Newcastle University

COMPUTING SCIENCE

Bitcoin: Perils of an Unregulated Global P2P Currency

Syed Taha Ali, Dylan Clarke and Patrick McCorry

TECHNICAL REPORT SERIES

No. CS-TR-1470 May 2015

TECHNICAL REPORT SERIES

No. CS-TR-1470 **May, 2015**

Bitcoin: Perils of an Unregulated Global P2P Currency

Syed Taha Ali, Dylan Clarke, Patrick McCorry

Abstract

Bitcoin has, since 2009, become an increasingly popular online currency, in large part because it resists regulation and provides anonymity. We discuss how Bitcoin has become both a highly useful tool for criminals and a lucrative target for crime, and argue that this arises from the same essential ideological and design choices that have driven Bitcoin's success to date. In this paper, we survey the landscape of Bitcoin-related crime, such as dark markets and bitcoin theft, and speculate about possible future possibilities, including tax evasion and money laundering.

Printed and published by Newcastle University,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

ALI, S, T; CLARKE, D; MCCORRY, P;
Bitcoin: Perils of an Unregulated Global P2P Currency
[By S. T Ali, D. Clarke, P. McCorry
Newcastle upon Tyne: Newcastle University: Computing Science, 2015.

(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1470)

Added entries

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR-1470

Abstract

Bitcoin has, since 2009, become an increasingly popular online currency, in large part because it resists regulation and provides anonymity. We discuss how Bitcoin has become both a highly useful tool for criminals and a lucrative target for crime, and argue that this arises from the same essential ideological and design choices that have driven Bitcoin's success to date. In this paper, we survey the landscape of Bitcoin-related crime, such as dark markets and bitcoin theft, and speculate about possible future possibilities, including tax evasion and money laundering.

About the authors

Taha Ali obtained his BSc. (Eng) from GIK Institute, Pakistan in 2002. He completed his M.S., and Ph.D. in Electrical Engineering in the University of New South Wales, Australia, in 2006 and 2012 respectively. He is currently a Research Associate in the School of Computing Science, Newcastle University, UK. His research interests include e-voting, cryptocurrencies, body area networks, and software defined networking.

Dylan Clarke received MMath, MSc and PhD degrees from Newcastle University. He has a background in web application and CRM system development for local government. He is currently a Research Associate with Newcastle University. His research interests include e-voting, security, dependability and distributed algorithms.

Patrick McCorry received his BSc. (Hons) Computer Science from Newcastle University and is currently a research student at Newcastle University. His background involves working on middleware to support transaction servers while working for IBM. His research interests include cryptocurrencies, distributed systems and cryptography.

Suggested keywords

BITCOIN
CRYPTOCURRENCIES
DARK MARKETS
RANSOMWARE

Bitcoin: Perils of an Unregulated Global P2P Currency

Syed Taha Ali, Dylan Clarke, Patrick McCorry

School of Computing Science
Newcastle University, UK
{taha.ali,dylan.clarke,patrick.mccorry}@newcastle.ac.uk

Abstract. Bitcoin has, since 2009, become an increasingly popular online currency, in large part because it resists regulation and provides anonymity. We discuss how Bitcoin has become both a highly useful tool for criminals and a lucrative target for crime, and argue that this arises from the same essential ideological and design choices that have driven Bitcoin's success to date. In this paper, we survey the landscape of Bitcoin-related crime, such as dark markets and bitcoin theft, and speculate about possible future possibilities, including tax evasion and money laundering.

1 Introduction

Bitcoin emerged in 2009 with the aim to provide a secure and independent currency alternative to the global financial infrastructure, which has seen massive downturns and scandals in recent years. In the words of Bitcoin creator, Satoshi Nakamoto:

> *"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."* [1]

To realise this libertarian agenda, Bitcoin was envisaged as a trustless decentralized network where all transactions are cryptographically verified by users and recorded in a decentralized ledger. This ledger, the blockchain, is populated by miners who compete in a lottery-style contest. So far the Bitcoin experiment has been very successful in certain respects: users have ownership over their wealth, third parties cannot manipulate currency creation, transaction fees are very low, and users can achieve a certain measure of anonymity.

