Journal of Forensic Research

Andrew and Douglas, J Forensic Res 2018, 9:3
DOI: 10.4172/2157-7145.1000420

Research Article Open Access

Bitcoin Investigations: Evolving Methodologies and Case Studies

Andrew LR[1] **and Douglas AO**[2*]

[1]*Champlain College, Burlington, USA*

[2]*University of North Georgia College of Arts and Letters, Dahlonega, USA*

[*]**Corresponding author:** Douglas AO, University of North Georgia College of Arts and Letters, Dahlonega, USA, Tel: 404-904-1228, E-mail: douglas.orr@ung.edu

Received date: April 16, 2018; **Accepted date:** May 08, 2018; **Published date:** May 14, 2018

Abstract

Bitcoin is a decentralized, pseudonymous, virtual currency which has been linked to many nefarious activities, such as money laundering, ransomware demands, and the purchase of contraband goods and services. Although it has many redeeming features such as low transaction costs, no charge-backs, and service to the world's 2.5 billion unbanked, the public has become aware of Bitcoin through spectacular news stories of corruption and criminal activities. Techniques to investigate Bitcoin and to identify its users are therefore required to enforce laws and protect the public. This paper discusses what Bitcoin is and how it works, and explores various investigative methodologies to perform Bitcoin network analysis, transactional analysis, and wallet analysis. Finally, this paper discusses emerging issues and suggests areas for improvement with the goal of gaining general acceptance of investigative techniques for admissibility as scientific evidence in courtroom testimony.

Keywords: Bitcoin; Litecoin; Pseudonymous; Investigation; Analysis; Methodology; Forensics; Blockchain

Context

Bitcoin has captured the imagination of the financial world, and, more disturbingly, that of the criminal element, who seek to use its pseudonymous nature to conceal dealings related to nefarious activities such as transacting in contraband goods and services, receiving payment for ransomware attacks, or money laundering, especially on the dark web. The public has become aware of Bitcoin through trial coverage and articles related to these activities. Therefore, there is a need to familiarize investigators with Bitcoin's structure and to attempt, to the greatest extent possible, to penetrate its pseudonymous nature, and some users' anonymization efforts, to link transactions with suspects in a reproducible manner that will allow for admission into court as scientific evidence in the future. The purpose of this paper is to present the mechanics of Bitcoin and then develop a forensic methodology framework for the various types of Bitcoin investigations. Bitcoin fundamentals, peer-to-peer network analysis, blockchain transactional analysis, and wallet analysis will be discussed, with case studies presented for each type of investigation. Also, a brief examination of other crypto currencies will be performed, and future directions proposed.

Fundamentals

Bitcoin

Bitcoin, a decentralized, peer-to-peer, pseudonymous cryptocurrency and an electronic payment system, has rapidly expanded in recognition since the seminal work [1] was distributed to an obscure cryptography mailing list on metzdowd.com [2]. Because it is both a protocol and a currency, there can be confusion; 'Bitcoin' (capitalized, singular) refers to the protocol, software and network, while 'bitcoins' (lower case, multiple) refer to the units of currency, as does 'BTC'.

The foundations of Bitcoin, executed through cryptography, are confidentiality, integrity, non-repudiation, and authentication [3]. Bitcoin is the first successful execution of a distributed cryptocurrency as originally described on the cypherpunks mailing list [4]. The FBI was aware of Bitcoin relatively quickly [5].

Genesis and evolution

The genesis block was created on January 3, 2009 and the first open-source network client, Bitcoin v0.1, was published on the cryptography mailing list of metzdowd.com on January 9, 2009 [6].

Bitcoin continues to evolve to grow and address various challenges. Bitcoin follows a Bitcoin Improvement Proposal (BIP) process to introduce changes and features, as suggested by users, but the assessment of the proposal and the decision whether to implement lies solely with the developers [7]. The methods to implement approved BIPs are soft forks and hard forks. Soft forks are updates that do not conflict with the existing software, and are completely reversible if popular consensus is not achieved; hard forks are mandatory, irreversible updates, without which the program cannot be used [8].

Blockchain

The blockchain is a public, distributed ledger, which records every transaction that occurs in the Bitcoin network, negates the double-spend1 problem, functions in place of an intermediary [9], and is composed of a series of blocks, which in turn consist of groupings of transactions. (Figure 1) The blockchain is defined as "the longest path from any block to the genesis block" [10] with the distance referred to as the 'height'. Double-spend attacks are resisted using a distributed proof-of-work2-based service, which assumes that the processing power is shared among network users and that most of them are honest [7]. At this time, the blockchain is approximately 110 GB [11].

