitcoin transaction. The end-user experience described in Subpart III.A glosses over many of the fundamental processes underlying the Bitcoin protocol. As end-users, Al and Beth interact with only their respective clients in a Bitcoin transaction, as illustrated by Figure 2. This elementary level of understanding is adequate for most Bitcoin participants.

Figure 2. Simplified illustration of a Bitcoin transaction. *How Does Bitcoin Work?*, BITCOIN.ORG, https://bitcoin.org/en/how-it-works (last visited Apr. 18, 2015).

However, digital forensic investigators need a more thorough understanding of the protocol. To appreciate Part IV's discussion of the digital forensic techniques proposed to de-anonymize Bitcoin participants, the underlying processes of a Bitcoin transaction, illustrated by Figure 3, must be examined.

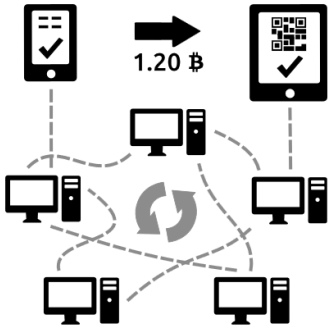


Figure 3. Full illustration of a Bitcoin transaction. *How Does Bitcoin Work?*, BITCOIN.ORG, https://bitcoin.org/en/how-it-works (last visited Apr. 18, 2015).

The key to understanding the processes underlying a Bitcoin transaction is recognizing that there are no corporeal bitcoins to point at.[75] A bitcoin is not a physical object (like a dollar bill or gold) or even a digital object (like an electronic file) that can be stored or transferred. Rather, "a bitcoin can be thought of as a chain of transactions from one owner to the next, where owners are identified by a public key . . . that serves as a pseudonym."[76] A set of steps and transactions, as seen in Figure 4, from origin to Owner1, from Owner1 to Owner2, from Owner3 to Owner4, and so on, constitutes a Bitcoin transaction. Figure 4 depicts the basic transactional flow.

Figure 4. Transaction history showing bitcoin path through multiple Bitcoin addresses. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 38 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

Public-Key Cryptography

Having eliminated third party intermediaries from the transactional flow, Bitcoin uses alternative methods to verify the transaction and prevent double spending. To verify these transactions and prevent double-spending,[77] Bitcoin relies on public-key

[75] *See How Do Bitcoin Transactions Work?*, COINDESK (Mar. 20, 2015), http://www.coindesk.com/information/how-do-bitcoin-transactions-work.
[76] Meiklejohn, supra note 38, at 128.
[77] *See supra* p. 3 for discussion of double-spending problem.

cryptography. Public-key cryptography answers the question, "How do we know Al was authorized to send 1.20 BTC to Beth?"[78] By using public-key cryptography, the transaction between Al and Beth can be verified through the electronic signature created in the process.

The use of public-key cryptography requires that both Al and Beth have their own cryptographic key pair: a private key and a matching public key. A unique key pair is created whenever a new Bitcoin address is generated through a client.[79] When Beth clicked "Create New Address" on her client, what she was really doing was generating a cryptographic key pair consisting of a private key (which Beth keeps to herself in her client's wallet file) and a corresponding public key (which is shared with everyone). (In fact, Beth's new Bitcoin address is itself a hash[80] of the public key.[81]) This public key can later verify any message signed by its corresponding private key.

Transaction Message

Now focus on the message. A Bitcoin transaction consists of a public message to everyone that the payee (seller) is the new owner of the bitcoins formerly belonging to the payer (buyer). When Al instructed his client to send 1.20 BTC to Beth, his transaction contained a public message with three pieces of information: an input (the Bitcoin address that was earlier used to send Al those bitcoins); the amount of bitcoins Al is sending Beth (1.20 BTC); and an output (Beth's Bitcoin address).[82] This public message

[78] *See The Cryptography of Bitcoin*, INSIDE 206-105 (June 3, 2011), http://blog.ezyang.com/2011/06/the-cryptography-of-bitcoin.
[79] *See generally* Morgen E. Peck, *Bitcoin: The Cryptoanarchists' Answer to Cash* fig., IEEE SPECTRUM (May 30, 2012, 4:33 PM), http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg [hereinafter Peck].
[80] A hash is the output of a string of text run through an algorithm. Here, the public key is run through a hashing algorithm to produce the Bitcoin address.
[81] *See generally* Vitalik Butterin, *Developer's Introduction to Bitcoin*, BITCOIN MAGAZINE (Jan. 1, 2014), https://bitcoinmagazine.com/9249/developers-introduction-bitcoin.
[82] *See supra* note 72.

is signed by the private key corresponding with the Bitcoin address Al is transferring bitcoins from. Given Al's public key, everyone can see that the message is authentic and that Beth is the new owner of the 1.20 BTC formerly belonging to Al. Previous and subsequent transactions follow the same process, forming a chain of transactions as in Figure 5. As we shall now see, Change Addresses play an essential role in the chain of transactions.

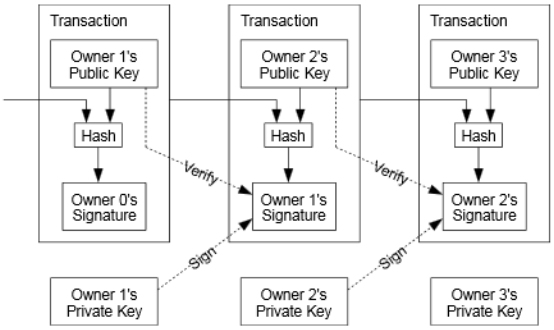


Figure 5. Chain of bitcoin transactions. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 2 (2008), https://Bitcoin.org/Bitcoin.pdf.

Change Addresses

Remember that in our hypothetical transaction, Al has 5 BTC but wants to transfer only 1.20 BTC to Beth. However, because bitcoins are merely records of transactions, bitcoins such as Al's 5 BTC cannot be split up. Payers can use only the whole output of a transaction. In our hypothetical, Al's 5 BTC comes from a single transaction. His payment to Beth of 1.20 BTC cannot be split up or split off from that transaction. This limitation can be analogized to using a $5 bill to pay a charge for $1.20—the entire bill must be transferred. As in the analogy, while the payer must use the whole output of a transaction to pay for a smaller charge, change must be received. In Bitcoin, this process is handled by the client. In this example, Al's Multibit client created

a transaction message containing the following pieces of information: an input of the origin of his 5 BTC; the amount he wants to transfer to Beth (1.20 BTC); and two outputs. One output instructs the transfer of 1.20 BTC to Beth. The other output directs the transfer of the change, the remaining 3.80 BTC, to a new Change Address for Al.

This process is illustrated in Figure 4. The last transaction in Figure 4 involved a payment of 48.8325 BTC. The alphanumeric string beginning 1422qjdw used a single transaction worth 50 BTC to make that payment and received 1.167 BTC in change at a new Change Address under its control, the alphanumeric string beginning 1AF2149t. Similarly, if no single transaction can accomplish a payment, multiple transactions can be combined, again with any change outputted to a new address under the payer's control. The second transaction in Figure 4 illustrates this process. As previously stated, every transaction is ultimately incorporated into the block chain, the computer ledger that every Bitcoin participant has a complete copy of. As we shall now see, miners play a critical role in verifying transactions and then incorporating verified transactions into the block chain.

Mining Blocks

Every transaction is broadcast to the Bitcoin network and grouped into blocks. These blocks are linked to each other to constitute the block chain—the public ledger of all Bitcoin transactions. A copy of this block chain is maintained and updated by every peer in the Bitcoin network. Since each peer in the Bitcoin network has a complete record of all transactions, the problems of double-spending and fraud are reduced or eliminated. The process of adding transactions to the block and incorporating them into the block chain serves two functions at once: it verifies the transactions and expands the money

supply. These functions are normally performed by central banks for fiat currencies. But Bitcoin lacks that central authority.

Instead, Bitcoin relies on participants called miners to perform these functions. Every Bitcoin transaction must be verified by a miner before it is written on the block chain. Miners use their computing power to verify transactions by solving complex mathematical problems.[83] The Bitcoin protocol provides miners with a practical incentive to perform the verification function. The first miner to solve the problem wins a bounty of bitcoins as well as the associated transaction fees. The bounty decreases and the difficulty of each problem increases as the global supply approaches its artificial limit of 21 million Bitcoins. Until November 28, 2012, a bounty was worth 50 BTC. After that date, the bounty halved to 25 BTC where it currently stands. As the difficulty of each problem increases, more computational power is needed. Today miners with massive

[83] For the ease of presentation, this is a simplification of the mining process. See Peck, supra note 79 for a more extensive explanation of the mining process.