These factors contributed to a surge in Bitcoin's popularity after the Cyprus banking crisis where the government authorized banks to impose losses on shareholders and large depositors. Bitcoin, trading at US$40 rose to US$200 as a result, and shortly after, soaring Chinese demand pushed it up further, at one point past the US$1000 mark. Bitcoin prices now hover around the $350 mark [2], and the current market cap is at $4.7 billion [3]. Bitcoin is also gaining traction with vendors. Prominent brands such as Dell, WordPress, Paypal and Microsoft now offer Bitcoin payment options [4] and Bitcoin payment processors, such as Coinbase and BitPay, are seeing record growth and expansion. However, Bitcoin has also received substantial negative press due to its role in powering dark markets such as Silk Road. High-profile hacks of Bitcoin exchanges have resulted in thefts of hundreds of thousands of coins belonging to customers.

In this paper, we argue that these negatives should essentially be understood as the flip side of Bitcoin's key strengths, its ephemeral, trustless and distributed nature. We survey the range of Bitcoin-related criminal activity, such as dark markets, online extortion, malware, and theft, and highlight how these threats derive from the same fundamental qualities that have thus far also defined Bitcoin's success. We observe that this criminal activity is growing rapidly, becoming increasingly diverse and sophisticated, and presenting us with a variety of new ethical and legal dilemmas.

Many of these issues were not foreseen by the Bitcoin community, and we anticipate more will emerge as adoption increases. Visualizing these threats as a natural consequence of Bitcoin's ideology and design choices also allows us to speculate about future threats before they occur. We discuss distinct future possibilities such as tax evasion, money laundering, and esoteric scenarios where the Bitcoin P2P network itself may be exploited for criminal activity.

In conclusion, we observe that this ideological conflict within Bitcon is likely the reason that proposed solutions to these threats are falling short.

2 Bitcoin and Crime

We begin by describing how Bitcoin has triggered a boom in online black markets by effectively 'de-risking' illegal transactions.

2.1 Dark Markets

Silk Road: Silk Road was an anonymous online drug market, accessible to the general public from July 2011 [5]. A combination of technologies, including Bitcoin, were used to protect anonymity with the goal that the identity of sellers would be protected absolutely, whereas buyers would need to provide sellers with a physical shipping address for the product. If law enforcement officers infiltrated the site as sellers they may be able to obtain addresses for buyers, but no information about sellers (a higher value target) other than what may be leaked from the content of the seller's communications or the packaging of the shipment.

Silk Road was only accessible as a TOR hidden service [6], thereby preventing users from discovering the IP address of the site, and also preventing outside observers from discovering that a particular user had accessed the site. Payments were made using Bitcoin, thereby preserving anonymity of all parties, and an escrow service was provided to give buyers more confidence in their dealings [7]. The site also provided advice on how to package drugs to bypass common detection methods, and the site owners actively encouraged community discussion about the quality of sellers and related customer experiences. The website interface and user experience was modelled on the pattern of legitimate online marketplaces, such as eBay and Amazon. In testimony to its success, Silk Road was widely acknowledged as the 'eBay of drugs' [8], making it "easier and faster to order drugs than it is to order a pizza" [9], and raking in an estimated annual revenue of $1.2 billion.

Dark Markets go Mainstream: Silk Road was shut down by the FBI in October 2013 after the arrest of the alleged owner of the site. Silk Road 2.0 was launched soon after and then shut down [10], and currently a Silk Road 3.0 site is available. However, there has been a massive surge in the number of sites selling drugs online using the Silk Road model, and the overall effect is that even the online drugs marketplace has now, in a sense, become decentralized. Researchers at the Digital Citizens Alliance [11] note that when Silk Road was taken down, there were four dark markets dominating the landscape and totalling about 18,000 drug listings. A year later, in October 2014, a dozen large markets accounted for some 32,000 drug listings, alongside a significant increase in advertisements for other illicit goods such as weapons. There is now even a dedicated Google-style search engine [12] which allows buyers to compare listings across multiple dark markets.

Since these sites exist as TOR hidden services, their addresses can be publicly posted. This not only makes them easy to find for the novice Internet user but also allows users to post reviews of suppliers on public message boards. This has bizarrely enough resulted in a situation where customer service and product quality are now key differentiators between drug suppliers. Customers openly discuss their experiences with different suppliers on public forums. Some even post results of chemical tests they have performed on the product they purchase.