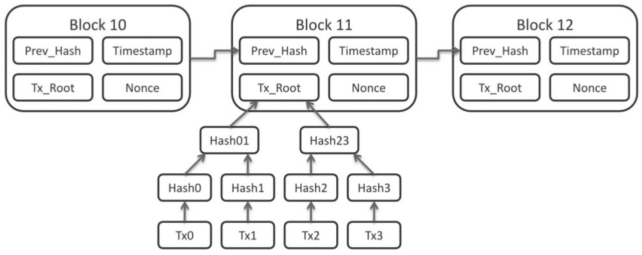

Figure 1: Blockchain structure.

Illustration of blockchain structure [12] used under Creative Commons Attribution-ShareAlike 3.0 Unported. Note that Prev_Hash represents the hash of the previous block, and Tx_Root is also referred to as the Merkle Root.

Blockchain technology is being considered separately for many applications, but its intrinsic function and value is in providing a mathematically demonstrable means of settling transactions between parties that do not trust each other without resorting to a 'trusted third party' [13].

The pseudonymous nature of Bitcoin is based on this ledger referring to aliases-Bitcoin addresses-as opposed to something more personally identifiable [14]. Bitcoin addresses are "directly derived from elliptic-curve public keys" [15] and a user can routinely have hundreds of different addresses, all managed by their wallet [14].

Each block contains a SHA-2563 hash of the previous block, which links blocks into a series, forming the blockchain, which traces all the way back to the genesis block [15].

Transactions

Electronic coins, in this case bitcoins, are defined as "a chain of digital signatures," [1] where each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin [1] (Figure 2) Elliptic key cryptography is used to instantiate public-key cryptography protocols because they offer smaller key sizes and more efficient implementation while preserving security levels [15].

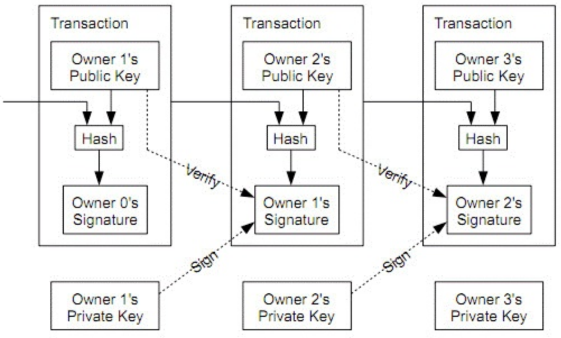

Figure 2: Bitcoin as a chain of digital signatures.

Demonstration of bitcoins as a chain of digital signatures, as various transactions is undertaken [1].

The transfer of bitcoins ownership from one user to another is accomplished by attaching, at the end of the new transaction, a digital signature (using the owner's private key) of the hash of the previous transaction and information about the new owner's public key [15]. This digital signature can be verified with the help of the owner's public key [15]. Transactions consist of three parts: the sender, the receiver and a digital signature (the 'witness') that verifies the sender's right to send the bitcoins [16]. After a transaction is created, it is broadcast to the Bitcoin network for validation and inclusion in a block [14].

Address re-use is the discouraged practice of using a single address for multiple transactions which reduces the privacy of both the user and other parties transacted with, and allows an observer to gather more information; organizations like the open bitcoin privacy project rate wallets partially on their ability to reduce such user behavior [17].

Multi-input transactions occur when a payment is being made by a user, but the amount of that payment exceeds the value in any given individual input address in that user's wallet, but not the user's balance [7]. Under these circumstances, the wallet will choose a set of BTCs from the multiple input addresses and prepare the transaction, which allowed the conclusion that all these addresses belong to the same user [7].

By default, a new shadow address is generated automatically by the main Bitcoin client when the total inputs exceed the required transfer amount, and 'change' is required; therefore, if there are old output addresses with a single new address (which has never before appeared), it is reasonable to conclude that this new address is a shadow address associated with the input address [7]. The use of shadow addresses is the only mechanism, other than its reliance on pseudonyms that Bitcoin employs to enhance user privacy [14].