No individual person drafts the mathematical problems that the miners must solve. Rather, the problem self-adjusts after a set number of transactions according to a difficulty formula embedded in the Bitcoin protocol. The difficulty formula acts as a damper on the Bitcoin economy. It is designed to ensure that a new block of transaction is verified by miners every 10 minutes—if miners attempt to verify blocks more quickly, the formula auto-adjusts to increase the difficulty of the problem.

Miners run software on their computers that bundle transactions from the past 10 minutes into a block. That block is not yet chained to the previous blocks in the block chain.

As previously stated, to verify a block of transactions and include it in the block chain, miner must solve a mathematical problem. The process involves generating a cryptographic hash by using the SHA-256 algorithm. Running this algorithm on the block of transaction data (and the date from the previous transactions on the verified block chain) produces a unique hash value. If any data in the block has been tampered with, a different hash value would result.

Producing the hash value is computationally easy—any computer would be able to do it, and everyone would mine Bitcoins, causing extreme inflation in the economy. This is where the difficulty formula comes in. The difficulty formula sets a self-adjusting limit for the hash value. As the difficulty increases, the hash value starts with an ever increasing number of zeroes.

Running the SHA-256 algorithm over the same block of transaction data (and the data about the previous transactions on the verified block chain) would always result in the same hash value. To change the hash value to equal a value below the self-adjusting limit, miners incorporate a nonce into the data. The nonce is a random piece of data that changes the hash value. Solving the problem involves the miner trying to find the right nonce to produce a hash value below the self-adjusting limit.

Once the miner finds the right nonce, the block is solved/verified. The solution can then be submitted to the network, and the block of transaction data can be incorporated in the block chain. Then the next block of transactions can be solved and added next to this block, elongating the block chain.

data centers or who are part of mining collectives are the most successful bounty winners. After the miner solves the problem, the verified transaction is incorporated in the block chain.

Summary

In summary, Bitcoin participants generate one or more cryptographic key pairs and publicize the associated Bitcoin address to receive bitcoins.[84] If a payer wants to transfer bitcoins to a payee, he or she broadcasts a signed transaction message throughout the Bitcoin network to publicize the ownership transfer.[85] This transaction eventually reaches a miner, who collects it with other transactions into a block and begins to solve the complex mathematical problem to verify it.[86] Once a miner solves the problem, he or she broadcasts their success throughout the network and receives the bounty.[87] The verified block soon joins the block chain, which is updated for every peer in the network.

IV. USING THE TECHNIQUES OF TRAFFIC AND TRANSACTION GRAPH ANALYSIS TO PENETRATE BITCOIN'S PSEUDO-ANONYMITY

Bitcoin participants enjoy a much greater degree of privacy than persons who use other money-transfer means.[88] Though every Bitcoin transaction is recorded in the block chain, the public addresses associated with each transaction are not directly linked to identities. As long as that separation exists, pseudo-anonymity is maintained. However,

[84] Meiklejohn, supra note 38, at 128.
[85] Meiklejohn, supra note 38, at 128.
[86] Meiklejohn, supra note 38, at 128-29.
[87] Meiklejohn, supra note 38, at 129.
[88] Brito & Castillo, supra note 1, at 9.

as Part II noted, modernly law enforcement authorities are attempting to penetrate that pseudo-anonymity when they suspect that bitcoins have been used in criminal transactions. Efforts to de-anonymize or degrade the anonymity of Bitcoin participants are the subject of ongoing academic scientific research. Although the Bitcoin protocol is designed to create pseudo-anonymity, the process leaves traces for digital forensic investigators to examine. These traces can be found in the peer-to-peer network itself or among the millions of transactions recorded on the block chain. Generally, research efforts in this area have taken one of two methods: traffic analysis and transaction graph analysis.[89] Traffic analysis analyzes the nodes connecting the peer-to-peer network while transaction graph analysis identifies clusters within the millions of transactions in the block chain.

A. Traffic Analysis: The Use of Nodes to Identify a Bitcoin Participant's IP Address

Bitcoin traffic analysis relies on the characteristics or vulnerabilities inherent in Bitcoin's peer-to-peer network to identify the IP address of users generating transactions. The key to this mode of analysis is appreciating the role of nodes in Internet communication. Traffic analysis attacks pseudo-anonymity by "fingerprinting [Bitcoin] users based on the connections they have to other nodes on the Bitcoin p2p network . . . When a user connects to another node, their IP address is advertised to that node. If an attacker is connected to enough nodes, these announcements can be watched and fingerprinting can be done."[90] Different researchers have proposed varying

[89] Chris Cowen, *Forensics and Bitcoin*, FORENSIC FOCUS (Jan. 16, 2015), http://articles.forensicfocus.com/2015/01/16/forensics-bitcoin/ [hereinafter Cowen].
[90] Cowen, supra note 89.

methodologies to exploit the nodes to identify the IP addresses of Bitcoin users.[91] This article concentrates on the work by Alex Biryukov et al.[92] To understand his work, we must examine Bitcoin's peer-to-peer network and relaying protocol in greater detail.[93]

Bitcoin Peer-to-Peer Network

Bitcoin has no central server or network infrastructure to maintain its economy. Rather, Bitcoin is composed of a network of individuals, each running software that communicates with other Bitcoin participants. Collectively, this peer-to-peer network is Bitcoin.

More technically, the Bitcoin network is composed of peers connected to others peers over unencrypted TCP channels. Each peer attempts to maintain eight outgoing connections to other peers, as illustrated by Figure 6. These eight peers are called entry nodes.[94] Peers that can accept incoming connections are servers.[95] Peers that cannot accept incoming connections, such as those behind firewalls, are clients.[96] Therefore, because they can accept incoming connections, all entry nodes are servers, but none is a client.

---

[91] For more details about each variation of Bitcoin traffic analysis, see Alex Biryukov et al., *Deanonymisation of Clients in Bitcoin P2P Network*, in PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 15 (Nov. 3, 2014), *available at* http://dx.doi.org/10.1145/2660267.2660379 [hereinafter Biryukov]; Dan Kaminsky, Chief Scientist, DKH, Black Hat USA 2011: Black Ops of TCP/IP 2011(Aug. 3, 2011) (slides available at http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011); Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 18TH INTERNATIONAL CONFERENCE, FC 2014 469 (Mar. 2014), *available at* http://www.bitcoinsecurity.org/wp-content/uploads/2014/01/Koshy-FC141.pdf.

[92] Alex Biryukov et al., *Deanonymisation of Clients in Bitcoin P2P Network*, in PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 15 (Nov. 3, 2014), *available at* http://dx.doi.org/10.1145/2660267.2660379 [hereinafter Biryukov].

[93] For ease of presentation, this is a simplified description of the peer-to-peer network and the relay protocol. For a more extensive examination, see Biryukov, supra note 92, at 17-18.

[94] Biryukov, supra note 92, at 17. The official Bitcoin software makes no distinction amongst servers, clients, and entry nodes. These are terms of use in Biryukov's research.

[95] Biryukov, supra note 92.

[96] Biryukov, supra note 92.

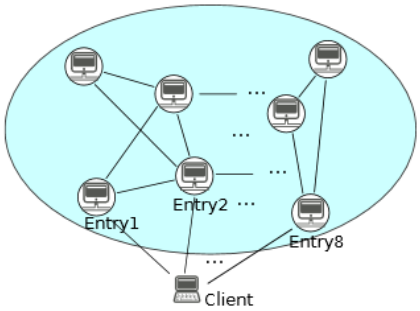


Figure 6. Bitcoin P2P network. Alex Biryuk et al., *Deanonymisation of Clients in Bitcoin P2P Network*, *in* Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 15, 17 (Nov. 3, 2014), *available at* http://dx.doi.org/10.1145/2660267.2660379.

Transaction and block messages are propagated throughout the network by being relayed through these entry nodes to other peers. When Al sends a transaction advertising that he is transferring ownership of 1.20 BTC to Beth, his computer sends an *inv* message to its immediate peers, the entry nodes.[97] The *inv* message lets the entry nodes know that there are transactions or blocks. The entry nodes request the full transaction by sending a *getdata* response to Al's computer. After receiving the full transaction data from Al, the entry nodes determine whether the data is valid. If the data is valid, the entry nodes relay the data farther throughout the network by sending *inv* to their own peers. The process continues until every Bitcoin peer has received the message. (Note however that peers will ask for data only if they do not already have it.)

A similar process is used to propagate IP addresses throughout the network. IP addresses are propagated to help peers discover other peers on the network. Every twenty-four hours, every computer in the network sends out an *addr* message to its entry nodes, which relay the message to their own peers and so on. The *addr* message contains the computer's IP address. Additionally, when it connects, every computer advertises its

[97] *See generally Network*, EN.BITCOIN.IT, https://en.bitcoin.it/wiki/Network (last visited Apr. 20, 2015).