This new phenomenon also raises complex new challenges for existing drug laws. Online customers are usually unaware of the location from which drugs will be shipped, and even when they are aware, this may be less of a consideration than testimonials of good customer service and drug purity. However, in many countries the laws prescribe harsher penalties for the import of prohibited drugs than they do for possession. Likewise, when buying drugs online with high packaging costs, it may be economical for suppliers to offer larger quantities at discounts, and for buyers to make larger and less frequent purchases. This may result in prosecution of those who buy drugs for personal use under laws intended to target suppliers [9].

De-risking Crime: Analyzing Silk Road in greater detail, researchers Aldridge and Dcary-Htu contend that these "cryptomarkets" are a "paradigm shifting criminal innovation" in that, by facilitating anonymous virtual transactions, they overcome the dangerous physical limitations of the drug trade, effectively de-risking the enterprise [7]. Physical drug deals are known to put the purchaser at an increased risk of violent crime [13], especially if they require the individual to deal with people from a culture where they do not understand cultural norms of behaviour [14]. Purchasing drugs online using Bitcoin as per the dark market business model and receiving them in the mail eliminates the need for users to visit drug dealers in person and is therefore much safer. This contrast is graphically highlighted if one considers the lifestyle of alleged Silk Road mastermind Ross Ulbricht [15]. Ulbricht was arrested at a local public library, in the science fiction section where he would oversee Silk Road's daily operations on his laptop using the library's public WiFi. This is a far cry from the stereotypical image of a typical drugs broker, running a billion dollar empire, and surrounded by bodyguards and hitmen.

Expanding on this theme, Infante speculates that the use of Silk Road may even have reduced incidences of death and other harm associated with cross-border drug smuggling . He estimates some 1,200 deaths potentially related to drug-violence may have been prevented over the course of the three years that Silk Road was in operation [16].

2.2 Theft and Malware

We next examine how Bitcoin's global reach has opened up new opportunities for online theft, extortion, and triggered a massive upsurge in malware.

Hacking Bitcoin Exchanges: Unlike traditional currencies, bitcoins exist exclusively as virtual assets and transactions, once made, are irreversible. This makes Bitcoin a fair target for hackers and scammers. Sophisticated attacks on Bitcoin exchanges, the cryptocurrency equivalent of bank heists, are now common. The MtGox saga has received significant media coverage. In February 2014, MtGox, the largest Bitcoin exchange in the world at the time, handling approximately 80% of all Bitcoin transactions, was allegedly hacked (or the victim of some other kind of fraud) and shut down shortly after [17]. 850,000 bitcoins belonging to customers were stolen, with a value of more than half a billion dollars. This significantly impacted user confidence in Bitcoin, which was correlated with a drop in Bitcoin value.

The list of Bitcoin exchanges and wallet services that have been successfully hacked and driven to collapse also includes names such as Bitcoinca, BitFloor, Flexcoin, Poloniex and Bitcurex. In a paper on the topic, researchers Tyler Moore and Nicolas Christin quantify the risks and hazards associated with Bitcoin exchanges and note that of 40 Bitcoin exchanges established recently, 18 soon shut down [18]. Several hundreds of thousands of dollars worth of customers' coins were stolen or lost in these incidents. Some of these sites were guilty of poor security design and practices, but it is also believed that hacks are becoming increasingly sophisticated. At the time of writing another incident involving the BitStamp exchange has been announced with 5 million dollars in losses [19].

Malware: Researchers from Dell recently reported [20] that 146 strains of malware have thus far been discovered that are designed to steal bitcoins from victims' computers. Around 50% of these successfully bypass most antiviruses. This count is up from 13 such strains discovered in 2012 and the rate of malware creation has loosely tracked the surge in Bitcoin exchange rate. These malware search victims' machines for common wallet formats to steal their private keys. Some advanced variants are equipped with keyloggers to target password-protected wallets. Yet another strain switches Bitcoin addresses on the fly when users' copy an address to the clipboard while making payments, replacing them with the malware owner's address, thereby diverting the payment to him [21].

Ransomware: In 2004, Young and Yung first suggested the idea of a virus that encrypts data on victims' computers using an asymmetric cipher and holds it hostage for ransom [22]. The decryption key is not embedded in the virus codebase, so the attack cannot be reverse-engineered. However, ransom payments had to traverse the traditional financial infrastructure which risked exposing the owner of the malware and therefore this scheme had limited appeal. However, Bitcoin's anonymity, independence of centralized authorities, and global accessibility makes it the ideal solution.

