Crime Law Soc Change (2018) 69:283–305
https://doi.org/10.1007/s10611-017-9756-5

# Bitcoin, crypto-coins, and global anti-money laundering governance

**Malcolm Campbell-Verduyn** [1]

Published online: 19 January 2018


**Abstract** Crypto-coins (CCs) like Bitcoin are digitally encrypted tokens traded in peer-to-peer networks whose money laundering potential has attracted the attention of regulators, firms and the wider public worldwide. This article assesses the effectiveness of the global anti-money laundering regime in balancing both the challenges and opportunities presented by these novel 'altcoins'. Two main arguments are advanced. First, the implications that crypto-coins presently pose for global anti-money laundering efforts stem less from the threats of their illicit uses as digital *currencies* and more from the opportunities presented by their underlying blockchain *technologies*. Second, despite several shortcomings, the risk-based approach pursued by the Financial Action Task Force (FATF) strikes an effective balance between the existing threats and opportunities that crypto-coins currently present. Rather than a conclusive evaluation however this article stresses the need for continual monitoring and investigation of the wider ethical implications raised by CCs for global efforts to combat money laundering in an era of rapid technological change.

## Introduction

What implications do 'crypto-coins' like Bitcoin pose for global anti-money laundering efforts? How effective is the global anti-money laundering regime in balancing the challenges and opportunities presented by the emergence of these novel digital tokens?

Earlier drafts of this paper were greatly improved by the careful criticisms and helpful suggestions of Eric Helleiner, Marcel Goguen, Mark Nance, participants in the FATF @ 25 workshop at the Federal Reserve Bank of Atlanta, researchers in the University of Toronto's Internet Research Network, and two anonymous journal referees. The usual disclaimers apply.

✉ Malcolm Campbell-Verduyn
mcverduyn@balsillieschool.ca

[1] Balsillie School of International Affairs, 67 Erb Street West, Office: Room 336, Waterloo, ON N2L 6C2, Canada

Discussions of what Bitcoin and its competitors *are* and what they *do* tend to be characterised by fundamental misunderstandings and highly divergent viewpoints. This article advances a nuanced two-fold argument that navigates between highly polarised extremes. First, the implications crypto-coins presently pose for global anti-money laundering stem less from the threats of their illicit uses as virtual *currencies* and more from the opportunities presented by their underlying blockchain *technologies*. Second, despite several shortcomings, the risk-based approach formulated by the leading global-level organisation involved in coordinating anti-money laundering efforts, the Financial Action Task Force (FATF), provides an effective balance between the existing threats and opportunities that crypto-coins currently present. The FATF's fostering of looser, decentralised governance networks is regarded as innovative and ultimately more effective than traditional centralised forms of coercion in an era of rapid and unpredictable technological change.

These arguments are elaborated over four sections. A first section outlines the challenges that crypto-coins presently pose for the global anti-money laundering regime by understanding these 'altcoins' as novel technologies rather than as currencies. The limits of industry and government efforts to address these potential challenges are then laid out in a second section that illustrates the gaps in global governance that the FATF has sought to address. A third section assesses the global coordination provided by the FATF in balancing both the potential risks as well as the benefits presented by this set novel set of technologies for anti-money laundering efforts. Rather than a conclusive evaluation the final section stresses the need for continual monitoring and investigation of the wider ethical implications raised by CCs for global efforts to combat money laundering.

## The challenges of crypto-coins to global anti-money laundering governance

Crypto-coins (CCs) are digitally encrypted sequences of numbers. Their central novelty lies in enabling digital transactions to be undertaken both securely and with varying levels of anonymity. These transactions are verified through decentralized peer-to-peer networks and then broadcast on public ledgers that encode the transaction histories of each individual CC. Bitcoin is by far the leading 'altcoin', having benefited from first-mover advantages with its establishment in 2009. The technical design for Bitcoin appeared in a 2008 white paper published by an unidentified person or group of persons under the alias Satoshi Nakamoto [1].[1] The open source nature of this design has given rise to hundreds of competing CCs as well as more recent experimentation with applications beyond CCs. Scholarly, regulatory and popular debates tend to focus on whether or not CCs serve as forms of money in the so-called "Internet of Money" [2], see also, [3–5]. This section argues that these 'altcoins' are less conventional forms of *money* than novel *technologies*. The challenges that these decentralised and quasi-anonymous technologies potentially pose to the global anti-money laundering regime are then considered.

[1] CCs are often referred to as Bitcoins in a generic manner similar to tissues being called Kleenex.

## The novelty of CCs

Debates on money laundering tend to assume economistic understandings of money as defined by three key properties: a medium of exchange, store of value, and unit of account. CCs are not widely utilised as media of exchange. The limited acceptability of CC beyond some tech-savvy communities and markets[2] stems from many factors, not least perceived difficulties with their 'usability', as well as the wider 'digital gaps' that render 'altcoins' beyond the reach of those less familiar or less able to transact with novel digital technologies. Less than 6 % of Americans, for instance, considered themselves to be "very familiar" with CCs in a 2015 survey by *PwC* ([6] p. 7). Another 2015 survey by this consulting firm found that less than 10 % of leading money managers had any familiarity at all with CCs [7].

Understanding CCs as conventional forms of money is rendered equally difficult by their unstable values. CCs are often praised as 'digital gold' due to their inherent yet finite quantity. For instance, a total of some 21 million bitcoins can be produced, of which 14 million already exist.[3] This limited supply renders the leading CC highly sensitive to changes in demand.[4] Easily bid up and down by speculators the unstable price of Bitcoin and other CCs render their values extremely volatile. The dollar price of Bitcoin has garnered widespread attention as it briefly surpassed $1000 in 2013 only to fall back down to the low hundreds where it remained until once again rising past $1000 following the inauguration of Donald Trump as American president [8]. Critics have stressed this volatility in arguing that a token "prone to collapsing or quadrupling in price is useless as a practical currency" [9]. Difficulties in safely storing CCs in digital wallets, banks, and exchanges that have been continually targeted by hackers further undermining the store of value function of CCs. Such hacks have ranged in size, from the 896 bitcoin theft from Alberta-based Flexcoin to the record loss of 850,000 bitcoin from Tokyo-based Mt. Gox in 2014 (11, 12, 13).[5]

Finally, CCs infrequently serve as standard units of account. The ability of CCs to keep "track of promises of future benefits in exchange for past transfers of resources" ([11], p. 25) has been recognised by economists, central bankers and financial regulators alike as *theoretically* serving the function of virtual unit of account [12, 13].[6] In actual *practice*, however, CC users largely continue accounting for the value of altcoins in relation to official state-backed currencies, primarily the American dollar [14]. The instability of exchange values and limited acceptability of CCs further undermines their uses as units of account. As the European Central Bank puts it, given "the low level of acceptance and the high volatility of their exchange rates and thus purchasing power make them unsuitable as a unit of account […] Bitcoin cannot be regarded as full forms of money at the moment" [15].

[2] The estimated annual transaction volume in Bitcoin alone grew from $2 million to over $100 million between 2012 and 2015 [6]. For an interactive map of businesses accepting Bitcoin see https://coinmap.org

[3] Units of CCs are conventionally put in lowercase. Estimates vary regarding when precisely production of Bitcoin will peak, with some indicating the year 2040 and others a century later.

[4] Bitcoin competitors such as Blackcoin and Peercoin boast less restrictive aggregate limits through technical mechanisms that control increases in supply for instance to one percent annually.

[5] Section three below elaborates on the story of Mt. Gox.

[6] As economists William Luther and Josiah Olson succinctly put it, "Bitcoin is Memory" [17]. Computer scientists have noted the possibility however that CCs with "a famous transaction history" might be more valuable than more mundane CCs, thwarting their ability to serve as standardized unit of account [18].

Why should global anti-*money* laundering efforts be concerned with CCs if "in practice few people actually use, or perceive, Bitcoin as money in a traditional sense" ([16], p. 3)?.Recent calls to expand studies of money ([17], p. 19) and heterodox understandings of money [18, 19] point to at least two reasons why CCs remain relevant to global anti-money laundering efforts. First, global anti-money laundering governance is concerned with illicit transactions and financial flows *whether or not they meet theoretical standards of money*. These global efforts seek to combat the 'mainstreaming' of proceeds from illicit activities into the legitimate financial system by preventing the linking of financial "upperworlds" and "underworlds" [20]. A second reason why CCs remain relevant to global anti-money laundering governance is due to the novel manners in which altcoins enable the nearly real-time undertaking, verification and publication of transactions across political boundaries. As the following subsections explore in turn, the decentralised and quasi-anonymous features of CCs potentially threaten longstanding global anti-money laundering efforts.