Miners

Bitcoin miners are geographically distributed nodes of computers whose role is to solve complex proof-of-work problems to confirm transactions and secure the blockchain [18]. Mining is how bitcoins are 'created', and miners are awarded a periodically halving number of bitcoins, plus transaction fees, for their successes. For the first 210,000 blocks, approximately the initial four years, miners were rewarded with 50 bitcoins; during the next four years, the reward was 25 BTC. Now, the mining reward is 12.5 BTC, and that reward will be cut in half again around June of 2020 [19]. Ultimately, the limit of 21 million BTC will be mined, with the last new bitcoin expected to be created in 2140. At this point, the mining reward will consist of the transaction fees.

To generate a new block, a miner must find a nonce4 value, which, when hashed with the Merkle root5 of all valid and received transactions, the hash of the previous block, and a timestamp, results in a value below a threshold as determined by the network difficulty [14]. This new block is verified by the other users on the network who check the hash calculations, and, once deemed valid, it is appended to the blockchain [14].

The complexity of the proof-of-work problem ('difficulty') is adjusted every 2,016 blocks and increases with the rising processing power of miners to ensure that, on average, a block is solved every ten minutes. One of the implications of this is that hobbyists, and others that cannot afford a substantial investment in mining hardware, have limited computing power, and therefore are unlikely to ever solve the

Citation: Andrew LR, Douglas AO (2018) Bitcoin Investigations: Evolving Methodologies and Case Studies. J Forensic Res 9: 420. doi: 10.4172/2157-7145.1000420

proof-of-work problems on their own. Mining pools solve that issue, by grouping like-minded individuals together to combine their resources and share rewards earned in the ratio of computing power provided [20].

In the beginning, when difficulty was low, miners could use laptops or desktops to mine bitcoins. As competition increased, and difficulty rose, miners created multi-graphic card rigs to harness the power of graphics processing units (GPUs). The final evolution was to Application Specific Integrated Circuits (ASICs), which continue to race to smaller and smaller chips, and greater electrical efficiency, while adding more and more to their hashes/second rates. ASICs are essentially mandatory for BTC mining as the cost of electricity in using any previous method outweighs the value of the expected reward.

Mixing services

Governmental Bitcoin exchange regulation introduced identity verification, which was speculated to inadvertently lead to an escalation in the battle for privacy through the adoption of anonymizing services [21]. Mixing services include traditional centralized laundering services, which may operate with anonymity themselves and fail to deliver outputs [22] and newer decentralized approaches. Proposed mixing services, including CoinParty [23] and CoinShuffle [24] offer decentralized transaction anonymization services and possible plausible deniability in an attempt to defeat the work by Spagnuolo et al.

CoinJoin is trustless mixing protocol, which works intrinsically with bitcoin, that can mix bitcoins within a single transaction without needing a central service or trust in among the participants [25]. Its mechanism is based on the ability of signatures required in a transaction to be formed in a distributed manner by a like-minded group [26].

Mixing services may not complicate peer-to-peer network analysis [27], and have no bearing on wallet analysis. However, these services do bring unique challenges to transactional analysis, and without logs of who got which bitcoins, investigations are not feasible [28].

Other cryptocurrencies

Bitcoin is responsible for just under 70% of the cryptocurrency market capitalization despite the current existence of 694 different cryptocurrencies [29]. The other cryptocurrencies are known as 'Altcoins' as many are derived from bitcoin, sometimes with changes to the speed at which transactions are added, the cryptographic algorithm used, or the use of proof-of-stake6 in addition to proof-of work to record transactions [30]. Altcoins are occasionally proposed to address perceived shortcomings of Bitcoin and some go as far as to predict that Bitcoin will be usurped by cryptocurrencies with improved technical and security features [31].

Litecoin (LTC) is a popular altcoin, with a current market cap of over $500 million [29]. Its block time (transaction confirmation time) is four times as fast as bitcoin at 2.5 minutes, it will ultimately have four times the number of coins in circulation as bitcoin, and it uses sCrypt7 as opposed to SHA-256 as the primary encryption scheme [32]. The use of sCrypt was designed to prevent or slow the adoption of ASICs-based mining (to avoid concentration of mining power), through its heavy use of RAM [32], but this was ultimately unsuccessful as Litecoin ASICS emerged in 2014.

As most altcoins are forks of either Bitcoin or Litecoin, an investigator can use very similar approaches and slightly modified tools to examine them.

Investigations

Network analysis

Background

Network analysis is the study of the Bitcoin peer-to-peer network. Much of the research to date has been focused on the goal of testing or improving Bitcoin user privacy, and CoinSeer was developed as a custom Bitcoin client to perform data collection for network analysis [33].