IP address to its entry nodes. This system ensures that every peer knows which IP addresses are connected to the network at the moment.

Biryukov Traffic Analysis

Traffic analysis exploits the role of nodes in this protocol to discover the IP address of users generating Bitcoin transactions. Biryukov's version of traffic analysis includes four steps:

1. **Obtain a list of peers and connect to as many servers as possible within the Bitcoin network**[98]

Initially, the researcher collects the entire list of peers by sending out a *getaddr* message.[99] After every server is found, 50 connections are made to each server.[100] At the time of Biryukov's research, there were approximately 8,000 reachable servers.[101] Each server can accommodate 117 incoming connections at once.[102]

2. **Compose a target list of addresses to focus on**[103]

These targets can come from various sources such as the range of IP addresses assigned to individual ISPs or online fora advertising addresses.[104]

3. **Map targets to their entry nodes**[105]

The third step is the key to Biryukov's methodology. When a target connects to an entry node, the target advertises its IP address to the node. Since the researcher is connected to all or most servers/entry nodes, he or she can determine which server received IP addresses from which target.

[98] Biryukov, supra note 92, at 19-20.
[99] Biryukov, supra note 92, at 20.
[100] Biryukov, supra note 92.
[101] Biryukov, supra note 92, at 17.
[102] Biryukov, supra note 92, at 17.
[103] Biryukov, supra note 92, at 20.
[104] Biryukov, supra note 92, at 20.
[105] Biryukov, supra note 92, at 20.

Biryukov opined that the identification of three servers/entry nodes is sufficient to triangulate to uniquely identify a target, but suggested that two nodes would be adequate for a large percentage of targets.[106]

4. Match transactions to the targets' entry nodes[107]

The researcher listens for *inv* messages advertising transactions among the connections he or she has established.[108] On finding a transaction, the researcher notes the first ten server addresses that forwarded the *inv* message.[109] The researcher then compares these addresses with the targets' entry nodes.[110] If there are two to three matches between the addresses forwarding the *inv* message and a specific target's entry nodes, the researchers can conclude that the target IP address initiated the transaction.[111] Thus, the end result of the analysis is the identification of an IP address, the address supposedly associated with the Bitcoin user whom the law enforcement authorities suspect.

B. Transaction Graph Analysis: Identifying Chokepoints such as Exchanges to Target with Subpoenas for the User's IP Address

While Professor Biryukov's traffic analysis relies on nodes to identify the IP address of a Bitcoin user, there is an alternative approach. The alternative approach, transaction graph analysis, complements traffic analysis.[112] In traffic analysis, researchers monitor the nodes in the peer-to-peer Bitcoin network to identify transactions

[106] Biryukov, supra note 92, at 20.
[107] Biryukov, supra note 92, at 20.
[108] Biryukov, supra note 92, at 20.
[109] Biryukov, supra note 92, at 20.
[110] Biryukov, supra note 92, at 20.
[111] Biryukov, supra note 92, at 20.
[112] *Bitcoin P2P Deanonymization Attack FAQ*, CRYPTOLUX, https://www.cryptolux.org/index.php/Bitcoin_P2P_deanonymization_attack_FAQ (last visited Apr. 23, 2015)[hereinafter Bitcoin P2P].

in real-time to de-anonymize users.[113] In contrast, in transaction graph analysis, researchers search for transaction patterns in the block chain to degrade the anonymity of participants.[114] In this mode of analysis, researchers trace the flow of Bitcoins, but they cannot de-anonymize individual users. Rather, this approach tracks the flow of Bitcoins to chokepoints in the Bitcoin economy such as exchanges.[115] These chokepoints then become targets for law enforcement agencies; an agency can subpoena the exchange to force the exchange to divulge the IP address of the Bitcoin user who maintains the account.[116]

Research by Sarah Meiklejohn et al. at the University of California, San Diego and George Mason University represents the most recent advances in transaction graph analysis.[117] This paper focuses on her work. To better understand her variation of transaction graph analysis, some additional information about the Bitcoin economy and its participants is necessary.

Bitcoin Economy and Participants

As of April 2015, the Bitcoin economy enjoyed around 105,000 transactions[118] and a daily transaction volume of around $40,000,000 USD.[119] The economy is filled with merchants, such as Overstock.com, and service providers, such as currency exchanges, payment processors, financial services, and others listed in Figure 7.

---

[113] Bitcoin P2P, supra note 112.
[114] *See* Cowen, supra note 89.
[115] Meiklejohn, supra note 38, at 135.
[116] Meiklejohn, supra note 38, at 135.
[117] For a review of earlier transaction graph analysis research, see Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 18TH INTERNATIONAL CONFERENCE, FC 2014 469, 472 (Mar. 2014), *available at* http://www.bitcoinsecurity.org/wp-content/uploads/2014/01/Koshy-FC141.pdf.
[118] *Bitcoin Number of Transactions Per Day*, BLOCKCHAIN.INFO, https://blockchain.info/charts/n-transactions (last visited Apr. 21, 2015).
[119] *Estimated USD Transaction Volume*, BLOCKCHAIN.INFO, https://blockchain.info/charts/estimated-transaction-volume-usd (last visited Apr. 21, 2015).

Figure 7. Seven Bitcoin company categories. CoinDesk, State of Bitcoin Q1 2015 (Apr. 10, 2015) (slides available at http://www.slideshare.net/CoinDesk/state-of-bitcoin-q1-2015).

As of April 13, 2013, there were 12,056,684 unique Bitcoin addresses on the network.[120] Because each Bitcoin address is unique, the address can be thought of as a pseudonym for an individual.[121] However, there are not 12,056,684 individuals on the Bitcoin network. Participants, including individuals and companies, can create as many unique Bitcoin addresses as they want. They are naturally motivated to do so for each transaction to protect their privacy.[122] Hence, a number of Bitcoin addresses can be pseudonyms for a single individual, merchant, or service provider operating in the Bitcoin economy.

Tracking transactions over 12 million Bitcoin addresses representing an unknown number of individuals or services is obviously a daunting task. To simplify the task and start linking Bitcoin addresses with identities, Meiklejohn and her colleagues collected ground truth data and clustered Bitcoin addresses.[123]

Step #1: Ground Truth Data Collection

[120] Meiklejohn, supra note 38, at 129.
[121] *See supra* pp. 8-9.
[122] *See supra* note 74.
[123] Meiklejohn, supra note 38, at 130-34.

First, the researchers transacted with as many services as possible to label those Bitcoin addresses as controlled by a particular known entity.[124] In their research, they engaged in 344 transactions with different merchants, exchanges, wallets, miners, and others.[125] For instance, when the researchers exchanged currency with the Bitstamp exchange, they tagged the associated public addresses used in the transaction as belonging to Bitstamp, as demonstrated in Figure 8.

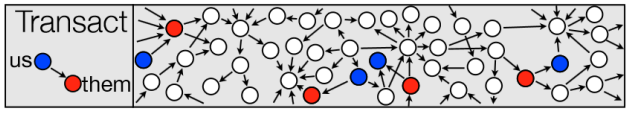


Figure 8. Performing transactions to tag known entities. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 48 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

Step #2: Bitcoin Address Clustering

The first step may yield a very large number of tagged entities and persons. In the second step, to create a more manageable transaction graph to analyze, the researchers cluster together multiple Bitcoin addresses that represent unique persons or entities.[126] The researchers employed two guidelines or heuristics to form the clusters:

Heuristic 1: "If two (or more) addresses are inputs to the same transaction, they are controlled by the same user."[127]

As previously stated, if a single input does not have a large enough balance to pay for a good or service, multiple inputs are combined or strung together to send a payment.[128] It made sense at the time of the research to assume that all the inputs used in

[124] Meiklejohn, supra note 38, at 130.
[125] Meiklejohn, supra note 38, at 130.
[126] Meiklejohn, supra note 38,. at 131.
[127] Meiklejohn, supra note 38, at 132.
[128] *See supra* pp. 18-19.

a transaction were owned by the same person or entity, since private keys were needed to spend the balances in those inputs.[129] An example is illustrated in Figure 9.