### Decentralised financial flows

Money laundering across national borders traditionally implicated large, multinational banks specialised in cross-border financial transactions. As such, global-level anti-money laundering (AML) efforts have traditionally "deputized" [21] multinational banks as centralised "choke points" [22] to report transactions suspected of laundering illicit funds. CC transactions, however, are undertaken between decentralised networks of users spread worldwide. Rather than centralised institutions like banks, CCs rely on these decentralised networks of users to verify the validity of transactions and avoid the problem of double spending.[7] In shifting from reliance on centralised financial institutions, CCs "neatly sidestep the plethora of anti-money laundering regulations developed over the past 25 years" ([23], p. 3). Without centralised institutions 'in charge' of CCs, no one set of institutions may be relied upon to impose AML requirements. There exist several 'nodes' in the CC ecosystem that can be targeted in global AML efforts. Before elaborating upon these, however, a second related threat to global AML governance is considered.

### Quasi-anonymous financial flows

Applications of digital technologies have long sought to navigate between transparency and anonymity ([24], p. 57–59). Attempts to balance these play out in novel manners with CCs. In theory, CC user addresses cannot be linked to real-world individual identities due to the complex mathematical scrambling employed in the public-key cryptography underlying CCs. Nevertheless, records of individual transactions are broadcast on so-called 'distributed public ledgers'. With Bitcoin, for example, the record of all transactions undertaken approximately every ten minutes is bundled together in 'blocks'. Linked together, these blocks form blockchains, as 'distributed public ledgers' are more commonly known. Contrary to sensationalistic media reports, CCs like Bitcoin are best characterised as *quasi-anonymous* technologies. Their novel attempts to balance of user anonymity and

[7] The problem of insuring that money that is transferred over long distances and borders is not simultaneously retained so that the same unit cannot be used by an individual to purchase goods more than once.

transactional transparency are paradoxically both attractions, as well as sources of risk for governments, firms and individuals in an age of "surveillance capitalism" [25].

The quasi-anonymity of CCs challenges traditional global AML efforts centred on the identification of individuals involved in money laundering. Such efforts are complicated by at least two factors. First, quasi-anonymity frustrates the requirement at the heart of global AML governance for financial firms such as banks to 'Know Your Customer' (KYC). Financial professionals tasked with recognising "evasive or defensive answers to questions" are confronted with the difficult task of identifying whom to direct their queries to ([23], p. 6). CCs reverse the traditional problem confronting AML efforts, from "parties known-transactions unknown" to "transactions known-parties unknown" [26]. In other words, the "very difficult challenge" posed by CCs, as Deloitte principal Fred Curry puts it, is that professionals "can't monitor transactions if [they] don't know who the parties are" (cited in [27]). The second and related problem potentially posed by the quasi-anonymity of CCs for AML efforts is obfuscating what constitutes the 'normal' rather than 'atypical' use of these 'altcoins'. This is the issue, as the legal scholar Robert Stokes has put it, of knowing exactly "what a suspicious BTC [Bitcoin] transfer would 'look' like" ([23], p. 5). How can financial professionals identify suspicious uses of CCs when a baseline for their typical use is neither widely known nor understood?

Together, the quasi-anonymity and decentralised nature of CCs pose important theoretical challenges to AML efforts. Table 1 below provides a more in-depth overview of the risks of money laundering posed by CCs at the three traditional 'stages' of money laundering. As these risks are more thoroughly detailed elsewhere, the following section proceeds to scrutinise varying individual and collective efforts undertaken to confront these possible challenges.

## Dispersed global AML efforts and governance gaps

In originally accepting only Bitcoin for exchange of illicit goods and services, the infamous online marketplace the Silk Road contributed to greater public awareness of

**Table 1** Money laundering risks posed by CCs

| | Potential exploitation of vulnerabilities at each stage | | |
|---|---|---|---|
| General risk factors | Placement | Layering | Integration |
| Quasi-anonymity | CCs can be used by criminals and associations | Suspicious names, particularly if money mules involved that cannot be flagged | Allowing cashing out of proceeds of crime to be passed on anonymously to individuals that cannot be traced |
| Real-time transactions | Proceeds of crime can be transferred to another CC in another country | Transactions occur in real-time, allowing little time to stop them if suspected of money laundering | Proceeds of crime can be moved rapidly through global financial system and withdrawn in another country |

Adapted from [28]

the potential for CCs to be implicated CCs in money laundering.[8] More widely, studies of Internet search engine data have correlated interest in the leading CCs with illegal activities such as money laundering [29]. While CCs theoretically enable "money launderers to move illicit funds faster, cheaper, and more discretely than ever before" ([30], p. 447], little evidence supports claims that such illicit activities are in fact being undertaken with CCs. Altcoin promoters have long asserted that the association of CCs with money laundering is "inflated" (Eddy Travia cited in [31]). Official studies have supported such claims. For instance, the 2015 British National Risk Assessment established that since "[t]here are a limited number of case studies upon which any solid conclusions could be drawn that digital currencies are used for money laundering… [t]he money laundering risk associated with digital currencies is low" [32].[9] As legal scholars have suggested, CC "laundering opportunities may well be more *perceived than real*" ([23], p. 5 emphasis added; see also [33], p. 332).

Nevertheless, the challenges that CCs *theoretically* pose to global AML efforts have been routinely touted as actual threats by financial regulators and law enforcement. The Bank of International Settlements (BIS) ([34] emphasis added) has warned that, due to their "pseudonymity" and global reach, CCs "are *potentially* vulnerable to illicit use". Similarly, the International Monetary Fund (IMF) has stressed how CCs "can be used to conceal or disguise the illicit origin or sanctioned destination of funds, thus facilitating the money laundering [sic]" [35], p. 27). For the SWIFT Institute, the advisory body to the Society for Worldwide Interbank Financial Telecommunication, CCs are a particular "target of those engaged in drug trafficking and money laundering" ([36], p. 7). Meanwhile, following warnings from the Federal Bureau of Investigation and its raid of the Silk Road [37], the American House Committee on Appropriations argued in 2014 that "Bitcoins and other forms of peer-to-peer digital currency are a potential means for criminal, terrorist, or other illegal organizations and individuals to illegally launder and transfer money" [38]. The purportedly growing use of Bitcoin and other CCs in the exchange of illicit goods and services in online marketplaces,[10] have induced further warnings from intergovernmental police organisations that CCs "are being used as an instrument to facilitate crime, particularly in regard to the laundering of illicit profits" [40].

The yet to be proven implication of CCs in money laundering has nevertheless led institution from the financial 'upperworld' to refrain from interacting with much of the 'altcoin' ecosystem. Leading insurers have shied away from underwriting insurance on CCs despite the clear need for such coverage stemming from continual breaches of both altcoin 'banks' and exchanges. In 2014 the British bank HSBC abandoned its CC hedge fund in order to avoid potential implication in further money laundering scandals [41]. The BIS has noted how banks have "tended not to engage directly with digital

[8] The original Silk Road was shut down by the US Federal Bureau of Investigation (FBI) in 2013. The alleged creator of the website, the American Ross Ulbricht, was sentenced to life in prison without parole for money laundering amongst other charges. Silk Road 2.0 was then closed down in 2014 following an international operation by police agencies from 17 different countries. Silk Road 3.0 once again opened in mid-2016 revealing the longer-term limit to international police crackdowns [32].

[9] Similarly, the worry that CCs may be used for terrorist financing remains more potential than proven [37, 38, 39, 40]. Contrary to initial reports, the perpetrators of the November 2015 Paris terrorist attacks did not rely on CCs [41, 42].

[10] *Europol* ([49], p. 46) notes, but offers no supporting evidence of the claim that Bitcoin features "heavily in many EU law enforcement investigations, accounting over 40% of all identified criminal-to-criminal payments".

currency intermediaries" and "sought to avoid interaction as a result of perceptions of risk and uncertainty over legal or compliance issues (such as AML/CFT)" ([34], p. 7). Large, multinational banks have sought to avoid further costs involved with AML compliance [42]. The managing director of American bank Morgan Stanley argued in a 2016 that until the "key question of who will be in charge" is settled, banks would not take CCs "seriously, principally because of anti-money laundering and 'know your customer' (KYC) rules" [43].

In seeking to mitigate potential money laundering risks, as well as to pre-empt national initiatives,[11] firms and industry associations in the CC ecosystem have elaborated their own voluntary AML standards. This section illustrates how the limits of both industry and national initiatives have led to a global governance gap that organisations such as the FATF are positioned to address.

## The limits of industry self-regulation

Firms in the 'altcoin' ecosystem have developed varying AML-compliant CC services. BitInstant, a now defunct leading New York City-based issuer of CC debit cards, promoted voluntary registration and compliance with AML laws. Exchanges of CCs into state-backed moneys, such as Hong Kong-based BitFinex, require customers to undertake more "comprehensive and thorough KYC and AML compliance implementation" that involves the provision of certified identification documents and valid proof of address [45]. BTC China [46], Hong Kong-based Gatecoin [47], as well as the British exchanges Bitstamp [48] and its rival CEX.IO [49] all enforce minimum AML standards by requiring customers to provide copies of their passports in verifying their identities. These firm-level AML efforts however vary considerably, with CC exchanges like HitBTC requiring identification only for account holders that they deem to be "suspicious" [50].