When a user first turns on a Bitcoin client, it attempts to connect with its peers using a hard-coded list, while at the same time sending out an addr message containing its own IP address and port to advertise its presence and permit other nodes to initiate connections [33]. The client can also send to a connected user a getaddr message to request the connected user's known peers, to which the connected user can reply with up to 1,000 addr messages, allowing the client to initiate additional connections [33].

The network uses a gossip protocol propagation method [33] to update and synchronize nodes' ledger replicas by signalling to its neighbours the availability of transaction and block messages with an inv message, to which an interested node can reply with a get data message [10]. The first node is called the 'origin', and each hop in broadcasting incurs a 'propagation delay' comprised of transmission time and verification time. It was found to take any given block about two weeks to reach everyone on the network [33].

Methodologies

Peer-to-peer network analysis has met with some success in linking transactions to IP addresses, but requires a long-term, live connection to the Bitcoin network, or the results of a previous connection from software such as CoinSeer [27].

Gavin Andresen, Chief Scientist at the Bitcoin Foundation explained the privacy risk of network monitoring:

Unless you are very careful in the way you use Bitcoin (and you have the technical know-how to use it with other anonymizing technologies like Tor or i2p), you should assume that a persistent, motivated attacker will be able to associate your IP address with your bitcoin transactions [34].

Early research showed that opening a connection to all public peers on the network simultaneously allowed mapping of IP addresses to Bitcoin addresses based on the assumption that "the first node to inform you of a transaction is the source of it. . . [this is] more or less true, and absolutely over time" [35]. At that point, even if 50,000 connections were required, it could be done in Python, with the bonus that this allowed an acceleration of one's own transactions, as they could be pushed to everyone at once [35]. Currently, there are less than 7,000 nodes [36], suggesting that this approach is feasible.

CoinSeer was built as a custom client with three components; the Collector was made to connect with all active nodes, collect all addr messages and send getaddr messages to each newly connected peer, and collect a total of nine different types of messages [35]. Data collected, including meta-data such as timestamp, sender IP and port, were stored in binary files and passed to the second component, the Parser, which deconstructed the files and put them into comma-separated files for loading into the database [35]. The third component of CoinSeer was analysis, which allowed for data summary, transformation and visualization [35]. Handshakes like partial fingerprints, which include blockchain height, client name and timestamp, may be used to connect isolated, anomalous events such as a node transmitting, from different IP addresses over time, a specific double-spend transaction, which was rejected by peers, and therefore not recorded elsewhere [35].

For five months, from July 24, 2012 to January 2, 2013, CoinSeer connected to a median of 2,678 peers and collected 60 GB of data per week, ultimately resulting, using highly conservative constraints, in the mapping of between 252 and 1,162 Bitcoin addresses to the IP addresses that likely owned them [27].

Koshy et al. concluded that the use of mixing services did not affect their methodology. The use of online eWallets, which own the Bitcoin address instead of the user, resulted in the Bitcoin address being associated with the eWallet's IP address [27]. However, the eWallet service provider then is a chokepoint, whose user information may be vulnerable to being compelled by law enforcement [27].

Case Study

Using CoinSeer, over 90% of the time, when analyzing peer-to-peer network traffic activity, the pattern was 'multi-relayer, non-rerelayed transactions', but some atypical behavior was noted [27]. In one case, a transaction was relayed from a single IP, and never relayed again; which is very unusual for the "gossip" protocol, with only 2.5% of transactions following a single-relayer pattern; in this case ownership of the attempted transaction is attributable to the IP address, but never appears in the blockchain [27]. This case demonstrates the intelligence-gathering and non-targeted nature of network analysis, though the information may be of investigative use afterwards.

Transactional Analysis

Background

Transactional analysis is primarily the study of the blockchain. An early paper digested all Bitcoin transactions to date, with an emphasis on transactions that were greater than 50,000 Bitcoins, concluded that almost all those transactions were descendants of a single 90,000 BTC transaction from November 2010 [18].

Another early paper studying anonymity and privacy on the bitcoin network noted the gap between actual and potential anonymity, and using transactional analysis, concluded that significant effort would be required to defeat their clustering heuristic based on bitcoin change addresses. The work of Meiklejohn [20] was augmented into a more automated and scalable modular framework called BitIodine [28] which incorporated classification and labelling, attempted to identify users through web scraping, and was tested successfully on several real-world cases.

A recent paper studied the privacy risks associated with the use of cryptocurrencies to make web payments [37] and showed that third-party web trackers typically have sufficient information to uniquely identify the transaction on the blockchain, and connect it to the user's cookie and actual identity. Further, if two purchases from the same user were identified, their entire cluster of transactions and addresses on the blockchain could be identified, despite use of the CoinJoin protocol or similar [37].