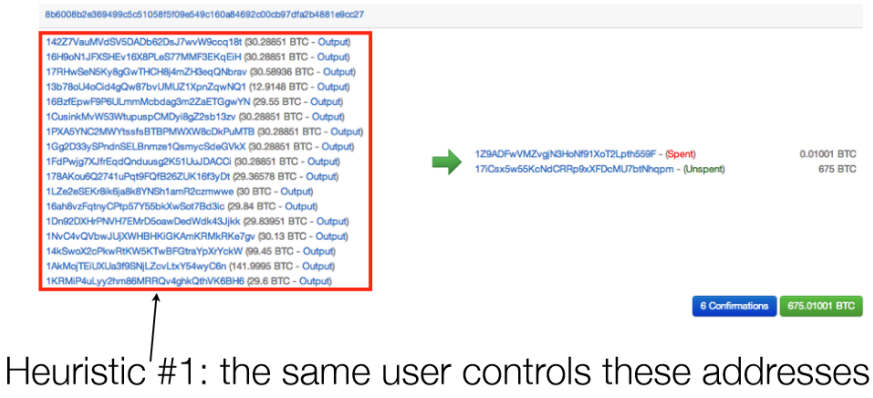


Figure 9. Multi-input transaction. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 51 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

At the time of the research in 2013, it was fairly safe to assume that only one entity controlled all the inputs used to make a single transaction.[130] It was unlikely that a privacy-conscious sender (the sort of sender attracted to Bitcoin) would share his or her private keys with others.[131]

Heuristic 2: "The one-time change address is controlled by the same user as the input address."[132]

To further collapse the number of addresses into clusters, Heuristic 2 takes advantage of Change Addresses. As previously stated, inputs cannot be split up for smaller transactions. To allow payments, inputs larger than the payment are sent, with

[129] Meiklejohn, supra note 38, at 132.
[130] Meiklejohn, supra note 38, at 132.
[131] Meiklejohn, supra note 38, at 132.
[132] Meiklejohn, supra note 38, at 133. For the ease of presentation, this is a simplified overview of Heuristic 2. For a more in-depth overview, see Meiklejohn, supra note 38.

the remaining Bitcoin sent to a Change Address under the payer's control.[133] In the example, Al had 5 BTC with which to pay Beth 1.20 BTC. Al's 5 BTC cannot be split up, since it represents a whole transaction history. This characteristic forces Al to send the entirety of the 5 BTC to make a 1.20 BTC payment. However, the remainder of 3.80 BTC is transferred to a Change Address under Al's control. Since the Change Address is under the control of the same person or entity that controlled the input address, both change and input addresses can be clustered together, as demonstrated by Figure 10.[134]

Figure 10. Change address control. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 64 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

Step #3: Bootstrapping

Third, the researchers overlaid the overall Bitcoin network graph with both the entities positively tagged through transactions in step #1 and the address clusters found in step #2.[135] As previously stated, in step #1, Professor Meiklejohn's team transacted with numerous Bitcoin participants to determine which addresses they controlled. The

[133] *See supra* pp. 18-19.
[134] Meiklejohn, supra note 38, at 133. To reduce the false positive rate to 0.28%, researchers waited a week before labeling an address as a change address. *Id.*
[135] Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 95 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf)[hereinafter Meiklejohn II].

researchers then bootstrapped any tagged transactions within a cluster.[136] For instance, assume the researchers transacted with Bitstamp and tagged that particular Bitcoin address as Bitstamp's. If that Bitstamp address falls within a cluster, every other address in that cluster can be inferred to belong to Bitstamp, as Figure 11 demonstrates.

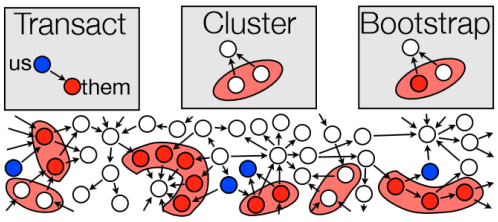


Figure 11. Complete process to cluster transaction graph into a smaller number of distinct entities. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 95 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

After running these processes, the research team concluded that 12,056,684 unique Bitcoin addresses collapsed into 3,383,904 distinct clusters.[137] The researchers succeeded in identifying 2,197 clusters, accounting for over 1.8 million addresses, as visualized in Figure 12.[138]

[136] Meiklejohn II, supra note 135.
[137] Meiklejohn, supra note 38, at 133.
[138] Meiklejohn, supra note 38, at 133.

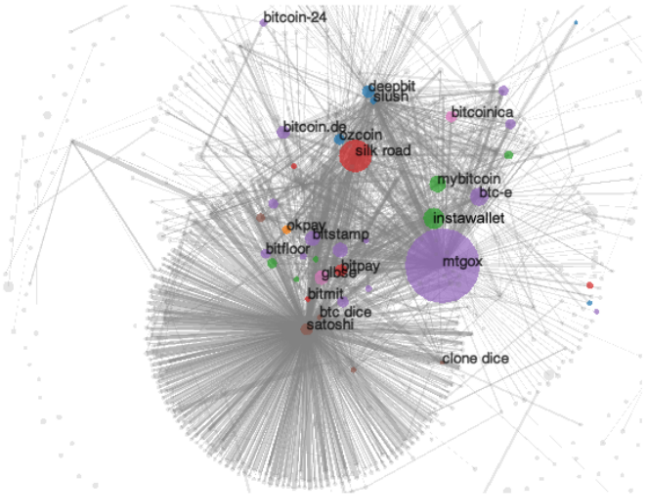


Figure 12. Visualization of user network. Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, *in* PROCEEDINGS OF THE 2013 INTERNET MEASUREMENT CONFERENCE 127, 135 fig.6 (Oct. 23, 2013), *available at* https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

After analyzing the clusters, the researchers discovered that particular services, some of which are represented in Figure 7, are central to the functioning of the Bitcoin economy.[139] These centralized services include exchanges. Exchanges serve as natural chokepoints in the Bitcoin economy. For instance, for anyone, including a criminal, to cash out of the Bitcoin economy, they must use an exchange to convert Bitcoins to fiat currency.[140] Therefore, exchanges become attractive targets for subpoenas by law enforcement agencies.

Step #4: Tracking Illicitly Obtained Bitcoins to Exchanges or Other Subpoenable Services

The processes described in steps #1-3 make the tracking of money flows easier by identifying some of the major service islands in the stream of Bitcoin transactions. To

[139] Meiklejohn, supra note 38, at 134.
[140] Sites like localbitcoins.com allow people to buy bitcoins from sellers in the physical world, but doing so may only work on a small scale. Meiklejohn, supra note 38, at 135.

track whether illicitly obtained bitcoins ever touch one of these identified islands such as an exchange, researchers focused on following Change Addresses originating from suspicious Bitcoin addresses.[141]

Using Heuristic 2 assuming that the one-time change address is controlled by the same user as the input address, researchers can track a "peeling chain" of transactions.[142] In a peeling chain, a single address with a large amount of Bitcoins conducts a transaction in which a small amount is sent to a recipient address (the "peel") and the remaining amount is sent to a Change Address, as seen in Figure 13.[143]

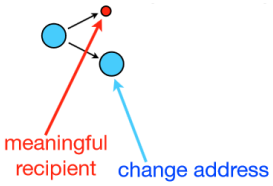
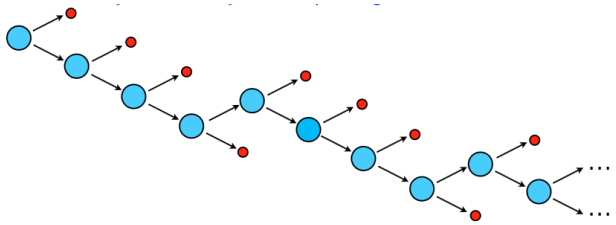


Figure 13. Peeling transaction. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 106 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

From the Change Address, the process repeats until the large amount is reduced, as seen in Figure 14.[144] At that point, the Change Address can be combined with other input addresses to form a large amount in a single address. At that point, the peeling process may repeat again.[145]



[141] Meiklejohn, supra note 38, at 135.
[142] Meiklejohn, supra note 38, at 135.
[143] Meiklejohn, supra note 38, at 135.
[144] Meiklejohn, supra note 38, at 135.
[145] Meikleohn, supra note 38, at 135.

Figure 14. Following the peeling chain of change addresses. Sarah Meiklejohn et al., Presentation to the 2013 Internet Measurement Conference: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names 109 fig. (slides available at https://cseweb.ucsd.edu/~smeiklejohn/files/imc13-slides.pdf).

By following the Change Addresses, researchers can trace peels of Bitcoin to services that were identified earlier by the clustering heuristics.[146] Those services now become targets for subpoenas seeking additional information that may eliminate the pseudo-anonymity of users.[147] The law enforcement agency can compel the service to disclose the Bitcoin participant's IP address. In short, a transaction graph analysis should lead to the same result as a traffic analysis, an IP address, but through a fundamentally different methodology.