Variance between the AML efforts of individual firms has led to efforts to develop a set of common guidelines. In attempting to develop "common risk management and compliance standards" ([51], p. 834), Delaware-based body called the Digital Asset Transfer Authority (DATA) released a draft set of "global AML guidelines" for comment in 2015. Emphasising the need to balance AML efforts with "fundamental rights and values, including civil liberties, financial privacy and inclusion, transparency and accountability" its draft guidelines urged CC firms to each implement "a basic AML Compliance Program *whether or not required by law*" ([62 p. 2, emphasis in original). AML compliance was specified by the DATA as involving written internal procedures and annual employee training on risk-based due diligence assessments that are overseen by independent Chief Compliance Officers. These draft guidelines suggested that firms collect customer names and addresses as well as "consider implementing more in- depth customer identification and verification procedures – especially for customers and products identified in the risk assessment as high risk" ([62], p. 4). Such "in-depth" procedures include "everything from simply 'googling' the person or company involved or checking the appropriate government agency for corporate registration, to requesting banking and other references, to obtaining credit or business reports, and even obtaining a criminal background check" ([52], p. 5). Finally,

[11] The hackers, technologists, and "wildcat bankers" [54] forming the CC community are renown for wariness of centralised authority. They tend to promote a world of small government and diminished state sovereignty.

the DATA guidelines urge firms to monitor the potential for money laundering to occur through the "entire cycle of a relationship".

Emerging industry efforts to develop AML standards have led to optimistic predictions that all major 'altcoin' operators would comply with some kind of AML regulations over time (e.g. [53]). However, re-occurring scandals and the warnings of police and financial bodies cited above have "drawn serious attention" ([54], p. 157) by national regulators and instigated a perceived need to impose more consistent AML standards throughout the CC ecosystem [35].

## National AML efforts: racing to the top and bottom

National regulators have sought to apply existing as well as new AML measures in the CC ecosystem. How existing laws and regulations of the country that has been most aggressive in prosecuting money laundering [55] and at the centre of global AML efforts [56][12]- the US- apply to CCs has been extensively analysed by legal scholars [e.g. 58–65] as well as drawn upon in several legal cases. For instance, the American Department of Justice (DoJ) invoked the Money Laundering Control Act of 1986 in prosecuting Bitinstant CEO Charlie Shrem, who pled guilty to aiding and abetting unlicensed money transmission in 2014. Shrem contended that his two-year jail sentence "terrified" potential money launderers from employing CCs [66]. In 2015, the US Financial Crimes Enforcement Network (FinCEN) of the US Treasury Department invoked the 1970 Bank Secrecy Act in its first ever-civil enforcement action against a CC exchange. San Francisco-based Ripple Labs was fined $700,000 for failing to implement effective AML programmes in the two years following the guidance FinCEN issued in 2013 [67]. A similar logic underpinned the DoJ case against the individuals operating the CC exchange Coin.mx who allegedly used a credit union to launder proceeds from ransom attacks against large institutions from the financial 'upperworld', such as JP Morgan Chase, as well as the media firm Dow Jones [68–71].

Beyond the US, various formal efforts have been undertaken to mitigate the use of CCs. 'Altcoins' are banned in several countries, including Bangladesh, Bolivia and Ecuador, while their legal status has remained questionable in others, such as Russia and Thailand [72]. In 2013 and 2014 the People's Bank of China and State Bank of Vietnam, respectively, issued laws banning financial services firms and their employees from handling and conducting any transactions in CCs. The Central Bank of Iceland argued in a 2014 decision that the purchase of CCs is in violation of the country's Foreign Exchange Act. The central bank of Indonesia also declared that "Bitcoin and other virtual currency are not currency or legal payment" [73]. While the European Central Bank has more generally warned that regional authorities "take care not to appear to promote the use of privately established digital currencies" ([74], [p. 2]), the European Banking Authority has recommended that regional authorities "discourage" credit institutions from

[12] Although a longstanding practice, money laundering only formally became criminalised in the 1980s American 'war on drugs'. With the more recent American-led 'war on terror', money laundering is also frequently conflated with terrorist financing [25]. Yet since these activities pose alternative problems for law enforcement and their entanglement hinders the fuller understanding of either form of financial crime [26] this analysis largely concentrates on the implications of CCs present to global-level efforts to combat the former.

dealing in CCs [75].[13] European countries such as The Netherlands have brought forward multiple legal cases against individuals suspected of money laundering through CCs [76].

Although supported by some analysts [77], these bans and other such top-down coercive efforts by states and quasi-state actors to mitigate money laundering through CCs have faced criticism. Legal scholar Kavid Singh [65] has for example pointed out that "heavy-handed" approaches fail to prevent the use of CCs for money laundering and other "clandestine transactions" as well as "eradicate" more legitimate uses of 'alt-coins', such as facilitating migrant remittances and payments to whistleblowers (e.g. [76] p. 15–18; for an overview see [16]). Yet 'heavy-handed' is a categorisation invoked quite loosely in otherwise meticulous legal scholarship. Singh implicitly refers to tactics that might undermine the benefits of CCs, such as requirements for the key centralised "focal points" in the CC ecosystem, such as exchanges, to transact with other operators and CC users that have met AML requirements [78, 79]. As identified in Table 1 above, the central problem with targeting exchanges and other "easily identifiable institutions with readily detectable headquarters" ([65], p. 58) is that such CC operators can simply re-locate in jurisdictions where such requirements are lax or that may be "non-cooperative" in enforcing AML efforts ([80], p. 4). For example, New York City witnessed an "exodus" [81] of its previously thriving CC industry after the state Department of Financial Services sought to impose a "very innovation unfriendly" Bitlicense registrations on CC operators in 2015 [82]. In order to obtain this license firms must undertake "initial and annual risk assessments, ten-year records of all transactions, suspicious activity reports, a customer identification program, checks and compliance, annual internal or external audits, and no structuring to evade reporting, or obfuscating identity" ([63], p. 601). Just as water flows towards lower points of gravity [83], CC operators may be induced by such high standards to undertake regulatory arbitrage in shifting their activities towards less 'strict' jurisdictions and murkier areas of the 'shadow financial system' where AML regulations are much 'looser' and the reach of AML efforts remain 'weaker' [84].[14] As the BIS has stressed, "the decentralised nature of these digital currency schemes means that it is difficult to impose such restrictions on transactions" ([34], p. 10).

Yet 'races to the bottom' are also often accompanied by 'races to the top'. New York State and other jurisdictions have attempted to distinguish themselves as legitimate centres for CC activity. Singapore has since 2014 required virtual currency exchanges based in the city-state to verify customer identities and report suspicious transactions to its Suspicious Transaction Reporting Office [28, 85]. The English Channel island of Alderney has set up a cluster of AML-compliant CC services in its attempt to become the leading international CC transaction centre [86]. Competing for the title of "Bitcoin Isle" is the neighbouring Isle of Man, which amended its main AML legislation to include CCs and is developing similar "pioneering regulation and funding schemes"

[13] The money laundering potential of CCs attracted further formal attention in the European Union following the November 2015 Paris terrorist attacks as the European Commission ([85], p. 39) proposed to amend the Fourth Anti-Money Laundering Directive to bring CC exchanges under existing AML laws and create "a central database registering [CC] users' identities".

[14] Though it should be noted that some two dozen firms, including the prominent exchange Coinbase, have remained in the state and applied for such a license.

[87]. Such efforts to create legitimate AML-compliant jurisdictions, however, do little to limit the potential for money laundering activities to thrive other jurisdictions.

National authorities have also sought to impose their AML requirements on CC operations beyond their jurisdictions. In May 2013 the US Department of Homeland Security issued a seizure warrant to the American-based firm undertaking transfers for the once dominant Tokyo-based CC exchange Mt. Gox, which complied and received a money business service license only months before filing for bankruptcy protection following a devastating hack [61]. Beyond this prominent case and scholarly suggestions to rely on American hegemony [64], however, extraterritorial applications of US laws only go so far in providing *legitimate global* rather than unilateral AML standards for CCs. The unappealing choice for national regulators to either blatantly submit to the jurisdiction of American law or to impose bans to mitigate the use of CCs has instigated global level efforts.

### A gap in global AML governance

The limits of both industry- and national-level governance have instigated calls for coordinated global efforts to mitigate the potential uses of CCs for money laundering without curtailing their more beneficial features. The BIS argues that "[g]iven the nature of digital currencies, which are typically online and therefore not limited to national jurisdictions, a coordinated approach at a global level may be important for regulation to be fully effective" ([88], p. 12). Technologists Isaac Pflaum and Emmeline Hateley ([64], p. 1196) have also argued that "it is not possible to regulate virtual currency effectively at the international level without significant assistance between states that permit its usage". Such global collective action problems are certainly not new, having afflicted the governance of a range of emergent technologies in the past [89].

Several international organisations have been vying to provide standards coordinating national AML laws and regulations relevant to CCs. The United Nations Office on Drugs and Crime (UNODC) issued a detailed manual in 2014 for detecting and seizing CCs implicated in money laundering and, along with the Organization for Security and Cooperation in Europe (OSCE), has been training officials to investigate money laundering through CCs [90]. In 2015 the International Organisation of Securities Commissioners (IOSCO) established a "blockchain taskforce" [91] while the Commonwealth convened a ten member Working Group on Virtual Currencies in parallel efforts to coordinate AML approaches. Similarly, Interpol and Europol have established a joint partnership coordinating police activities "against the abuse of virtual currencies for criminal transactions and money laundering" [92]. The following section scrutinises efforts by the intergovernmental organisation specifically designed to coordinate AML efforts.