Methodologies

Transactional analysis offers the advantage of not requiring a live connection to the Bitcoin network, and instead is retrospective in nature as it uses a collection of the blockchain, and analysis with tools such as BitIodine [38]. Transactions can be manually reviewed on websites such as Blockchain.info or WalletExplorer.com.

Clustering is used to attempt to identify groups of addresses that belong to a single user. Heuristic I is multi-input transactions, and Heuristic II is shadow (or change) addresses. Use of both heuristics in an early study of the first 140,000 blocks of the blockchain (up to August 2011) resulted in grouping approximately 58% of bitcoin addresses with an average of 11.55 addresses per cluster [14]. Evasion of Heuristic I was concluded to be very difficult, as it is a basic operation of bitcoin [39]. Heuristic II could be evaded by returning change to the sender's address, but this would decrease the user's privacy through strengthening Heuristic I [14].

The validity of the assumption of Heuristic I where multi-input transactions are linked to a single user, is now questionable through the existence of the coin join protocol and some evidence of its use [26].

Integration of off-network information, such as publicly available information, and voluntary disclosures of bitcoin addresses from sources like forums and Twitter, allows even more mapping of Bitcoin addresses to identity information [40].

Orders books are normally available to support trading tools, and bitcoins on Bitcoin exchanges are often converted from other currencies, and result in a precise decimal value, with eight significant digits, which may be unique enough to map the transaction to a public key and associate it with the exchange [40].

Temporal analysis whereby public keys are used repeatedly at the same time may further associate a group of addresses with a single user [40].

The passive, retroactive techniques used to identify users based on Bitcoin web payments leverage online tracking through both leaks and intentional dissemination to third-parties [39]. This information would have to be compelled from the trackers and third parties for analysis. Online trackers have visibility into sensitive details of payment flows, including items' prices and identities, and this can provide sufficient information to uniquely link the transaction to the blockchain [39]. Furthermore, as per Goldfeder et al. [39] this information can be leveraged to illuminate the user's other web activities through tracking cookies, and to other bitcoin transactions through clustering techniques. In many cases, merchants send transaction-specific Bitcoin addresses, making it trivial to link to the blockchain, or provide personally identifiable information (PII) for advertising and analytics purposes [39]. Extraction of PII and Bitcoin addresses by malicious trackers is another possibility [39].

Another form of transactional analysis is active analysis, where the investigator actively participates in the network, through deploying and tracking identified 'marked' bitcoins through transactions to discover addresses, possibly in collaboration with other users, or by operating a mixing service [40]. It is therefore clear that large services, like exchanges, wallet services and mixing services have the capability to track and identify a large subset of user activity [40].

BitIodine was designed as a collection of modules to parse, cluster, classify and visualize Bitcoin transactions and was successfully used to identify a likely cold storage Silk road (an infamous black market in the deep web) wallet with over 111,114 BTC, and quantify ransoms paid for CryptoLocker releases totaling 375.93 BTC [28]. Unfortunately, BitIodine is no longer being actively developed [41], though Spagnuolo is continuing to work on a new clusterizer [42].

Case Study

Carl M. 'French Maid' Force, former DEA agent involved in the Silk road investigation that eventually led to the conviction of Ross 'Dread Pirate Roberts' Ulbricht [41] was himself charged [42] and subsequently pleaded guilty to extortion, money laundering and obstruction of justice [43]. It was the blockchain investigative prowess of Special Agent Tigran Gambaryan of the IRS, using Blockchain.info and WalletExplorer.com, who provided, in Exhibit B of his criminal complaint [44] an elaborate tracing of all bitcoin transactions totaling 525 BTC through multiple addresses from Ulbricht to force (Figure 3).

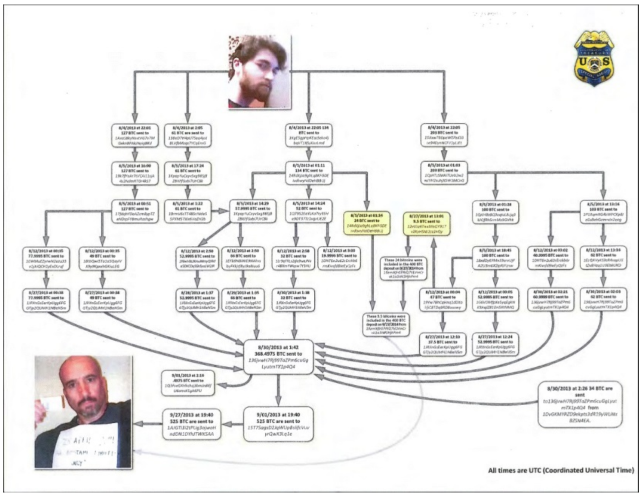

Figure 3: Bitcoin transaction tracing.