V. THE ADMISSIBILITY OF TESTIMONY BASED ON TRAFFIC AND TRANSACTION GRAPH ANALYSIS

Traffic and transaction graph analyses are cutting-edge techniques that have not yet been used in the courtroom. The 2015 Silk Road trial provided one of the first chances for a court to consider the evidentiary issues related to Bitcoin. However, at that trial the prosecution did not attempt to introduce expert testimony based on either traffic analysis or transaction graph analysis. Therefore, there is no case law precedent providing evidentiary guidance about the admissibility and weight of these techniques. The standards articulated by *Kelly/Frye* and *Daubert* will determine whether courts can admit testimony based on these techniques in the future.

A. Admissibility in General

[146] Meiklejohn, supra note 38, at 137.
[147] Bitcoin exchanges are most likely subject to FinCEN regulations that require, amongst other things, customer record keeping requirements. Brito & Castillo, supra note 1, at 29-30. *See also* FIN. CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FIN-2013-G001 APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013), *available at* http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

Under the Kelly/Frye *General Acceptance Standard*

In *Frye v. United States*, the Court of Appeals of the District of Columbia held that "while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs."[148] In *People v. Kelly,* the California Supreme Court adopted *Frye*'s general acceptance standard; and the California courts eventually expanded the standard into a tripartite test that: The expert must be qualified; the theory or technique the expert employs must be generally accepted; and the expert must follow proper test procedure in applying the theory or technique to the facts of the case.[149] That test has been dubbed the *Kelly/Frye* standard in California. In *Kelly,* the California Supreme Court stated that it approved of the "essentially conservative nature" of the general acceptance standard.[150] "*Frye* was deliberately intended to interpose a substantial obstacle to the unrestrained admission of evidence based upon new scientific principles."[151] Although the California Supreme Court moved closer to embracing the *Daubert* standard in *Sargon Enterprises, Inc. v. University of Southern California*,[152] the court explicitly stated that the *Kelly*/*Frye* regime still applies in California.[153]

Both traffic and transaction graph analyses would most likely fail the general acceptance test. Both analyses attempt to de-anonymize Bitcoin users. However, "[w]hen

---

[148] Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923).
[149] People v. Kelly, 17 Cal. 3d 24, 30 (1976).
[150] *Id.* at 31.
[151] *Id.*
[152] David L. Faigman & Edward J. Imwinkelried, *Wading into the Daubert Tide: Sargon Enterprises, Inc. v. University of Southern California*, 64 HASTINGS L.J. 1665, 1694 (2013).
[153] Sargon Enterprises, Inc. v. Univ. of S. Cal., 55 Cal. 4th 747, 772 n.6 (2012) ("Nothing we say in this case affects our holding in *Leahy* regarding new scientific techniques."). The *Sargon* standard applies to all types of expert testimony. The *Kelly/Frye* standard applies at least to novel, instrumental scientific techniques. Thus, in California the latter type of testimony is arguably subject to both standards.

identification is chiefly founded upon an opinion which is derived from utilization of an unproven process or technique, the court must be particularly careful to scrutinize the general acceptance of the technique."[154] To establish general acceptance, the proponent must demonstrate the "technique has become generally accepted by a typical cross-section of the relevant scientific community."[155] The courts "must consider the quality, as well as quantity, of the evidence supporting or opposing a new scientific technique. Mere numerical majority support or opposition by persons minimally qualified to state an authoritative opinion is of little value under the foregoing cases."[156]

There is currently no evidence of extensive support for either traffic analysis or transaction graph analysis. The lack of support is undoubtedly largely due to the relative novelty of these techniques. The hypothesis of traffic analysis was proposed in 2011,[157] but the initial efforts to employ the analysis to de-anonymize Bitcoin users at the IP level were not attempted until 2014[158]. The first attempts at clustering and tracking Bitcoin addresses did not occur until 2011,[159] and Meiklejohn's refinements were not developed until 2013[160]. While there has been some coverage of these developments in the Bitcoin press,[161] there are currently no published critical assessments of the techniques by

---

[154] People v. Kelly, 17 Cal. 3d 24, 32 (1976) (citing People v. Law, 40 Cal. App. 3d 69, 85 (Cal. Ct. App. 1974)).
[155] People v. Leahy, 8 Cal. 4th 587, 611-12 (1994) (internal quotation omitted).
[156] *Id.* at 612.
[157] Dan Kaminsky, Chief Scientist, DKH, Black Hat USA 2011: Black Ops of TCP/IP 2011(Aug. 3, 2011) (slides available at http://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011).
[158] Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 18TH INTERNATIONAL CONFERENCE, FC 2014 469 (Mar. 2014), *available at* http://www.bitcoinsecurity.org/wp-content/uploads/2014/01/Koshy-FC141.pdf.
[159] *See* MARTIN HARRIGAN & FERGAL REID, AN ANALYSIS OF ANONYMITY IN THE BITCOIN SYSTEM (May 7, 2012), *available at* http://arxiv.org/pdf/1107.4524v2.pdf.
[160] Meiklejohn, supra note 38.
[161] *See, e.g.,* Andy Greenberg, *Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road's Black Market*, FORBES (Sept. 5, 2013, 10:36 AM), http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market.

scientists outside the Bitcoin world. Without evidence of popular support for these techniques in the relevant scientific fields, the techniques cannot be considered generally accepted. If a court scrupulously applied the *Frye* test, the result should be the exclusion of the testimony.

This result is in the line with *Frye*'s philosophy that is "willing to forego admission of such techniques completely until reasonably certain that the pertinent scientific community no longer views them as experimental or of dubious validity. This all-or-nothing approach was adopted in full recognition that there would be a considerable lag between scientific advances and their admission as evidence in a court proceeding."[162] As previously stated, the proponents of the *Frye* test such as the California Supreme Court favor the test in part because of its conservative nature. The proponents fear that trial judges will admit testimony about expert theories and techniques before they have undergone adequate scrutiny to ensure their reliability. To date, traffic analysis and transaction graph analysis have received only minimal scrutiny.

Under the Daubert *Empirical Validation Test*

Although the general acceptance test was the dominant standard until 1993, in that year the Supreme Court rendered its decision in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* *Daubert* provides a different, more liberal standard for admitting cutting-edge research into court.[163]

In *Daubert*, as a matter of statutory construction the Supreme Court ruled that the Federal Rules of Evidence (FRE) superseded the *Frye* standard for admitting expert

[162] People v. Stoll, 49 Cal. 3d 1136, 1156 (1989) (internal citation and quotation omitted).
[163] Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 579 (1993).

evidence.[164] In conjunction with other Rules, FRE 702 regulates the admission of expert testimony.[165] Forty four states have adopted evidence codes patterned after the FRE,[166] and some variation of *Daubert* is now the governing law in almost two thirds of the states.[167] The *Daubert* Court remarked that the FRE "[relaxed] the traditional barriers to opinion testimony."[168] Using the preliminary fact-finding procedure prescribed in FRE 104(a), the judge must conduct an inquiry to determine whether evidence is admissible.[169] More specifically, the judge must determine under FRE 702 "whether the expert is proposing to testify to (1) relevant, reliable scientific knowledge that (2) will assist the trier of fact to understand or determine a fact in issue."[170]

The *Daubert* Court noted that the text of Rule 702 refers to "scientific . . . knowledge." Drawing on several amicus briefs submitted by individual scientists and scientific organizations, the Court adopted a methodological definition of "scientific knowledge." The Court explained that the expert must marshal enough empirical data and reasoning to support the conclusion that the use of the expert's theory or technique will enable the expert to accurately draw the specific type of inference he or she proposes testifying to. The Court emphasized that the trial judge's inquiry by FRE 702 is a "flexible one.[171]" However, the Court provided trial judges with a non-exhaustive list of six factors to assist judges in deciding whether the proffered theory or technique is

[164] 509 U.S. at 587.
[165] 509 U.S. at 589.
[166] 1 Edward J. Imwinkelried, Paul C. Giannelli, Francis A. Gilligan & Fredric I. Lederer, Courtroom Criminal Evidence § 4, at 10 (5th ed. 2011).
[167] 1 Paul C. Giannelli, Edward J. Imwinkelried, Andrea Roth & Jane Campbell Moriarty, Scientific Evidence § 1.14 (5th ed. 2012).
[168] 509 U.S. at 588.
[169] 509 U.S. at 588.
[170] *Daubert*, 509 U.S. at 592.
[171] 509 U.S. at 594.

sufficiently reliable:[172] Is the theory or technique: (1) testable?; (2) Has the theory been tested?;[173] (3) Is the theory peer reviewed and published;[174] (4) subject to a known or potential rate of error;[175] (5) subject to operation standards;[176] and/or (6) generally accepted?[177] We shall now apply these factors to traffic and transaction graph analysis. In discussing the former technique, we shall emphasize Professor Biryukov's research while in reviewing the latter technique we shall discuss Professor Meiklejohn's work.