## FATF to the rescue?

The Paris-based Financial Action Task Force (FATF) is an intergovernmental organisation officially comprised of thirty-five member-states and two regional organisations. Including its associate and observer members, as well as members of FATF-style regional bodies, some 170 countries are linked to the FATF, which is widely recognised

to form the heart of the global AML regime [56].[15] The 40 recommendations developed following its 1989 founding, along with the further 9 recommendations promulgated in the aftermath of the 11 September 2001 attacks, are widely regarded as the key global standards advancing a common AML approach [28]. Since their 2003 revision, these voluntary, non-binding recommendations have emphasised a 'risk-based approach' prioritising preventative measures "commensurate with the risks identified" ([93], p. 11). In contrast to a more uniform 'rules-based approach', the 'risk-based approach' provides national regulators with considerable discretion in implementing measures to achieve the common goal of reducing money laundering [94]. This more flexible and decentralised approach, combined with forums for mutual learning and evaluation is indicative of "networked" [95] and "experimentalist" [96] forms of governance that have been more widely identified in contemporary global governance.

The FATF recommendations and their 'risk-based approach' have been applied to CCs. Attention to the altcoin ecosystem by the task force began rather belatedly, a half-decade following the establishment of Bitcoin. A 2013 report assessed Internet-based payment systems in general terms [97]. A detailed and quite nuanced report published the following year then acknowledged both the legitimate potential of CCs ([98], pp. 8–9) as well as how the complex and segmented technical infrastructures underpinning CCs involve entities spread across "jurisdictions that do not have adequate AML/CFT controls". A 2014 report also stressed how the existence of the CC ecosystem "in a digital universe entirely outside the reach of any particular country" entailed that "responsibility for AML/CFT compliance and supervision/enforcement may be unclear" ([98], p. 8–9). Identifying this lack of governance clarity served as justification for FATF involvement in the CC ecosystem. Guidance consistent with its purposely broad 40 + 9 recommendations was then released in 2015 with the dual purpose of helping market actors identify and act on the money laundering threats posed by CCs, as well as of aiding national authorities to develop standard legal and regulatory frameworks to support global AML efforts [99].[16]

In attempting to mitigate the money laundering potential of CCs, the FATF guidance relies on the longstanding twin pillars of global AML efforts identified by scholars ([101], p. 181). First, the FATF suggests national authorities set up "coordination mechanisms" to proactively share information in manners that promote deeper understanding of the risks of money laundering in the CC ecosystem ([99], p. 8). Second, the risk-based approach suggests that national authorities target the specific 'nodes' most likely to be at the forefront of money laundering and whose "activities intersect with the regulated fiat currency financial system" ([99], p. 6). Rather than individual users or producers of CCs, the FATF suggests for countries to regulate the institutions at highest risk of involvement in money laundering because they "send, receive, and store" CCs. The 2015 FATF guidance specifies that *exchanges* be targeted for enhanced monitoring. Yet the FATF calls on exchanges *themselves* to "undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information" ([99], p. 12). The forty-fourth clause suggests that CC exchanges identity users

[15] For a list of full members, associate members, and observers of the FATF see http://www.fatf-gafi.org/about/membersandobservers/

[16] The FATF issued a second report in 2015 more specifically detailing the potential for CCs to be implicated in terrorist financing [108]. The case of an American teenager who had pled guilty to promoting- but not undertaking- efforts to fund the Islamic State through CCs was highlighted.

using national identity numbers or Internet Protocol addresses, as well as conduct online searches "for corroborating activity information consistent with the customer's transaction profile" ([99], p. 13).

What measures does the FATF then suggest regulatory authorities undertake in responding to exchanges or other actors in breach of AML requirements? Its 2015 guidance calls for such exchanges to be met with "enhanced due diligence measures" ([99], p. 8). These measures include straightforward prohibition ([99], p. 9) as well as "a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative)" ([99], p. 10). What on first glance appears to form a rather 'harsh' governance approach is nuanced by subsequent suggestions that coercive measures "should take into account, among other things, the impact a prohibition would have on the local and global level of ML/TF [money laundering/terrorist finance] risks, including whether prohibiting VC [virtual currency] payments activities could drive them underground, where they will continue to operate without AML/CFT controls or oversight" ([99], p. 9). In other words, the FATF urges national authorities to recognise how complete bans on CC might further exasperate regulatory arbitrage and "cross-border" divergences in the governance of exchanges operating as key nodes between the financial "upperworlds" and "underworlds" [18].

## Evaluating the FATF guidance

The effectiveness of the FATF and its non-obligatory recommendations has long been subject of scholarly debate [83], e.g. [102–104]. Several commentators have criticised the weak and largely symbolic role of the FATF in appearing to be 'doing something' about money laundering without restricting "the freedom of capital movements, in any way" [99], p. 104; e.g. [105–107]. Other scholars have stressed the success of this intergovernmental organisation in motivating a range of state and non-state actors worldwide to prioritise AML efforts without resorting to coercive formal laws ([56], p. 86; [56], p. 47). Existing analyses therefore range from a narrower emphasis on the success of efforts to *standardise* varying AML efforts to more general success in *preventing* money laundering.[17]

The proceeding evaluation stresses a different understanding of effectiveness: the balance achieved between mitigating the *potential challenges* without curtailing the *actual opportunities* presented for AML efforts. This understanding of effectiveness is invoked for two reasons. First, as the 2015 FATF guidance on CCs is only rather slowly being transposed into national and regional regulations, the narrower emphasis on the success of efforts to *standardise* varying AML efforts is difficult to presently assess. Second, with little evidence currently implicating CCs in money laundering it is important to consider whether the potential *benefits* of blockchain technology for global AML efforts are also being promoted by the FATF.

Unsurprisingly, CC supporters have criticised FATF suggestions that existing AML standards be extended to the 'alt-coin' ecosystem. Doing so, industry proponents have maintained, would once again lead CC activities to flow to parts of illicit financial system that remain effectively 'off-limits' to regulators. Industry bodies such as the Digital Finance Institute have argued that the "regulate or shut down" [23] approach advocated by the FATF would not only force parts of the CC ecosystem into the illicit 'underworld' but lead institutions from the financial

[17] Others yet critique the inherent difficulty in measuring effectiveness of AML policies ([116], p. 641).

'upperworld' to avoid engagement with CC operators due to longstanding concerns with the costs of AML compliance (see more generally [105], p. 621, 628–9). In avoiding engagement with CCs, financial institutions seek to 'de-risk' by forfeiting involvement in activities where the costs of complying with AML regulations are regarded as outweighing any potential gains.

Three more specific criticisms can be levied at the FATF's risk-based approach. First, the FATF perpetuates the heavy reliance of global AML governance on market actors ([94, 105, 109, 110], p. 620). The 2015 guidance proposes that countries require financial and non-financial firms to assess money laundering risks themselves when dealing with CCs. Indeed, the very first clause advocates that market actors "refine technical processes used to reliably identify and verify customers" ([99], p. 12). The FATF also calls on industry associations to "develop policies and practices for members that allow them to identify specific transactions as coming from a member that has applied appropriate [customer due diligence] CDD and is conducting appropriate transaction monitoring" ([99], p. 14). This emphasis on market initiatives (e.g. [99], p. 8) overlooks problems involved with relying on industry-sponsored data, as well as for regulators to be materially and intellectually 'capture' by industry interests ([111, 112] p. 152–3). Top-down attempts at fostering industry cooperation have spurned push-back from the decentralised CC community, including denunciations by leading individuals in the Blockchain Alliance, an organisation consisting of 16 CC servicers and seven American regulatory agencies [113]. The FATF has sought to justify its emphasis on market solutions by arguing that the inability to "target one central location or entity for investigative purposes… undermines countries' ability to employ effective, dissuasive sanctions" and "presents a significant challenge to law enforcement's ability to trace illicit proceeds that are laundered" ([99], p. 11). Despite its recognition of such difficulties, the FATF suggests national authorities review these challenges in order "to identify potential gaps and take action" ([99], p. 11) like "licensing and registration" as well as nudging exchanges to adopt "customer identification/verification and recordkeeping requirements". In short, the risk-based approach tends to overlook the risks involved with a reliance on industry solutions.

Second, and relatedly, the FATF guidance tends to rely on magic-bullet "technology-based solutions" ([99], p. 14). The 2015 guidance suggests that, if left alone by regulators, market actors might develop "application programming interfaces (APIs) that provide customer identification information" or third-party digital identity systems that would themselves need to be regulated ([99], p. 14). The FATF suggestion to combat the enhanced money laundering potential created by a new set of technologies with further technical innovations encourages what Europol ([114], p. 69) and others have derided as a technological "arms race" between CC users and regulators. Besides criticism that the technology to undertake such efforts is not yet in existence [27], the development of "identity gatekeepers" or "[s]ome kind of central authority […] to undertake identification processes" is fundamentally at odds with the preference for decentralisation and distrust of centralisation in the CC community.