Exhibit B from the criminal complaint, issued by Special Agent Tigran Gambaryan of the IRS against Carl M. Force, tracing transactions totaling 525 bitcoins from Ulbricht to Force, detailing addresses, amounts, and date/time stamps [45].

Wallet Analysis

Background

The Bitcoin wallet is where private keys are stored, and allows the user to conveniently conduct Bitcoin transactions. Wallets automate the mechanics of sending and receiving bitcoins and are referred to as a 'client' when they actively participate in the network. Lightweight wallets save on disk space and bandwidth by not keeping a comprehensive copy of the blockchain, unlike full node wallets [46]. Instead, as of the second half of 2011, simplified payment verification (SPV) was implemented to allow for lightweight wallet use [47]. Some concerns have been expressed regarding potential loss of privacy associated with SPV clients [47].

There are many different forms of wallets, all of which are designated as hot (connected to the internet) or cold (offline). Cold wallets are obviously more secure, and are used for long-term holdings, while hot wallets are for regular use. Wallets can be desktop, mobile, web, physical, hardware, or Bitcoin clients [48]. Web-based wallets avoid the need to download the entire blockchain, but, depending on where the private keys are stored, the user may be trading convenience for security [47].

Methodologies

Complete wallet analysis of the original Bitcoin client does not require having possession of the wallet's (optional) passphrase to perform its decryption; passwords are only required to initiate transactions, as using a passphrase encrypts just the private keys [47]. Many artefacts, regardless of wallet encryption, can be recovered using forensic tools, such as the python script BTCscan [48] and Magnet Forensics' IEF or Axiom products [49].

The use of Magnet Forensics' IEF or Axiom products allows an investigator to recover addresses associated with the wallet, the 'labels' or comments that the user may have added for convenience (both from the wallet.dat file), and queries on the Bitcoin network (from debug.log) which may or may not relate to local user activity [49]. There may also be backup wallet files, which can be named anything, but at least in the case of the common Bitcoin-Qt (now Bitcoin Core) client, offset 0x12 contains the string 'b1' [50].

Case study

Ross Ulbricht was arrested in the science fiction section of Glen park public library in San Francisco on October 1, 2013, with his laptop open and logged into Silk Road's internal Staff Chat as 'dread' [51]. During the trial, the FBI forensic examiner, Thomas Kiernan testified that the laptop was seized while unencrypted, and the wallet.dat file was found on the laptop and on an encrypted USB drive as a backup [52] FBI Special Agent Ilhwan Yum testified about the government's access to the Silk road wallets and Ulbricht's laptop wallet, and alluded to the ease of performing an analysis to see if Silk road bitcoins had been transferred to Ulbricht's personal wallet [52]. Yum testified that, on behalf of the FBI, he had seized 20,000 BTC from the Iceland Silk road server and 144,000 BTC from the Ulbricht's laptop wallet [52], which requires access to the private keys, meaning the wallet itself was not encrypted. Ulbricht was ultimately convicted of seven charges relating to engaging in a criminal enterprise, drug trafficking, and money laundering, and sentenced to life in prison [53].

Emerging issues and future directions

There are issues related to the general evolving nature of Bitcoin through the BIP process and specific changes that will impact investigators and their tools. One current issue is Segregated Witness (SegWit) versus Bitcoin Unlimited, which centers on block size, and Bitcoin's ability to scale to process large numbers of transactions. SegWit was proposed by Bitcoin Core developers in BIP 141 [54] and creates a structure containing validation data (also called the witness data) separate from the transaction data itself, introducing a new transaction format that will increase the transaction capacity of each block. SegWit can be implemented with a soft fork. Bitcoin Unlimited is a hard fork approach supported by many miners which removes the Bitcoin Core hard-coded block size limit of 1 MB to a consensus sized block [8] Regardless of which approach is ultimately instituted, current blockchain parsing methods may be impacted, impairing the performance of investigative tools.