As a result, ransomware is now thriving. CryptoLocker, a ransomware trojan which demanded payment in bitcoins, was first observed in September 2013. CryptoLocker claimed 250,000 victims and earned an estimated $30 million in just 100 days [23]. It has since then spawned an entire family of malware. A variant, CryptoWall, infected over 600,000 systems in the past six months, holding 5 billion files hostage, earning attackers more than US $1 million. CryptoWall even infected the systems of official government departments. The office of the Dickson County Sheriff in the US paid the ransom in full to decrypt their archive of case files. Durham Constabulary in the UK has refused [24].

In a recent blogpost, researchers at McAfee Labs point out that this class of ransomware is now being crowdsourced. Tox [25] is a free and easy-to-deploy ransomware kit that 'customers' can download from a website and use to deliberately infect computers belonging to others. Tox uses TOR and Bitcoin, it resists typical malware detection tools, and can be customized, prior to installation, as to the amount of ransom the malware charges. The Tox website tracks all installations and charges 20% of any claimed ransoms. The authors note that other classes of malware may soon incorporate this crowdsourcing and profit-sharing model.

Bitcoin Mining: Malware have also been discovered which covertly mine cryptocurrencies on victims' machines. These malware either mine independently or participate in public or dark mining pools, connecting either directly or through proxies [26]. Customized malware builds have also been found for smartphones, webcams, and even network storage devices. One botnet successfully utilized network attached storage devices over a two month period to mine $600,000 worth of Dogecoin, a Bitcoin inspired alt-currency [27].

However, in the case of Bitcoin, mining malware is no longer proving a profitable venture given the increased block difficulty level and the rise of mining pools, and some commercial botnets which offered mining services (such as ZeroAccess) have now stopped offering mining as a service.

3 Future Threats

Here, we briefly consider some hypothetical examples of criminal activity which derives directly from Bitcoin's anonymous and trustless nature. We observe that Bitcoin's lack of regulation facilitates tax evasion and money laundering. We also consider esoteric threats which use the Bitcoin P2P network.

Tax Evasion: In a panel discussion recently [28], when asked about Bitcoin enabling tax evasion, Princeton's Edward Felten commented: "You could argue that [Bitcoin] does [make it easier to avoid taxes] because it's a transaction that doesn't involve the banking system." However, he downplayed the risk: "The conspiracy to not report income has to be too large in a sizeable company, and the consequences of getting caught [for] the leaders are too large."

While this may be true for large corporations, it is not very difficult at the individual level to evade taxes. Due to the economic downturn, there is already a growing trend in underreporting taxes. Tens of millions of ordinary people, people who are not career criminals but instead nannies, fitness teachers, barbers, construction workers, etc. are increasingly participating in the shadow economy and working off the books. In 2013, economist Edgar Feige estimated that there was an estimated 2 trillion dollar gap in what Americans reported to the IRS - a huge sum when compared to a 385 billion dollar estimate by the IRS in 2006 [29]. This trend might increase: 30% of Americans today are self-employed and some predict this figure will rise to 50% by 2020 [30]). There is no way of knowing if income is taxable unless the recipient voluntarily reports it, and this growing freelance economy may prove very hard to track if they start transacting in Bitcoin.

Tax Havens and Money Laundering: There is also an ongoing discussion about Bitcoin functioning as a tax haven and its use in money laundering. Traditionally, tax evasion or money laundering would require criminals to divert funds through a complex financial maze involving multiple actors such as banks, shell companies, and offshore accounts. Governments in recent years have found it more effective not to target offshore tax havens directly, but to cooperate with foreign governments and attack links in the financial infrastructure, namely banks. A good example of this trend is the US Foreign Account Tax Compliance Act (FACTA) which targets tax cheats by requiring foreign banks to directly report to the US Internal Revenue Service about financial accounts held by US taxpayers [31]. Failure to do so exposes the bank to the risk of being penalized on its earnings from American investments.