Testable or Tested

Due to a number of ethical concerns,[178] Biryukov tested his traffic analysis technique only on the Bitcoin testnet, not the actual Bitcoin network.[179] His estimates of success and false positive rates for the actual network were based on testnet results.[180] The question is whether those estimates can properly be extrapolated to the actual network. This technique is so new that it is hazardous to venture an opinion whether that extrapolation is warranted. Further research is certainly needed to answer that question with any degree of confidence.

In contrast, Meiklejohn used the actual Bitcoin network to conduct her transactions and the actual block chain to cluster the data.[181] Hence, with respect to this factor, there is a stronger case for the admission of testimony based on transaction graph analysis.

---

[172] 509 U.S. at 593.
[173] 509 U.S. at 593.
[174] 509 U.S.. at 593-94.
[175] 509 U.S. at 594.
[176] 509 U.S. at 594.
[177] *Daubert*, 509 U.S. at 594.
[178] For example, studying actual transactions on the Bitcoin network might have intruded on the privacy of Bitcoin participants – who had presumably resorted to the Bitcoin protocol in part because they were so concerned about protecting their privacy.
[179] Biryukov, supra note 92, at 21-22
[180] Biryukov, supra note 92, at 20.
[181] Meiklejohn, supra note 38, at 130-38.

Peer Reviewed and Published

Papers describing both techniques have been presented at conferences.[182] However, little is known about the reaction of the other conferees to the presentations. There is no hard evidence that the conferees responded favorably and expressed satisfaction with the methodology of the research supporting the techniques.

Rate of Error

Although Biryukov tested traffic analysis on only the testnet, he attempted to extrapolate the results to the real Bitcoin network. The extrapolation yielded low success rates and high false positive rates.[183] Biryukov conservatively estimated that when triangulating with three servers/entry nodes, only 11% of transaction could be successfully identified. When triangulating with two servers/entry nodes, the success rate rose to 35% of transactions.[184] However, the increased success rate came at the expense of a higher false positive rate.[185] For each client suspected of generating the transaction, the probability that it was the right client was about 55%--barely above random chance.[186] This high false positive rate should give courts pause.

Meiklejohn did not publish overall false positive rates for transaction graph analysis. However, she reported an initial false positive rate for Heuristic 2. Some addresses labeled as Change Addresses were in fact not so.[187] When clustered and bootstrapped, these addresses could be falsely associated with entities. By adopting

[182] *See Call for Papers*, ACM CCS 2014, http://sigsac.org/ccs/CCS2014/cfp.html (last visited Apr. 22, 2015); *Call for Papers*, IMC 2013, http://conferences.sigcomm.org/imc/2013/cfp.html (last visited Apr. 22, 2015).
[183] Biryukov, supra note 92, at 20.
[184] Biryukov, supra note 92, at 20.
[185] Biryukov, supra note 92, at 20.
[186] Biryukov, supra note 92, at 20.
[187] Meiklejohn, supra note 38, at 133.

conservative measures, Meiklejohn reduced the false positive rate to 0.17%.[188] She adopted additional measures to drive the rate down further, but that rate has not been published.[189] Like Biryukov's high false positive rate, the incompleteness of Meiklejohn's published results should make a trial judge wary about approving the admission of testimony based on transaction graph analysis.

Operation Standards

Neither technique has published standards of operation. Consequently, it will be difficult for subsequent researchers to duplicate the experiments by Biryukov and Meikeljohn to see if they can duplicate their results. One of the strengths of the scientific method is the ability of later researchers to duplicate earlier experiments to determine whether the results were reliable or artifacts. The prospect of subsequent replication of the test gives the original researchers a powerful incentive to conduct their experiment scrupulously, and later experiments duplicating the earlier results can confirm the validity of the earlier results. Until there are standard methods for applying traffic analysis and transaction graph analysis, those techniques will lack that added assurance of reliability.

General Acceptance

As previously stated, neither technique currently enjoys general acceptance.[190]

Summary

The upshot is that neither traffic analysis nor and transaction graph analyses passes muster under *Daubert*. Especially since there are concerns about the application of the other five factors to the techniques, the lack of general acceptance is probably fatal to admissibility. Though *Daubert* superseded *Frye*, general acceptance is still a relevant

[188] Meiklejohn, supra note 38, at 133.
[189] Meiklejohn, supra note 38, at 133.
[190] *See supra* pp. 33-35.

consideration in the inquiry.[191] General acceptance has been demoted from the status of a test to that of a factor, but it is relevant circumstantial evidence of the methodological soundness of the theory or technique. If the theory or technique has garnered general acceptance, other experts have presumably critiqued the underlying research and found it to be methodologically satisfactory. However, if general acceptance is lacking, the court cannot assume that other researchers have reviewed the research and deemed it sound. In the *Daubert* Court's words, while a "reliability assessment does not require . . . explicit identification of a relevant scientific community and an express determination of a particular degree of acceptance within that community[,] . . [w]idespread acceptance can be an important factor in ruling particular evidence admissible, and a known technique which has been able to attract only minimal support within the community may properly be viewed with skepticism."[192]

These techniques do not enjoy general acceptance due to their relative novelty.[193] The only substantial discussions of these techniques appear in the papers published by the technique's developers. The broader scientific community has not yet had the opportunity to critically assess the underlying empirical data and reasoning or, more importantly, to attempt to replicate their results.[194] On balance, a review of the application of the *Daubert* factors to these two techniques leads to the conclusion that in the current state of the art, trial judges should bar testimony based on these techniques.

[191] *Daubert*, 509 U.S. at 594.
[192] 509 U.S. at 594 (internal citations and quotations omitted)
[193] *See supra* p. 34.
[194] *See supra* p. 34.

This conclusion does not contradict the general permissiveness of the FRE.[195] It is true that the *Daubert* opinion employs the adjectives, "liberal" and "permissive." Moreover, as previously stated, the Court construed the FRE as superseding the more "austere" *Frye* standard. Yet, the FRE still imposes limits on the admissibility of scientific evidence.[196] As the *Daubert* Court underscored, the Court was assigning trial judges a "gatekeeping" role to shield the jury from unreliable expert testimony. The Court acknowledged that "a gatekeeping role for the judge, no matter how flexible, inevitably on occasion will prevent the jury from learning of authentic insights and innovations. That, nevertheless, is the balance that is struck by Rules of Evidence designed not for the exhaustive search for cosmic understanding but for the particularized resolution of legal disputes."[197]

B. The Specific Inferences That May Properly Be Drawn from Traffic and Transaction Graph Analysis

Assume *arguendo* that a court disagrees with the analysis presented in Subpart V.A. and concludes that in general, an expert may opine based on either traffic or transaction graph analysis. Even on that assumption, there is a significant remaining question: What specific inference may the expert to testify to? In particular, should the judge limit the expert to testifying that the Bitcoin account is linked to an IP address, or should the judge allow the expert to go further and opine that a particular person or entity was the Bitcoin user?

Unless the trial judge closely regulates the digital expert's opinion testimony, fact-finders might be tempted to draw unwarranted inferences from traffic and transaction

[195] *Daubert*, U.S. 509 at 589.
[196] 509 U.S. at 589.
[197] 509 U.S. at 597.

graph analyses and the IP addresses they identify. As noted before, Bitcoin's pseudo-anonymity is compromised once an identity is linked to a transaction's public address. In traffic analysis, a suspect transaction can be linked to an IP address. In transaction graph analysis, a suspect transaction can be linked to a service, such an exchange, which may maintain a record of IP addresses.[198] While the expert's identification of the IP address may be reliable, it is quite another matter to automatically equate that address with the identity of a specific person or entity. They are two very different inferences.

An IP address (and similarly, a Bitcoin address) does not necessarily denote a specific individual. "Technology professionals have long understood that IP addresses are closer to a zip code than a social security number. Multiple people locally accessing or remotely funneling through a specific hotspot can share IP addresses. In short, IP address [sic] offers little clue to a users' true identity."[199] Nevertheless, unless the trial judge properly restricts the opinion testimony by the digital forensics expert, fact-finders may make an improper inferential leap from the identification of an IP or Bitcoin address to the identification of an individual or entity, the alleged user of the Bitcoin address.