A review of previous papers, including Meiklejohn et al. [20], Spagnuolo et al. [28], and [27], concluded that blockchain transactional analysis, the more difficult peer-to-peer network traffic analysis, and bitcoin mixing services still have room for further research, though caution was advised in the mixing services realm as development could have legal ramifications related to money laundering [55].

A final component to the discussions around methodologies is the attempt to standardize and reach general acceptance, so that scientific evidence testimony would be admissible in US courts under Frye [56], Kelly (in California) [57] or Daubert [58] standards. Current investigative techniques specified which require elevation to pass the admissibility tests include network analysis, and transactional graph analysis [59].

Conclusions

Three main investigative approaches were discussed. Network analysis is highly technical, somewhat experimental, and very nonspecific in its targets. The network surveillance must be in place, or recorded, for the period being studied, and can be defeated by anonymizing technologies like Tor, i2P or VPNs. A wide net must be cast, comprising of all active Bitcoin clients, to glean information that can lead to the connection between a bitcoin address and an IP address. This technique may gain traction in the future, once supporting research emerges to validate the pioneering work, which would allow it to be entered into the court as scientific evidence. Meanwhile, for those with the technical expertise and the resources, this technique is useful for intelligence gathering.

Transactional analysis has the advantage of retroactive access, but contains a wide range of tools to be mastered. It is very suited, and reasonably straightforward, for working with addresses known to be associated with a person of interest, but is meeting more challenges, especially to clustering assumptions around multi-input transactions given the CoinJoin protocol and presence of mixing services. However, analysis techniques like web scraping for off-network identity information, unique BTC quantity examination, temporal connections, and active participation, are all still effective. Overall, the quest for privacy in Bitcoin transactions, especially by sophisticated users, is meeting with success.

Wallet analysis has generally-accepted tools available to allow an investigator to confidently tie transactions to a wallet, regardless of whether the wallet is passphrase-protected. Expert witness testimony on methodologies and findings is feasible.

Overall, more research and tool development is still desirable to achieve general acceptance. Tools that are easy to understand and use are required for investigators, or alternatively, services that provide collection and analysis of Bitcoin activity are needed. Bitcoin appears to be here to stay, so it is expected that Bitcoin investigation will continue in the foreseeable future to require significant expertise, be time-consuming and therefore costly.

References

1. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system.
2. Nakamoto S (2008) Bitcoin P2P e-cash paper.
3. Doran MD (2014) A forensic look at Bitcoin cryptocurrency. Utica College, USA.
4. Dai W (1998) b-money.
5. FBI intelligence assessment (2012) (U) Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity.
6. Nakamoto S (2009) Bitcoin v0.1 released.
7. Gervais A, Karame G, Capkun S, Capkun V (2014) Is Bitcoin a decentralized currency? IEEE Secur Priv12: 54-60.
8. Beigel O (2017) Segwit vs. bitcoin unlimited and bitcoin's fork explained simply.
9. Brito J, Castillo A (2013) Bitcoin: A primer for policymakers. Mercatus center, George Mason University, USA.
10. Decker C, Wattenhofer R (2013) Information propagation in the bitcoin network. IEEE Xplore: 1-10.
11. Blockchain size (2017).
12. Wander M (2013) File: Bitcoin block data.svg.
13. Laskowski M, Kim HM (2016) Rapid prototyping of a text mining application for cryptocurrency market intelligence. Information reuse and integration (IRI), 2016 IEEE 17th International Conference IEEE: 448-453.
14. Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S (2013) Evaluating user privacy in bitcoin. International conference on financial cryptography and data security, Springer berlin heidelberg: 34-51.
15. Bos JW, Halderman JA, Heninger N, Moore J, Naehrig M, et al. (2014) Elliptic curve cryptography in practice. International conference on financial cryptography and data security, Springer berlin heidelberg: 157-175.
16. Beigel O (2016) What is Segwit? (Segregated Witness).
17. Open Bitcoin Privacy Project (2016) Bitcoin wallet privacy rating report. 2nd edn.
18. Ron D, Shamir A (2013) Quantitative analysis of the full bitcoin transaction graph. International conference on financial cryptography and data security, Springer berlin heidelberg: 6-24.
19. Bitcoin block reward halving countdown (2017).
20. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, et al (2013) A fistful of bitcoins: Characterizing payments among men with no names. Proceedings of the 2013 conference on internet measurement conference, ACM: 127-140.
21. Matonis J (2013) The politics of bitcoin mixing services.
22. Category: Mixing services (n.d)
23. Ziegeldorf JH, Grossmann F, Henze M, Inden N, Wehrle K (2015) CoinParty: Secure multi-party mixing of bitcoins. Proceedings of the 5th ACM conference on data and application security and privacy, ACM: 75-86.
24. Ruffing T, Moreno-Sanchez P, Kate A (2014) CoinShuffle: Practical decentralized coin mixing for bitcoin. European symposium on research in computer security, Springer international publishing: 345-364.
25. Maxwell G (2013) CoinJoin: Bitcoin privacy for the real world.
26. Meiklejohn S, Orlandi C (2015) Privacy-enhancing overlays in bitcoin. International conference on financial cryptography and data security, Springer berlin heidelberg: 127-141.
27. Koshy P, Koshy D, McDaniel P (2014) An analysis of anonymity in bitcoin using p2p network traffic. International conference on financial cryptography and data security, Springer berlin heidelberg: 469-485.
28. Spagnuolo M, Maggi F, Zanero S (2014) BitIodine: Extracting intelligence from the bitcoin network. International conference on financial cryptography and data security, Springer berlin Heidelberg: 457-468.
29. CryptoCurrency market capitalizations (2017).