However, Bitcoin, with its pseudonymity, its ephemerality, and its total independence of the banking infrastructure defeats this entire strategy. All that is required to successfully hide or launder funds with Bitcoin is a series of private anonymized transactions. There already exist 'laundry' services and tumblers which accept bitcoins from multiple sources and mix them in a way that the link between input and output addresses is broken.

Money laundering may not be an immediate threat due to Bitcoin's limited usage and high price volatility, but researchers have started to sound the alarm [32, 33]. The US government has applied money laundering rules to virtual currencies [34] and Europol, the EU law enforcement agency handling criminal intelligence, has requested greater policing powers [35] to meet this challenge.

Exploiting the Bitcoin Network: New research has shown that it is possible to exploit Bitcoin for non-payment purposes, such as timestamping data [36, 37] or building advanced financial services [38]. Likewise, we believe, threats will emerge which do not involve the currency but which use the underlying Bitcoin network. Some attacks have already been practically demonstrated.

Interpol has recently warned that the Bitcoin blockchain can serve as a vehicle for malware and illegal content [39]. In a demo at the Black Hat Asia conference, researcher Vitaly Kamluk, showed how a hacker may embed malicious payloads in the blockchain where it could be retrieved by malware on remote machines. In a similar vein, researchers have demonstrated that the Bitcoin P2P network can function as a reliable low-latency command-and-control (C&C) infrastructure to power botnets [40]. In existing botnets, C&C commands from the botmaster are typically delivered to bots over IRC networks, custom P2P protocols, or via HTTP sites. These communication channels are also therefore the botnet's key vulnerability, and allows security researchers and law enforcement to expose the botmaster and disrupt C&C communications.

In the case of Bitcoin-based C&C communications, the botmaster embeds commands in legitimate Bitcoin transactions using a variety of mechanisms (such as the transaction OP-RETURN field, subliminal channels, unspendable outputs, etc.) which are then dispatched over the Bitcoin network where bots may receive them. This has several advantages, most notably that it is far more robust and secure than current C&C methods. Disrupting C&C transactions in this case would not only violate the ideology Bitcoin was built upon, but it would likely impact legitimate Bitcoin users and significantly affect network usability as a whole. Botmasters also stand to benefit from greater anonymity and less risk using the Bitcoin network for C&C communications.

4 Discussion

As we observe from this brief overview of Bitcoin-related criminal activity, current and future, Bitcoin's strengths and weaknesses both derive from the same essential ideological and architectural design choices. For this reason, we believe there are no easy solutions to the problems we have discussed so far. Anonymity and lack of regulation which is meant to free users from central authorities also empowers drug dealers and money launderers. Denoting money as virtual assets to remove reliance on banks also opens the doors to hackers and malware. Setting up a global financial network exposes unwitting users to threats from all over the world and opens up a Pandora's box of ethical and legal issues.

This is akin to the Tor dilemma. Tor is much hyped as a platform providing Internet access to citizens living in the shadow of repressive regimes, but it is equally well known as the communication medium of choice for hackers and supports a thriving underground economy and trade in illicit pornography. There is no technological mechanism to disentangle these two usage scenarios. In supporting Tor, we implicitly acknowledge that the positive applications of the network justify the negative. This deadlock leaves us with questions: What now? Is it worth trying to fix Bitcoin? Can it even be fixed?

Several solutions are being developed which try to address some of the currency's problems. Online wallet services (such as Coinbase) aim to protect and simplify management of users' Bitcoin credentials. Hardware wallets (such as Trezor and BTChip) are available which store user credentials in protected hardware which is mostly kept offline. Multi-signature escrow services have been proposed for consumer protection (such as Bitrated.com) which allow for arbitration over disputes. Multisignature wallet services (such as CryptoCorp) propose to use fraud detection algorithms to co-sign user transactions to protect them from scammers and malware. Researchers are working on 'coin-tainting' techniques [41] to identify and track illegal transactions and clustering techniques to identify single ownership of groups of Bitcoin addresses.

However, none of these solutions decisively solve our problems. Some, ironically, even suggest a return to the regulated centralized framework that Bitcoin originally rebelled against. As we have learnt from the experience of WiFi, it would be unrealistic to expect the majority of people today to protect Bitcoin addresses and wallets from sophisticated hackers and malware. Online wallet services and multisignature facilities, much like banks, take away the key elements of anonymity and privacy, as they are privy to all user transactions. Depending on which part of the world these services are based in, governments may even be able to regulate them via legislation. The same applies for companies like CoinBase and Bitpay which act as a conversion portal between Bitcoin users and traders/merchants who accept traditional currencies. These companies could be subject to regulation which might negatively interfere with the customer experience.