Unfortunately, in the past some courts have drawn precisely that improper inference. The issue has arisen in copyright infringement cases. In copyright holders' lawsuits against file-sharers suspected of copyright infringement, plaintiffs often had only IP addresses as identifying information.[200] Undeterred, copyright holders filed John Doe

[198] Brito & Castillo, supra note 1, at 8.
[199] Jason Mick, *U.S. Legal System Finally Figures Out IP Address != Specific Person*, DAILYTECH (May 4, 2011, 3:07 PM), http://www.dailytech.com/US+Legal+System+Finally+Figures+Out+IP+Address++Specific+Person/article21542.htm.
[200] Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 GEO. L.J. 1, 16 (2006)[hereinafter Cohen].

lawsuits against anonymous file-sharers.[201] In these cases, the copyright holders sometimes sent subpoenas to ISPs for identifying information associated with each IP address suspected of copyright infringement.[202] Initially, courts granted these subpoenas with no regard to the distinction between IP address and individual identity. *Arista Records LLC v. Does 1-16* is illustrative. There the District Court noted that the plaintiff's investigator was "able to *identify* by IP address, which are unique in and of themselves, a user of P2P networks who is distributing or sharing music files over the network."[203] Likewise, in *Voltage Pictures, LLC v. Does 1-5,000*, the District Court stated that "[t]he putative defendants are currently *identified* only by their IP addresses and are not named parties."[204] These early file-sharing cases erroneously treated IP addresses as the equivalent of the identity of unique individuals and entities.

Fortunately, recently courts have become more conscious of the difference between IP addresses and individual identities.[205] In a recent file-sharing case, the Eastern District of New York observed that

> [a]n IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones . . . Different family members, or even visitors, could have performed the alleged downloads. Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular

[201] Cohen, supra note 199.
[202] Cohen, supra note 199.
[203] Arista Records LLC v. Does 1-16, No. 1:08-CV-765-GTS/RF, 2009 WL 414060, at *1 (N.D.N.Y. Feb. 18, 2009), *aff'd*, 604 F.3d 110 (2d Cir.2010) (emphasis added).
[204] Voltage Pictures, LLC v. Does 1-5,000, 818 F. Supp. 2d 28, 41 (D.D.C. 2011) (emphasis added).
[205] *See* Elf-Man, LLC v. Cariveau, No. C13-0507RSL, 2014 WL 202096, at *2 (W.D. Wash. Jan. 17, 2014); AF Holdings LLC v. Rogers, No. 12CV1519 BTM BLM, 2013 WL 358292, at *3 (S.D. Cal. Jan. 29, 2013); Patrick Collins, Inc. v. Doe 1, 288 F.R.D. 233, 237-39 (E.D.N.Y. 2012).

> subscriber and download the plaintiff's film . . . These developments cast doubt on plaintiffs' assertions that the ISP to which each Defendant subscribes can correlate the Defendant's IP address to the Defendant's true identity or that the subscribers to the IP addresses listed were actually the individuals who carried out the complained of acts.[206]

Since the plaintiff's subpoena requesting identifying information from ISPs identified only IP addresses, the court found that the subpoena lacked specificity and was unlikely to lead to identifying information about specific individuals.[207]

The Eastern District's analysis reflects a more accurate, sophisticated understanding of how IP addresses work. The early file-sharing cases existed in a world with wired connections linking a single computer to an ISP via an IP address.[208] However, today the majority of Internet-connected households have wireless routers allowing multiple devices and users to share a single IP address.[209] Hence, the link between an IP address and a specific individual is now more tenuous.

The same issue will arise if the courts contemplate enforcing subpoenas to reveal identifying information about IP or Bitcoin addresses derived from traffic and transaction graph analyses. Fact-finders must avoid the unjustified inferential leap from an IP or Bitcoin addresses to the identity of an individual without corroborating information. In many cases, that corroboration will probably be available. However, when there is no corroboration, there may be legally insufficient proof that the defendant person or entity was the Bitcoin user who put the network to illegal use.

---

[206] *In re* BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84 (E.D.N.Y. 2012) (internal citations and quotations omitted).
[207] 295 F.R.D. at 88.
[208] 296 FR.D. at 84.
[209] 296 F.R.D. at 84.

VI. CONCLUSION

If the courts rigorously apply the *Frye* and *Daubert* standards governing scientific evidence, the traffic and transaction graph analyses should not be admitted due to their lack of general acceptance. Much research remains to be done. If researchers duplicate and refine the pioneering work done by Biryukov and Meikeljohn, a consensus could emerge in the future.

To complicate matters, Bitcoin itself is currently in a state of flux, which may affect the relevance of these techniques. For instance, transaction graph analysis relies upon Heuristic 1, assuming that if two or more addresses are inputs to the same transaction, the addresses are controlled by the same user.[210] However, as Meiklejohn recently conceded, that assumption is increasingly questionable.[211] The advent of new idioms of use and services, such as CoinJoin, can obscure the connection between inputs and users.[212] These developments may reduce the effectiveness of transaction graph analysis and render it irrelevant as these services expand.

The potentially rapid obsolescence of these techniques illustrates the importance of the trial judge's role as gatekeepers in determining the admission of scientific evidence. In that gatekeeping capacity under *Daubert*, judges are tasked with continually reviewing scientific orthodoxy in light of changing conditions and new research. Though the adversarial system may not be the most efficient or effective method of discerning scientific truth, the system at least recognizes the mutability of scientific "truths." Digital forensics experts can help the courts recognize that reality in Bitcoin cases.

---

[210] *See supra* pp. 27-28.
[211] World Crypto Network, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, YOUTUBE (Oct. 16, 2014), https://youtu.be/5ZduzDJTg9Y [hereinafter World Crypto].
[212] World Crypto, supra note 210.; *see also CoinJoin*, EN.BITCOIN.IT, https://en.bitcoin.it/wiki/CoinJoin (last visited Apr. 23, 2015).

APPENDIX: SAMPLE DIRECT EXAMINATION OF EXPERT WITNESS

According to Professor Edward J. Imwinklereid,[213] the direct examination of an expert witness should adopt a minimalist philosophy. He identifies twelve elements that should normally be covered in a direct examination:

Witness 1: Educator or Teacher

1. Qualification
2. Validity of underlying theory
3. Validity of technique implementing theory

Witness 2: Technician or Reporter

4. Qualification
5. Chain of custody/Facts of case
6. Working order of any instrumentation used
7. Proper test procedure
8. Test result

Witness 3: Evaluator or Interpreter

9. Qualification
10. Test result
11. Interpretive standard
12. Final opinion—Explanation of opinion—Restatement of final opinion

For the ease of presentation, each element identified above will appear in parentheses next to each relevant question. Additionally, for the sake of brevity and to stay within the page proscription, this is a truncated sample direct examination.

[213] Edward L. Barrett, Jr. Professor of Law Emeritus, UC Davis School of Law.

In this sample direct examination, assume the functions of Witnesses 1, 2, and 3 are performed by one expert witness in a federal court subject to *Daubert*.[214]

LESLIE NAKAMOTO, called as a witness by the Government, having been duly sworn, testified as follows:

DIRECT EXAMINATION

MS. PROSECUTOR

Q. Good morning, Ms. Nakamoto.

A. Good morning.

Q. What is your highest level of education? (1)(4)(9)

A. I completed a master's degree in cybersecurity at the University of Maryland.

Q. What was the requirement for a master's degree? (1)(4)(9)

A. I had to complete a research thesis.

Q. What was the subject of your thesis? (1)(4)(9)

A. The subject of my thesis was cryptanalysis, which is the study of systems, like computers, to find vulnerabilities that would allow me to gain access to protected content.

Q. Where do you work? (1)(4)(9)

A. The Federal Bureau of Investigation's cybercriminal squad in New York.

Q. What is your position with the FBI? (1)(4)(9)

A. Special agent.

Q. How long have you served as special agent at the FBI? (1)(4)(9)

A. 5 years.

[214] The direct examination of Ilhwan Yum, the United States' expert witness regarding Bitcoin in the Silk Road trial, proved illustrative. Transcript of Record, USA v. Ulbricht, No. 1:14-cr-00068 (S.D.N.Y. Feb 04, 2014), ECF No. 212.

Q. While working as a special agent at the FBI, did you have any experience with Bitcoin? (1)(4)(9)

A. Yes, I did.

Q. Approximately how many Bitcoin transactions have you engaged in? (1)(4)(9)

A. I would say hundreds, probably around 400 transactions.

Q. Have you tracked bitcoins before? (1)(4)(9)

A. Yes, I have.

Q. And how often have you done that? (1)(4)(9)

A. A dozen or so times.

Q. How do you keep up with developments in Bitcoin? (1)(4)(9)

A. I go to at least two or three cybersecurity conferences a year where researchers present new research on Bitcoin. I also follow a dozen or so blogs and forums dedicated to Bitcoin to see if there are any new developments.