Third, stress on high-risk exchanges overlooks a wider set of other potentially lower-risk yet nevertheless important hubs in the CC ecosystem. The focus on 'nodes' at the "edges" of the system [108] neglects the money laundering potential in the activities of a host of other actors closer to the core of the 'altcoin' ecosytem. The narrow definition of what precisely constitutes a CC exchange, for instance, overlooks how the producers of

'alt-coins', such as miners,[18] might also serve as key 'nodes' in facilitating money laundering. As legal commentators have pointed out, "although the mining process does not inherently implicate money-laundering concerns, lucrative transaction fees for miners willing to verify fraudulent transactions might incentivize criminal behavior" ([65], p. 55). Not 'going low' and advocating that potentially less risky actors also be targeted, such as wallet companies, limits the scope of the FATF guidance ([115], see also [116]).

Despite such shortcomings, the founders and key backers of the FATF- the Group of 7 leading industrialised countries ([117], p. 9)- have supported the attempts of this intergovernmental organisation to plug the "patchwork of inconsistent and incomplete attempts to counter criminal abuse of the [blockchain] technology" ([64], p. 1215). Compared with the nascent efforts of other international regulators,[19] the risk-based guidance on recommendations that are "non-binding, and carry no penalties for violations" ([64], p. 1196) do provide for flexible variation across jurisdictions as well as the building trust between regulators and a CC ecosystem that is intenselydistrustful of centralised 'interventions'. The following sub-section highlights the further governance options available and assesses the necessity of such alterantives given the current non-monetary status of CCs.

**Other options exist! but are they necessary?**

One alternative not considered in the 2015 FATF guidance is the creation of competing national CCs. Suggestions have been consistently floated by firms and regulators for governments to create 'state-sponsored CCs' [118]. In 2015 the UK Home Office recommended the creation of a government-backed virtual state currency [119]. Australian, British, Canadian, Chinese, Dutch, Russian, Singaporean, South Korean, Swedish and Zimbabwean central bankers have all explored the issuance of national CCs (e.g. [120–124]. While these 'state-sponsored' CCs are being contemplated for varying purposes,[20] the Singapore-based Interpol Global Complex for Innovation has gone furthest in developing an actual 'simulation CC' for training of AML authorities in spotting the "misuse" of real 'altcoins' [125].

The option of creating 'national CCs' is largely unnecessary at the present time. Beyond injecting further competition into an increasingly crowded 'altcoin' marketplace,[21] the creation of AML-compliant state-sponsored CCs may do little to prevent the use of other CCs in money laundering. Expending resources to develop national

[18] Miners are the producers of CCs who are rewarded with new CCs for verifying transactions. Brett Scott provides a useful comparison in likening these actors to a "network of clerks who check to see that participants actually have the funds they claim to have, and who then record a change to the decentralized blockchain ledger" ([21], p. 2). Originally indended to be undertaken by individual personal computers, the computing power required to profitably verify the growing number of transactions on the Bitcoin blockchain now requires specialised computer rigs. The complexity and expense of such operations has led to the formation of teams- also known as alliances, collectives or 'pools'- of miners who now control large shares of Bitcoin mining. The size of these pools can be tracked at <https://blockchain.info/pools>.

[19] For instance, BIS merely acknowledged that "distributed ledgers are an innovation that could have a range of impacts on many areas, especially on payment systems and services" [44].

[20] The ability to trace transaction is a major incentive. More generally however the fear of missing out on potential savings from payments servicing, the facilitation of further shifts away from the use of cash, and related enhanced ability to monitor transactions for both security and tax purposes. The latter is elaborated upon below.

[21] As Thomson Reuters Accelus puts it, "if sovereign governments move toward issuing digital currency, then competition may overwhelm private currency such as Bitcoin" ([133], p.12).

CCs is premature given the absence of evidence that CCs are being used either as traditional forms of money or for money laundering. Despite its limits, the 2015 FATF guidance focus on centralised institutions exchanging CCs into state-backed money as well as on market solutions appears sufficient for the time being. Nevertheless, given the instabilities fostered by a reliance on market-based processes in the not-so-distant 2007-8 global financial crisis as well as the inherent difficulties in measuring money laundering ([105], p. 622), this claim is advanced very cautiously. Before clarifying that this argument in no way calls for regulatory inaction, the remainder of this sub-section examines the specific technological features of CCs that the FATF guidance calls on authorities to consider prior to implementing 'harsh' measures such as bans.

Even longstanding critics of technology-based solutions have recognised the "enormous potential" that the blockchain underlying CCs provide for addressing a range of governance gaps (cited in [126]). Blockchains may specifically contribute to least two aspects of global AML efforts. First, private and semi-private 'permissioned' blockchains allow centralised entities to authorise access to particular CCs [127]. Identabit and Cambridge Blockchain for instance have built-in proof of identity features that go far beyond the voluntary user registration relied upon by even the most AML-friendly CC exchanges [128]. One of the chief competitors to the Bitcoin blockchain, Ripple, has sealed 'gateways' that authenticate identities and grant permission to users of its CC, which is called XRP. Such gateways have led Ripple to be regarded as far more "AML friendly" by the Institute of International Finance, the leading global banking sector association, which has praised the potential of this CC to "enforce various supervisory measures such as know-your-client (KYC) and anti-money laundering (AML) procedures" [129]. Firms from the financial 'upperworld' have also made considerable investments in permissioned blockchains to minimise the money laundering potential of 'alt-coins' [92]. The FATF guidance ([99], p.14) endorses these additional applications of blockchain technologies, explicitly advocating for developments "built on fundamentally different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring".

Second, the FATF guidance avoids mitigating the wider support blockchain technologies provide to the information sharing and identity management underpinning global AML efforts. Blockchains can be utilised to create AML-compliant registries [130] as well as tools to identify the holders of CC wallets in nearly real-time and to create blacklists of users [97, 98]. The Isle of Man has built on the former in its efforts to become the leading AML-compliant jurisdiction while more than a half dozen large banks have trailled variations of the latter. To foster "more efficient KYC checks" Singapore is drawing on blockchain technologies with a national know-your-customer platform containing "government-verified personal details of residents" [131]. Blockchain firms like Switzerland-based Chainalysis are working with a range of regulators, law enforcement, and financial service providers to determine the origin of CCs held by any address [132]. Wider applications of blockchain technologies, such as for verifying the authenticity of identity documents, are being incorporated by firms specialised in the provision of "identity management" services [133, 134]. The consultancy PwC explains how blockchain technologies can enable identification procedures:

> A wealthy individual who needed to prove their identity could walk into a PwC office with their passport and identity documents […] The firm's staff would run

> checks on who the person was, then scan and upload the documents on to the blockchain. The next time that person wanted to prove their identity, they could refer to those records, eliminating the need for later paperwork costing time and money (cited in [135]).

These blockchain-based initiatives respond to calls to establish profiles of 'altcoin' users by drawing on Big Data analytics in identifying individuals associated with particular CC addresses [23]. As the journalist Sarah Jeong [136] explains, "because the Bitcoin network necessarily broadcasts the history of all transactions ever made, analysis of this data can unveil revealing information about particular nodes and their transactional activities". By locating particular patterns of use, companies like BlockTrail and Coinanalytics enhance the ability of intergovernmental police organisations like Europol and Interpol to match CC transactions with individual profiles [53, 137]. Transaction flows are associated with identities matching specific users by drawing on so-called CC 'forensics' developed by computer scientists [138, 139]. These and other initiatives illustrate the "function creep" [140] of blockchain technologies towards *contributing* to rather than solely *undermining* the information and identification efforts of global AML governance. They also more widely exemplify how novel technologies not only challenge but may also support regulatory efforts [141, 142]. The paradox of blockchain technology is therefore that while AML efforts must "deal with imperfect knowledge of identities", they "may exploit perfect knowledge of all transactions" [108].

In advocating rather than undermining the development of such initiatives, the FATF does risk encouraging counter measures that may diminish the effectiveness of its guidance. The advent of blockchain-based identification measures has encouraged the parallel development of anonymisation techniques. For instance, attempts to identify CC users types have been countered by 'anonymizers' that transfer CCs in and out of state-backed currencies using different identities [30]. Firms called 'mixers' or 'tumblers' allow CC users to pool together to prevent identity tracking by 'mixing' and joining transactions together into unpredictable combinations [143].[22] The money laundering capacity of mixers with names like BitLaundry and Bitcoin Fog has been recognised by computer scientists [108].[23] Another technology called the Dark Wallet developed by a collective of "politically radical coders" including the inventor of the 3D gun seeks to "neuter" attempts to tie individual identities to CC transactions and ownership by mixing and further encrypting transaction histories [144]. Finally, CCs like Zcash and Zerocoin as well as Dash, formerly known as Darkcoin, have arisen to provide complete anonymity in digital transactions [145–147]. Reflecting these developments, a wider split has occurred between advocates and sceptics of efforts to harness blockchain technologies in support of global AML efforts [31].