Researchers have also questioned the strategy of tainting suspect bitcoins as a crimefighting technique [42]. Blacklisting certain coins will reduce their value, making them harder to spend, and this ultimately stands to have a destabilizing effect on the currency as a whole.

5 Conclusion

We have shown that Bitcoin has become both a useful tool for criminals and a target for crime. Furthermore, the desirability of Bitcoin for criminals derives directly from its anonymity and freedom from central regulation, otherwise desirable properties that the Bitcoin network was designed to provide.

We believe this fundamental paradox at the heart of Bitcoin is the reason why Bitcoin-related crime is rapidly growing and diversifying. As we observe, the trends show a marked increase in the mainstream proliferation of dark markets, a surge in Bitcoin-related malware, and a growing number of attacks on Bitcoin exchanges. Our analysis also provides a useful perspective to reason about future criminal possibilities, such as tax evasion and money laundering. This may also include non-financial applications, such as hijacking the Bitcoin network for illicit communications.

References

1. M. Bustillos. *The Bitcoin Boom.* The New Yorker, April 2013. `http://www.newyorker.com/tech/elements/the-bitcoin-boom`.
2. Kitco News. *2013: Year Of The Bitcoin.* Forbes, Dec. 10 2013. `http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/`.
3. CoinMarketCap. *Crypto-Currency Market Capitalizations.* BitcoinTalk, July 28 2014. `https://coinmarketcap.com/`.
4. Hugh Langley. *Bitcoin value surges as Microsoft starts accepting cryptocurrency.* TechRadar, Dec. 11 2014. `http://www.techradar.com/news/internet/bitcoin-value-surges-as-microsoft-starts-accepting-cryptocurrency-1276552`.
5. Monica J. Barratt. Silk Road: eBay for Drugs. *Addiction*, 2012.
6. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, Berkeley, CA, USA, 2004. USENIX Association.
7. Judith Aldridge and David Décary-Hétu. Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *Social Science Research Network Working Paper Series*, May 2014.
8. Daily Mail. *Mastermind behind $180M 'eBay of drugs' Silk Road convicted after jury deliberates just three hours*, Feb 4 2015.
9. Stuff. *Silk Road Drug Buyers in Court*, Dec. 3 2014. `http://www.stuff.co.nz/auckland/63779228/Silk-Road-drug-buyers-in-court`.
10. FBI. *Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court*, Nov. 6 2014. `http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court`.
11. Joon Ian Wong. *Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust.* CoinDesk, Oct. 6 2014. `http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/`.
12. DeepDotWeb. *Interview With Grams Search Engine Admin: Exciting Features Ahead!*, May 3 2014. `http://www.deepdotweb.com/2014/05/03/interview-with-grams-search-engine-admin-exciting-features-ahead/`.
13. Marc Macyoung and Chris Pfouts. *Safe in the City.* Paladin Press, 1994.