30. Gandal N, Halaburda H (2014) Competition in the cryptocurrency market.
31. Iwamura M, Kitamura Y, Matsumoto T (2014) Is Bitcoin the only cryptocurrency in the town? Economics of cryptocurrency and Friedrich A. Hayek.
32. Ahamad S, Nair M, Varghese B (2013) A survey on crypto currencies. 4th International conference on advances in computer science, AETACS: 42-48.
33. Koshy P (2013) CoinSeer: A telescope into bitcoin. The Pennsylvania State University, USA.
34. Chester J (2015) How questions about terrorism challenge bitcoin startups, Forbes.
35. Kaminsky D (2011) Black Ops of TCP/IP. Black Hat, Chaos communication camp.
36. Global Bitcoin nodes distribution, (2017).
37. Goldfeder S, Kalodner H, Reisman D, Narayanan A (2017) When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, ArXivar.
38. Reid F, Harrigan M (2013) An analysis of anonymity in the bitcoin system. Security and privacy in social networks, Springer New York: 197-223.
39. Spagnuolo M (2016) mikispag/bitiodine.
40. Spagnuolo M (2017) mikispag/rusty-blockparser.
41. US v Ulbricht, No.14-cr-68 (KBF) S.D.N.Y (2014).
42. US v. Force, No.15 CR 319 RS N.D. Cal (2015).
43. Queally J (2015) Ex-DEA agent pleads guilty to stealing bitcoins during silk road investigation. Los Angeles Times.
44. Gambaryan T (2015) Criminal complaint.
45. Gervais A, Capkun S, Karame GO, Gruber D (2014) On the privacy provisions of bloom filters in lightweight bitcoin clients. Proceedings of the 30th annual computer security applications conference, ACM: 326-335.
46. Nyairo D (2015) 7 types of Bitcoin wallets, Coin Outlet.
47. Skudnov R (2012) Bitcoin clients. Turku University of Applied Sciences, USA.
48. Cohen C (2015) Forensics and bitcoin, Forensic Focus.
49. Saliba J (2013) Bitcoin forensics-A journey into the dark web. Magnet Forensics.
50. Saliba J (2013) Bitcoin forensics part II: The secret web strikes back. Magnet Forensics.
51. Greenberg A (2015) Undercover agent reveals how he helped the FBI trap silk road's ross Ulbricht. Wired.
52. United States of America v. Ross William Ulbricht trial transcript. (2017) Silk Road Tales and Archives.
53. Walker L (2015) Silk Road mastermind gets life prison sentence. Newsweek, USA.
54. Lombrozo E, Lau J, Wuille P (2015) bitcoin/bips. GitHub.
55. Herrera-Joancomartí J (2015) Research and challenges on bitcoin anonymity. Data privacy management, autonomous spontaneous security, and security assurance, Springer International Publishing: 3-16.
56. Ordsel V. Frye v. United States, 293 F. 1013 (Court of Appeals, Dist. of Columbia 1923).
57. People v. Kelly, 549 P.2d 1240 (17 Cal. 3d 24, 130 Cal. Rptr. 144 1976).
58. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (113 S. Ct. 2786 125 L. Ed. 2d 469 1993).
59. Imwinkelried EJ, Luu J (2015) The challenge of bitcoin pseudo-anonymity to computer forensics. Criminal Law Bulletin, UC Davis Legal Studies Research Paper No. 462.