Complex attempts to maintain anonymity and avoid centralisation threaten to push the CC ecosystem further into to financial 'underworld' while limiting its wider attraction for either legitimate or illegitimate uses as traditional forms of money in the financial 'upperworld'. Indeed, the practical and intellectual complexities involved with 'mixing' and further encryption of transactions are unlikely to enhance the attractiveness of these CCs for money laundering nor for more everyday monetary transactions. Legal

[22] See for instance the anonymisation method 'CoinJoin': https://en.bitcoin.it/wiki/CoinJoin

[23] https://laundryzlzgnni4n.onion.to/; Bit Fog was linked to the laundering of stolen Bitcoins from a Chinese exchange in 2015 [152]. and create blacklists of userslaundering of stolen Bitcoins from a Chinese exchange

researcher have already attributed the lack of "large-scale" money laundering with CCs to "a lack of technical knowledge and resources among the relevant populations" ([33], p. 336). Short of significant reductions in these not insignificant technical hurdles, the FATF guidance provides an effective balance between the actual opportunities and potential challenges that the advent of CCs presents to global AML governance.

## Conclusions

What are the implications of 'crypto-coins' (CCs) like Bitcoin for global anti-money laundering governance? This article argued that the threats CCs pose to global AML efforts are presently more theoretical than actual. Despite at times sensationalistic media coverage, little evidence directly implicates CCs in widespread money laundering. As the sociologist Ole Bjerg usefully reminds us, money laundering did not originate with the advent of CCs ([3] p. 69). National currencies and a host of other digital technologies currently present equal if not greater money laundering challenges [148]. CCs currently provide less of a *threat* and more of an *opportunity* to global efforts to combat this illicit practice. Focusing on the novel technological features underlying CCs rather than their conventional uses as traditional forms of money, helps to consider not only the threats but also the concrete possibilities for 'altcoins' to support global AML efforts.

How effectively has the global AML regime balanced the challenges and opportunities presented by the emergence of Bitcoin and competing CCs? This article contended that in spite of several important limits, the risk-based approach pursued by the FATF currently provides an effective balance in mitigating the *potential* risks and *actual* opportunities that CCs present to global AML efforts. Its decentralised risk-based approach was regarded as appropriate for addressing money laundering in the decentralised networks in which CC transactions occur. The FATF more widely approach accords with networked and experimental forms of governance that appear to be more effective than centralised forms of coercion in digital realms where operations can shift to less restrictive jurisdictions with relative ease and speed. Nevertheless, this argument was advanced cautiously, recognising several risks with the 'risk-based approach', such as the reliance on technologies and market-based solutions.

Together then these arguments should be taken as a call for moderation between inaction and overreaction. Networked and decentralised global governance approaches still involve persistent roles for the monitoring for which the FATF is renowned. Yet, should CCs begin to more closely resemble conventional forms of money- particularly as media of exchange and more stable stores of value- as well as to be used for money laundering, then more traditional approaches will need to be considered. How exactly 'harsher' approaches, such as those undertaken to shut down Silk Road 1.0 and 2.0, might be implemented and international coordinated in manners that avoid global races to the bottom remain of central importance for policy-makers and scholars alike to consider.

Wider methodological and epistemological issues also require further contemplation. How can evidence of money laundering be collected from activities characterised by pseudo-anonymity? How much evidence might be necessary to justify more coercive international actions? How can the coordination and assessment of global anti-money laundering efforts evaluate the ethical implications arising from applications of novel technologies that allow for both the undertaking and monitoring of digital transactions?

Scholars are only now beginning to address these wider issues with regards to CCs [e.g. 149–151]. Just as the horizons of research on money can be expanded, so too can measurements of effectiveness include the ethical, political, social, as well as economic implications stemming from the rapid and unpredictable changes to the character of global financial flows in the twenty-first century.

## References


1. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf.
2. Wladawsky-Berger, I. (2014). Bitcoin and the internet of money. *Wall Street Journal*.
3. Bjerg, O. (2016). How is bitcoin money? *Theory, Culture & Society, 33*(1), 53–72.
4. Selgin, G. (2015). Synthetic commodity money. *Journal of Financial Stability, 17*, 92–99.
5. Yermacka, D. (2015). Is bitcoin a real currency? An economic appraisal. In D. L. K. Chuen (Ed.), *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data* (pp. 31–43). London: Academic Press.
6. *PwC*. (2015). Money is no object: Understanding the evolving cryptocurrency market. https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf. Accessed on 16 Aug 2016.
7. *PwC*. "PwC launches new global technology team to harness Bitcoin technology". 21 January. http://pwc.blogs.com/press_room/2016/01/pwc-launches-new-global-technology-team-to-harness-bitcoin-technology.html. Accessed 27 Aug 2016.
8. Graham, L. (2016). Bitcoin boosted by safe-haven demand after Trump victory. *CNBC*.
9. McCrum, D. (2017) Bitcoin passes $1,000 but only number that matters is zero. *Financial Times*.
10. Quandl. (2016). Bitcoin estimated transaction volume USD. https://www.quandl.com/data/BCHAIN/ETRVU-Bitcoin-Estimated-Transaction-Volume-USD. Accessed 27 Aug 2016.
11. Kocherlakota, N. R. (1998). Money is memory. *Journal of Economic Theory, 81*(2), 232–251.
12. Banque de France. (2013). The dangers linked to the emergence of virtual currencies: the example of bitcoins. *Focus*, 10.
13. Arthur, C. (2013). Bitcoin now 'unit of account' in Germany. *Guardian*.
14. Beer, C., & Weber, B. (2014). Bitcoin: the promise and limits of private innovation in monetary and payment systems. *Monetary Policy & the Economy, 4*(14), 53–66.
15. *European Central Bank*. (2015). Virtual currency schemes – a further analysis. ISBN 978–92–899-1560-1.
16. Scott, B. (2016). *How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?* (UNRISD Working Paper No. 2016-1).
17. Cohen, B. (2016). The IPE of money revisited. *Review of International Political Economy*, p. 24.
18. Moini, M. (2001). Toward a general theory of credit and money. *Review of Austrian Economics, 14*(4), 267–317.
19. Maurer, B. (2005). *Mutual life, limited: Islamic banking, alternative currencies, lateral reason*. Princeton: Princeton University Press.
20. van Duyne, P. C., von Lampe, K., & Passas, N. (2002). *Upperworld and underworld in cross-border crime*. Nijmegen: Wolf Legal Publishers.
21. Roberge, I. (2007). Misguided policies in the war on terror? The case for disentangling terrorist financing from money laundering. *Politics, 27*(3), 196–203.
22. Shields, P. (2005). When the 'information revolution' and the US security state collide: money laundering and the proliferation of surveillance. *New Media & Society, 7*(4), 483–512.
23. Stokes, R. (2013). Anti-money laundering regulation and emerging payment technologies. *Banking & Financial Services Policy Report, 32*(5), 1–10.
24. DeNardis, L. (2014). *The global war for internet governance*. New Haven: Yale University Press.
25. Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.
26. Murck, P. (2013). Beyond silk road: potential risks, threats, and promises of virtual Currencies [Hearing before the *committee on Homeland Security and Government Affairs*, 113th Congress, first session]. Washington: U.S. Government Printing Office.
27. Rubenfeld, S. (2015). FATF pushes risk-based approach toward virtual currencies, services. *Wall Street Journal*.