14. Marc Macyoung. *Violence, Blunders and Fractured Jaws: Advanced Awareness Techniques and Street Etiquette*. Paladin Press, 1992.
15. Parmy Olson. *The man behind Silk Road - the internet's biggest market for illegal drugs*. The Guardian, Nov. 10 2013. http://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht.
16. Andre Infante. *Coin Report: How Many Lives Did Silk Road Save*. CoinReport, June 26 2014. https://coinreport.net/many-lives-silk-road-save/.
17. Christian Decker and Roger Wattenhofer. Bitcoin Transaction Malleability and MtGox. In *19th European Symposium on Research in Computer Security (ESORICS)*, September 2014.
18. Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In *Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.
19. Stan Higgins. *Bitstamp Claims $5 Million Lost in Hot Wallet Hack*. CoinDesk, Jan. 5 2015. http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/.
20. Andy Greenberg. *Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say*. Forbes, Feb. 26 2014. http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/.
21. Alex Hern. *A History of Bitcoin Hacks*. The Guardian, March 18 2014. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency.
22. A. Young and M. Yung. *Malicious Cryptography: Exposing Cryptovirology*. John Wiley & Sons, 2004.
23. Violet Blue. *CryptoLocker's crimewave: A trail of millions in laundered Bitcoin*. ZDnet, Dec. 22 2013. http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/.
24. Dan Goodin. *We "will be paying no ransom," vows town hit by Cryptowall ransom malware*. Ars Technica, June 7 2014. http://arstechnica.com/security/2014/06/we-will-be-paying-no-ransom-vows-town-hit-by-cryptowall-ransom-malware/.
25. Jim Walter. *Meet 'Tox': Ransomware for the Rest of Us*. McAfee Labs - Blog Central, May 23 2015. https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us.
26. Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Chris Grier, Damon McCoy, Stefan Savage, Nicholas Weaver, Alex C Snoeren, and Kirill Levchenko. Botcoin: Monetizing Stolen Cycles. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2014.
27. Liam Tung. *NAS device botnet mined $600,000 in Dogecoin over two months*. ZDnet, June 18 2014. http://www.zdnet.com/article/nas-device-botnet-mined-600000-in-dogecoin-over-two-months/.
28. Kyle Torpey. *Bitcoin and Tax Evasion: Are the Possibilities Overstated?* Inside Bitcoins, Oct. 28 2014. http://insidebitcoins.com/news/bitcoin-and-tax-evasion-are-the-possibilities-overstated/25805.
29. James Surowiecki. *The Underground Recovery*. The New Yorker, April 29 2013. http://www.newyorker.com/magazine/2013/04/29/the-underground-recovery.
30. Jeff Wald. *How An Exploding Freelance Economy Will Drive Change In 2014*. Forbes, Nov. 25 2013. http://www.forbes.com/sites/groupthink/2013/11/25/how-an-exploding-freelance-economy-will-drive-change-in-2014/.

31. Kevin Palmer. *FACTA: New Federal Law Causes Swiss Banks to Reject American Investors*. Watchdog Wire, Oct. 23 2012. http://watchdogwire.com/blog/2012/10/23/facta-new-federal-law-causes-swiss-banks-to-reject-american-investors/.
32. Robert Stokes. Virtual Money Laundering: The case of Bitcoin and the Linden dollar. *Information & Communications Technology Law*, 2012.
33. Malte Moser, Rainer Bohme, and Dominic Breuker. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. In *eCrime Researchers Summit (eCRS), 2013*. IEEE, 2013.
34. Jeffrey Sparshott. *Web Money Gets Laundering Rule*. Wall Street Journal, March 21 2013. http://www.wsj.com/articles/SB10001424127887324373204578374611351125202.
35. Jane McCallion. *Europol calls for Greater Bitcoin Policing Powers*. ITPro, March 25 2014. http://www.itpro.co.uk/public-sector/21903/europol-calls-for-greater-bitcoin-policing-powers.
36. Jeremy Kirk. *Could the Bitcoin Network be Used as an Ultrasecure Notary Service?* PCWorld, May 24 2013. http://www.pcworld.com/article/2039705/could-the-bitcoin-network-be-used-as-an-ultrasecure-notary-service.html.
37. Danny Bradbury. *BlockSign Utilises Block Chain to Verify Signed Contracts*. CoinDesk, Aug. 27 2014. http://www.coindesk.com/blocksign-utilises-block-chain-verify-signed-contracts/.
38. *Counterparty: Pioneering Peer-to-Peer Finance*. Accessed 22-July-2014.
39. Thomas Fox-Brewster. *Bitcoin's Blockchain Offers Safe Haven For Malware And Child Abuse, Warns Interpol*. Forbes, March. 27 2015. http://www.forbes.com/sites/thomasbrewster/2015/03/27/bitcoin-blockchain-pollution-a-criminal-opportunity/.
40. Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao. ZombieCoin: Powering Next-Generation Botnets with Bitcoin. In *2nd Workshop on Bitcoin Research*, 2015.
41. Arthur Gervais, Ghassan O Karame, Vedran Capkun, and Srdjan Capkun. Is Bitcoin a Decentralized Currency? *IEEE Security & Privacy*, 12(3):54–60, 2014.
42. Malte Möser, Rainer Böhme, and Dominic Breuker. Towards risk scoring of bitcoin transactions. In *1st Workshop on Bitcoin Research*, 2014.