Q. What is Bitcoin? (2)

A. Bitcoin is a digital currency. It's like cash for the Internet. You can buy products or services online with it. Like cash, when you buy products using bitcoins, you don't really know who the person across from you is. But unlike cash, when you buy stuff using bitcoins, the transaction is permanently documented on this file called the block chain. So even though you have no clue who made the transactions, the transaction itself can be seen. In this way, the block chain is like a ledger keeping tracking of who paid who, without knowing specific names. The block chain lives online and everyone can see it if they wanted to. It contains every single bitcoin transaction ever made.

Q. How do you even get a bitcoin? (2)

A. There are a few ways, but most people buy bitcoins at currency exchanges. They are like foreign exchanges, where you can exchange dollars for euros. Except here, it can be dollars for bitcoins.

Q. Going back to the block chain, what do you see when you look at it? (2)

A. You see transactions, like A paid B. But you also see every previous and subsequent transaction. You can see that A paid B, then B paid C, then C paid D, and so on. By looking at the block chain, you can see the entire transaction history of Bitcoin.

Q. Now, before you said that you don't really know who you're dealing with when paying with bitcoin. So in your example, who is A, B, C, and D then? (2)

A. A, B, C, and D are Bitcoin addresses, not names. They are strings of numbers and letters that work like email addresses. Each person can have any number of Bitcoin addresses, just like email addresses. And to send bitcoins to someone, you need to know their Bitcoin address, much like how I would need to know your email address to send you an email. But just because I have a Bitcoin address, doesn't mean I know who is behind that Bitcoin address, much like how I would not necessarily know who is behind an email address.

Q. Are there any ways to help discover who is behind a Bitcoin address? (3)

A. Yes, there are two ways to do so: you can track down the user's IP address or you can track a Bitcoin address to a currency exchange.

Q. Let's talk about tracking down a user's IP address. What is an IP address to start with? (3)

A. An IP address is a string of numbers assigned by your Internet Service Provider to your network connection.

Q. How many IP addresses are out there? (3)

A. There must be millions.

Q. So how do you know which ones to focus on? (3) (5)

A. We had been following the Defendant, or rather, his pseudonym, Humperdinck, for a while now on Bitcoin forums. He was on these forums to advertise his new website, Silk Road 4.0. But he also spent time on the forums complaining about his Internet Service Provider, Comcast. Comcast controls a range of IP addresses, which it then doles out to customers. Since we knew Humperdinck used Comcast, we focused our attention on the entire Comcast IP address range.

Q. So how do you track down a specific IP address? (3)

A. You do that by listening to the entire Bitcoin network and seeing what transactions get sent. When a transaction gets sent, you can triangulate where it came from and identify the IP address that sent the transaction.

Q. Let's break that down. What does the Bitcoin network look like? (3)

A. The Bitcoin network just refers to all Bitcoin users' computers linked together in a giant web. When the computers are linked together, they share their IP addresses with each other.

Q. And what does it mean for a transaction to get sent? (3)

A. When you send bitcoins to someone, you let everyone on the Bitcoin network know about it by sending a transaction message. The first people to get it are your immediate network neighbors, who we call the entry nodes. Then your entry nodes forward the message to their network neighbors. And so on and so forth until the entire network knows that you, as represented by a Bitcoin address, sent the transaction.

Q. So how do you figure out the IP address of the person sending a transaction? (3)

A. First, we connect directly with as many computers as possible on the Bitcoin network at once. By doing that, we have an idea of who is connected to whom. Then, if we find a transaction, we make a list of which computers received the transaction message first. Since we know who is connected to whom already, we take the list and compare it to everyone's entry nodes. If there are 2-3 matches between the list and someone's entry nodes, we can assume he was the one who sent out the transaction.

Q. How old is this technique? (3)

A. This technique was first discussed in 2011, shortly after Bitcoin was born.

Q. How reliable is this technique? (3)

A. It was presented and published at a security conference. The technique is also testable.

Q. Let's switch and talk about the other technique to help discover who is behind a Bitcoin address. How can you track a Bitcoin address to an exchange? (3)

A. It's a two-step process. First, you make a map of everyone you can in the Bitcoin economy. Second, you start following a suspect Bitcoin address's transactions across this map until they hit an exchange to cash out their bitcoins.

Q. Let's talk about the first step. How do you make a map of the Bitcoin economy? (3)

A. The Bitcoin economy is made up of exchanges, merchants, financial services, and everything else that you would find in any economy. But as I said before, each person or business can have more than one Bitcoin address, much like how everyone can have more than one email address. Last time someone checked, there are about 12 million

Bitcoin addresses. But those 12 million Bitcoin addresses represent less than 12 million individuals or businesses. So to make sense of so many Bitcoin addresses, we created a map. To make the map, we first tagged a bunch of Bitcoin addresses. And then we clustered together Bitcoin addresses that belonged to the same person or business.

Q. How did you tag Bitcoin addresses? (3)

A. We transacted with known businesses. As I mentioned before, to pay someone in bitcoins, you first need to know which Bitcoin address to send it to. So we paid merchants, went to exchanges, and spent our bitcoins all over the place. And each place would tell us which Bitcoin address to send payment to. We would then tag that Bitcoin address as belonging to that specific business.

Q. How did you cluster Bitcoin addresses? (3)

A. We clustered addresses by making two assumptions. The first assumption is that if two Bitcoin addresses are used to make a single transaction, then both Bitcoin addresses are owned by the same person. In order to spend bitcoins from a Bitcoin address, you need a secret key. If you spend bitcoins from two addresses at the same time, we are assuming you have the secret key for both and you don't share it with anyone else. The second assumption is that if you get change back for overpaying from your Bitcoin address, the new Bitcoin address that change sits in is also owned by you.

Q. So what happened when you tagged and clustered all these Bitcoin addresses? (3)

A. We ended up with a map of over 2,000 identified clusters of addresses. For instance, we now knew a cluster of Bitcoin addresses that belonged to a single exchange.

Q. Let's talk about the second step. How do you track a Bitcoin address through this new map? (3) (5)

A. We find a suspect Bitcoin address to start following. In this case, Humperdinck was advertising his new website on public forums. To accept payments, he advertised a Bitcoin address where people can send bitcoins.

Q. How do you follow transactions from a Bitcoin address? (3)

A. Every transaction is visible on the block chain. Some Bitcoin addresses follow a pattern where they start off with a massive balance that gets whittled down through small transactions. But with every transaction visible on the block chain, we're able to follow this pattern. And since we had a map, we could see where the bitcoins were going.

Q. How old is this technique? (3)

A. This technique was first discussed in 2011, shortly after Bitcoin was born.

Q. How reliable is this technique? (3)

A. It was presented and published at a conference. This technique has already been tested.

Q. Turning to the facts of this case, how long have you been involved in this case? (5)

A. Since the very beginning.

Q. Who conducted the analyses described earlier? (5)

A. I did.

Q. How did you know which IP range to focus on? (5)

A. I was the one who monitored the forums and saw Humperdinck's posts about problems with his Internet Service Provider, Comcast.

Q. How did you know which Bitcoin address was being used for Silk Road 4.0? (5)

A. I was the one who monitored the forums and saw Humperdinck's posts advertising his Silk Road 4.0's address.

Q. How did you perform the analyses? (6)

A. I used a 2014 Macbook Pro with the Google Chrome browser installed to conduct the analyses.

Q. Was that computer in working order? (6)

A. Yes, I tested it before starting.

Q. What procedure did you follow? (7)

A. I followed the process outlined by the original research papers that established these techniques.

Q. What were the results of the analyses? (8) (10)

A. With IP tracking, we identified the entry nodes for the Comcast range of IP addresses as well as a list of nodes that first received a transaction message. With transaction tracking, we tracked small-amount payments to a number of addresses.

Q. What are the standards to interpret the results of the analyses? (11)

A. The standards are articulated in the original research papers themselves. For IP tracking, the mapped entry nodes can be correlated with the list of nodes that first received a transaction message. Two to three entry nodes can form a unique signature for a client node. For transaction tracking, the block chain of allows us to follow transactions from Bitcoin address to Bitcoin address until they reach a Bitcoin address that can be correlated to one that we previously identified.

Q. What conclusion can you draw from these analyses?

A. By correlating the mapped entry nodes to the list of nodes that first received a transaction, we were able to triangulate to the node that first sent out the transaction. Since all nodes send out their IP addresses to nodes they are connected to, we were able to grab the transaction node's IP address. This IP address, along with other identifying information, allowed us to seek a subpoena from Comcast for additional identifying information about where this IP address may lead. By correlating Bitcoin addresses that originated from Silk Road 4.0's address with a list of identified addresses, we were able to see which exchanges those transactions passed through. We hoped that those exchanges fully implemented customer record keeping requirements so that a subpoena may provide us with additional identifying information about individuals associated with the pass-through addresses.