28. Choo, K.-K. R. (2015). Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In D. L. K. Chuen (Ed.), *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data* (pp. 283–307). London: Academic Press.
29. Yelowitz, A., & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters, 22*(13), 1030–1036.
30. Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Indiana Law Journal, 89*(1), 441–472.
31. Nicholls, J. (2016a). Are decentralised currencies better at curing AML woes? Experts split. *Blockchain Briefing*.
32. Her Majesty's Treasury and Home Office. (2015). *UK national risk assessment of money laundering and terrorist financing*. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf.
33. Brown, S. D. (2016). Cryptocurrency and criminality: the Bitcoin opportunity. *The Police Journal, 89*(4), 327–339.
34. Committee on Payments and Market Infrastructures. (2015). CPMI Report on Digital currencies. *Bank for International Settlements*. Available at http://www.bis.org/cpmi/publ/d137.htm.
35. He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., … & Verdugo-Yepes, C. (2016). *Virtual currencies and beyond: initial considerations* [IMF Staff Discussions Note SDN/16/03].
36. Valcke, P., Vandezande, N., & van de Velde, N. (2015). *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4*. [Working paper number 2015-001]. London: The SWIFT Institute.
37. Cyber Intelligence Section and Criminal Intelligence Section. (2012). *Bitcoin virtual currency: unique features present distinct challenges for deterring illicit activity*. Federal Bureau of Investigation. Available at http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf. Accessed 27 Aug 2016.
38. American House Committee on Appropriations. (2013). *Commerce, justice, science, and other related agencies appropriation bill,* 2014. 113th United States Congress. https://www.congress.gov/113/crpt/hrpt171/CRPT-113hrpt171.pdf. Accessed 27 Aug 2016.
39. Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In A.R. Sadeghi (Ed.), *Financial cryptography and data security* [FC 2013. Lecture notes in computer science, 7859] (pp. 25–33). New York: Springer Berlin Heidelberg.
40. Escritt, T. (2014). Police need powers to tackle virtual money laundering: Europol. *Reuters*.
41. Weir, M. (2014). HSBC severs links with firm behind Bitcoin fund. *BBC*.
42. McLannahan, B. (2017). US banks 'wasting billions' trying to track crime. *Financial Times*.
43. Van Steinis, H. (2016). Handled right, blockchain could help banks and their customers. *Financial Times*.
44. Hern, A. (2014). A history of bitcoin hacks. *The Guardian*.
45. Bitfinex. (n.d.). *Terms of Service*. https://www.bitfinex.com/terms. Accessed 27 Aug 2016.
46. Southurst, J. (2013). World's largest Bitcoin exchange BTC China now requires ID. *CoinDesk*.
47. Gatecoin. (n.d.) *Anti-money laundering and counter-terrorist financing (AML/CFT) policy summary statement*. https://gatecoin.com/amlpolicy. Accessed 27 Aug 2016.
48. Bitstamp. (n.d.) *Bitstamp limited anti-money laundering ("AML") and counter terrorist financing ("CTF") policy*. https://www.bitstamp.net/aml-policy/. Accessed 27 Aug 2016.
49. CEX.IO. (n.d.). *AML/KYC Policy*. https://cex.io/aml-kyc. Accessed 27 Aug 2016.
50. HitBTC. (n.d.) *HitBTC terms of use*. https://hitbtc.com/terms-of-use. Accessed 27 Aug 2016.
51. Hughes, S., & Middlebrook, S. (2014). Regulating cryptocurrencies in the United States: current issues and future directions. *William Mitchell Law Review, 40*, 813–844.
52. Digital Asset Transfer Authority (2015). *Draft Anti-Money Laundering Guidelines*. Available at: http://datauthority.org/blog/2015/07/01/global-aml-kyc-guidelines-data/.
53. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., Voelker, G. M., Savage, S., & McCoy, D. (2013). A fistful of bitcoins: characterizing payments among men with no names. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 127–139.
54. Simser, J. (2015). Bitcoin and modern alchemy: in code we trust. *Journal of Financial Crime, 22*(2), 156–169.
55. Roberge, I. (2011). The Financial Action Task Force. In D. Held & T. Hale (Eds.), *The Handbook of Transnational Governance Innovation* (pp. 45–50). Cambridge: Polity Press.
56. Jacobi, A. P. (2012). The FATF as the central promoter of the anti-money laundering regime. In K. S. Helgesson & U. Mörth (Eds.), *Securitization, accountability and risk management: Transforming the public security domain* (pp. 16–33). London: Routledge.
57. Wong, J. (2016). Bitcoin exchanges can't stop getting hacked, no matter what security system they use. *Quartz*.
58. Bollen, R. (2013). The legal status of online currencies: are bitcoins the future? *Journal of Banking and Finance Law and Practice, 24*(3), 272–293.

59. Christopher, C. M. (2014). Whack-a-mole: why prosecuting digital currency exchanges won't stop online laundering. *Lewis and Clark Law Review, 18*(1), 1–36.
60. Elwell, C. K., Murphy, M. M., & Seitzinger, M. V. (2015). *Bitcoin: questions, answers, and analysis of legal issues*. Washington: Congressional Research Service.
61. Farmer, P. (2014). Speculative tech: the Bitcoin legal quagmire and the need for legal innovation. *Journal of Business & Technology Law, 9*(1), 85.
62. Penrose, K. L. (2013). Banking on Bitcoin: applying anti-money laundering and money transmitter laws. North Carolina Banking Institute*, 18*, 529-551.
63. Kiviat, T. I. (2015). Beyond Bitcoin: issues in regulating blockchain transactions. *Duke Law Journal, 65*, 569–608.
64. Pflaum, I., & Hateley, E. (2013). Bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation. *Georgetown Journal of International Law, 45*, 1169–1215.
65. Singh, K. (2015). New wild west: preventing money laundering in the Bitcoin network. *Northwestern Journal of Technology and Intellectual Property, 13*(1), 38–64.
66. Raymond, N. (2014). Bitcoin backer gets two years prison for illicit transfers. *Reuters*.
67. Hudak, S. (2015). *FinCEN fines Ripple Labs Inc. in first civil enforcement action against a virtual currency exchanger*. Washington, DC: United States Department of the Treasury, Financial Crimes Enforcement Network. https://www.fincen.gov/news_room/nr/html/20150505.html. Accessed 27 Aug 2016.
68. Townend, D. (2015a). Credit union bribery concealed Bitcoin money laundering. *Payments Compliance*.
69. Fung, B. (2015). Why the Justice Department is going after this Bitcoin exchange. *Washington Post*.
70. Henning, P. (2015). The challenges of fighting money laundering. *New York Times*.
71. Reynolds, J. (2002). The new US anti-money laundering offensive: will it prove successful? *Cross Cultural Management: An International Journal, 9*(3), 3–31.
72. Smart, E. (2015). Top 10 countries in which Bitcoin is banned. *CryptoCoinNews*.
73. Bank Indonesia. (2014). Statement of bank Indonesia related to Bitcoin and other virtual currency. http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/SP_160614.aspx. Accessed 27 Aug 2016.
74. European Central Bank. (2016). Opinion of the European Central Bank. Available at: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf. Accessed 23 November.
75. European Banking Authority. (2014). *EBA Opinion on 'virtual currencies'*. (EBA/Op/2014/08).
76. Eikelenboom, S., & Dobber, J. (2017). OM voert strijd op tegen witwassen via bitcoin. *Financiele Dagblad*.
77. Engle, E. (2016). Is Bitcoin rat poison? Cryptocurrency, crime, and counterfeiting (CCC). *Journal of High Technology Law, 16*(2), 340–393.
78. Commonwealth Working Group on Virtual Currencies. (2015). Working Group Report. Available at: http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf. Accessed 24 November.
79. Wright, A., & De Filippi, P. (2015). *Decentralized blockchain technology and the rise of lex cryptographia*. Available at SSRN 2580664.
80. Tracfin. (2014). *Regulating virtual currencies: recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering* [Virtual Currencies Working Group Report]. Ministere des Finances et des Publics.
81. del Castillo, M. (2015). The 'great Bitcoin exodus' has totally changed New York's Bitcoin ecosystem. *New York Business Journal*.
82. Van Valkenburgh, P. (2015). Tracking Bitcoin regulation state by state. *CoinCentre*.
83. Nance, M. (forthcoming). The regime that the Financial Action Task Force on money laundering built. *Crime, Law, and Social Change*.
84. Young, J. (2015). While other companies leave NY, Coinbase submits BitLicense application. *Bitcoin Magazine*.
85. Townend, D. (2015b). Singapore PM makes blockchain leader case. *Blockchain Briefing*.
86. Connell, J. (2014). Alderney: gambling, Bitcoin and the art of unorthodoxy. *Island Studies Journal, 9*(1), 69–78.
87. Nicholls, J. (2016b). Isle of man sees Blockchain through prism of e-gaming triumphs. *Blockchain Briefing*.
88. Fernholz, T. (2015). Terrorism finance trackers worry ISIS already using Bitcoin. *Defense One*.
89. Porter, T. (2003). *Technology, governance and political Conflict in international industries*. London: Routledge.
90. United Nations Office on Drugs and Crime. (2017). *UNODC helps tackle bitcoin banking fraud and money laundering*. Retrieved from http://www.unodc.org/unodc/en/frontpage/2017/February/unodc-helps-tackle-bitcoin-banking-fraud-and-money-laundering.html.
91. Eyers, J. (2015). Why the blockchain will propel a services revolution. *Australian Financial Review*.

92. Europol. (2015). *Europol interpol makes cybercrime conference makes the case for multisector cooperation*. https://www.europol.europa.eu/latest_news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-greater-multisector-cooperation . Accessed 27 Aug 2016.
93. Financial Action Task Force. (2016). International standards on combating money laundering and the financing of terrorism and proliferation: the FATF recommendations. http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf. Accessed 15 Aug 2016.
94. Amicelle, A. (2011). Towards a 'new' political anatomy of financial surveillance. *Security dialogue, 42*(2), 161–178.
95. Slaughter, A. M. (2009). *A new world order*. Princeton: Princeton University Press.
96. Sabel, C. F., & Zeitlin, J. (2008). Learning from difference: the new architecture of experimentalist governance in the EU. *European Law Journal, 14*(3), 271–327.
97. Financial Action Task Force. (2013). *Guidance for a risk-based approach to prepaid cards, mobile payments and internet-based payment services*. http://www.fatf gafi.org/publications/fatfrecommendations/documents/rba-npps-2013.html. Accessed 15 Aug 2016.
98. Financial Action Task Force. (2014). *Virtual currencies: key definitions and potential AML/CFT Risks: FATF Report*. http://www.fatfgafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Accessed 15 Aug 2016.
99. Financial Action Task Force. (2015a). *Guidance for a risk-based approach: virtual currencies*.https://www.coe.int/t/dghl/monitoring/moneyval/Publications/Guidance-RBA-Virtual-Currencies.pdf. Accessed 15 Aug 2016.
100. Luther, W. J., & Olson, J. (2013). Bitcoin is memory. *Journal of Prices & Markets, 3*(3), 22–33.
101. Helleiner, E. (2002). The politics of global financial regulation: lessons from the fight against money laundering. In J. Eatwell & L. Taylor (Eds.), *International capital markets: Systems in transition* (pp. 177–204). Oxford: Oxford University Press.
102. Kern, A. (2001). The international anti-money-laundering regime: The role of the financial action task force. *Journal of Money Laundering Control, 4*(3), 231–248.
103. Sharman, J. (2011). *The money laundry: Regulating criminal finance in the global economy*. New York: Cornell University Press.
104. Zoppei, V. (2015). Money laundering: a new perspective in assessing the effectiveness of the AML regime. *The European Review of Organised Crime, 2*(1), 130–148.
105. Tsingou, E. (2010). Global financial governance and the developing anti-money laundering regime: what lessons for international political economy? *International Politics, 47*(6), 617–637.
106. Hülsse, R., & Kerwer, D. (2007). Global standards in action: insights from anti-money laundering regulation. *Organization, 14*(5), 625–642.
107. Truman, E. M., & Reuter, P. (2004). *Chasing dirty money: progress on anti-money laundering*. Washington: Institute for International Economics.
108. Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *eCrime Researchers Summit (eCRS)*. pp. 1-14.
109. Favarel-Garrigues, G., Godefroy, T., & Lascoumes, P. (2009). *Les sentinelles de l'argent sale au quotidian: Les banques aux prises avec l'antiblanchiment*. Paris: La Decouverte.
110. Liss, C., & Sharman, J. C. (2015). Global corporate crime-fighters: Private transnational responses to piracy and money laundering. *Review of International Political Economy, 22*(4), 693–718.
111. Pagliari, S. (2012). *Making good financial regulation: Towards a policy response to regulatory capture*. London: Grosvenor House Publishing.
112. Campbell-Verduyn, M. (2016). Merely TINCering around: the shifting private authority of technology, information and news corporations. *Business & Politics, 18*(2), 143–170.
113. Parker, L. (2015). Controversy arises as new Blockchain Alliance engages with US law enforcement. *Brave New Coin*.
114. Europol. (2015). *The internet organised crime threat assessment (IOCTA) 2015*. The Netherlands: European Law Enforcement Agency (Europol). https://www.europol.europa.eu/iocta/2015/. Accessed on Aug 16.
115. Black, J., & Baldwin, R. (2012). When risk- based regulation aims low: Approaches and challenges. *Regulation & Governance, 6*(1), 2–22.
116. De Koker, L. (2009). Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance. *Journal of financial crime, 16*(4), 334–352.
117. G7 Germany. (2015). *Leaders declaration* G7 *summit 7–8 June 2015*. https://sustainabledevelopment.un.org/content/documents/7320LEADERS%20STATEMENT_FINAL_CLEAN.pdf. Accessed 16 Aug 2016.

118. Deloitte. (2015). *State-sponsored cryptocurrency: adapting the best of Bitcoin's innovation to the payments ecosystem*. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-state-sponsored-cryptocurrency.pdf. Accessed 27 Aug 2016.
119. Spaven, E. (2015). Citi: UK Government Should Create Own Digital Currency. *CoinDesk*.
120. Stafford, P. (2016). Canada experiments with digital dollar on blockchain. *Financial Times*.
121. Sier, J. (2016). Chinese officials discuss bitcoin and their own digital currency. *Sydney Morning Herald*.
122. Chanjaroen, C., & Roman, D. (2016). Singapore to test digital currency in latest Fintech initiative. *Bloomberg*.
123. Eyers, J. (2016). Central banks look to the future of money with blockchain technology trial. *Australian Financial Review*.
124. Higgins, S. (2016). Dutch Central Bank to create prototype blockchain-based currency. *CoinDesk*.
125. Shan, H. P. (2015). Singapore-based Interpol centre creates virtual currency to fight crime. *The Straight Times*.
126. Nicholls, J. (2015). Blockchain requires 'regulatory war games', says Harvard professor. *Blockchain Briefing*.
127. Taylor, M. (2015). U.S. treasury official: 'blockchain can solve compliance problems'. *Blockchain Briefing*.
128. Identabit. (n.d.). *We are Identabit*. http://identabit.com/.
129. Institute of International Finance. (2015). *Banking on the blockchain: reengineering the financial architecture*.
130. Basquill, J. (2015b). Isle of man: blockchain 'reg tech' just the beginning. *Payments Compliance*.
131. Azhar, S., & Zaharia, M. (2016). Singapore to launch blockchain project for interbank payments. *Reuters*.
132. Prisco, G. (2015). Leaked chainalysis roadmap angers Bitcoin community. *Bitcoin Magazine*.
133. McMillan, R. (2014). Hacker dreams up crypto passport using the tech behind Bitcoin. *Wired*.
134. Kharif, O. (2014). Bitcoin 2.0 shows technology evolving beyond use as money. *Bloomberg*.
135. Wild, J. (2015). Blockchain believers seek to shake-up financial services. *Financial Times*.
136. Jeong, S. (2013). The Bitcoin protocol as law, and the politics of a stateless currency. Available at SSRN 2294124.
137. Basquill, J. (2015a). Interpol reveals Bitcoin tracking research. *Blockchain Briefing*.
138. Bohannon, J. (2016). The Bitcoin busts. *Science, 351*(6278), 1144–1146.
139. Luu, J., & Imwinkelried, E. J. (2016). The challenge of Bitcoin pseudo-anonymity to computer forensics. *Criminal Law Bulletin*.
140. Dahl, J. Y., & Sætnan, A. R. (2009). "It all happened so slowly"– on controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice, 37*(3), 83–103.
141. Auld, G., Cashore, B., Balboa, C., Bozzi, L., & Renckens, S. (2010). Can technological innovations improve private regulation in the global economy? *Business & Politics, 12*(3), 1–39.
142. Demetis, D. S. (2010). *Technology and anti-money laundering: A systems theory and risk-based approach*. Cheltenham: Edward Elgar Publishing.
143. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–236.
144. Greenberg, A. (2014). Dark wallet is about to make Bitcoin money laundering easier than ever. *Wired*.
145. Dash. (n.d.). *What is Dash?* https://www.dash.org/. Accessed 27 Aug 2016.
146. Zerocoin Project. (n.d.). *What is Zerocoin?* http://zerocoin.org/. Accessed 27 Aug 2016.
147. Zcash. (n.d.). *About*. https://z.cash/. Accessed 22 Nov 2016.
148. Richet, J-L. (2013). Laundering money online: a review of cybercriminals methods. United Nations Office on Drugs and Crime (UNODC).
149. Angel, J. J., & McCabe, D. (2015). The ethics of payments: paper, plastic, or Bitcoin? *Journal of Business Ethics, 132*(3), 603–611.
150. Reijers, W., & Coeckelbergh, M. (2016). The Blockchain as a narrative technology: investigating the social ontology and normative configurations of cryptocurrencies. *Philosophy & Technology*, 1–28. https://doi.org/10.1007/s13347-016-0239-x
151. Dierksmeier, C., & Seele, P. (2016). Cryptocurrencies and business ethics. *Journal of Business Ethics*, 1–14. https://doi.org/10.1007/s10551-016-3298-0.
152. Décary-Hétu, D., & Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75.
153. Irwin, A. S., Irwin, A. S., Milad, G., & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, 19*(4), 407–425.
154. Brill, A., & Lonnie, K. (2014). Cryptocurrencies: the next generation of terrorist financing? *Defence Against Terrorism Review, 6*(1), 7–30.
155. Bershidsky, L. (2015). *Leave Bitcoin alone*. Bloomberg: Abolish cash instead.
156. Perez, Y. (2015). Bitcoin, Paris and terrorism: what the media got wrong. *Coindesk*.
157. Polillo, S. (2013). *Conservatives versus wildcats: A sociology of financial conflict*. Stanford: Stanford University Press.

158. European Commission. (2016). *Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*. http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf>. Accessed 27 Aug 2016.
159. Financial Action Task Force. (2015b). *Emerging terrorist financing risks: FATF Report*. http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf. Accessed 15 Aug 2016.
160. Sharman, J. C. (2008). Power and discourse in policy diffusion: anti-money laundering in developing states. *International Studies Quarterly, 52*(3), 635–656.
161. Williamson, C., Vazquez, J., Thomas, J., & Sagona-Stophel, K. (2013). Technology in the fight against money laundering in the new digital currency age. Thomson Reuters Accelus. https://risk.thomsonreuters.com/sites/default/files/GRC00403_0.pdf. Accessed 16 Aug 2016.
162. Maina, J.W. (2015). 20,000 Customers affected as bter scrambles to refund stolen Bitcoin. *Cryptocoinsnews*.