FACULTY OF LAW

Lund University

Jesse H. Rigsby, IV

Virtual Currency, Blockchain Technology, and EU Law: The “Next Internet” in AML/CFT Regulation’s Shadow

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Henrik Norinder
Term: Spring 2016

Contents

Summary iv

Preface v

Abbreviations vi

I. Introduction 1

A. The “Next Internet”? 1

B. Criminals, Terrorists, and the Shadow of AML/CFT Regulation 4

C. The European Union Takes Notice 10

D. Thesis Outline and Sources and Methodology 13

E. Related Literature 14

II. AML/CFT Regulation in the EU 16

A. Fundamentals 16

B. EU Anti-Money Laundering Law in an International Context 24

III. Virtual Currency and Blockchain: A Factual and Legal Primer 27

A. Basic Concepts 27

B. Attributes Important to AML/CFT Regulation 29

i. Non-Legal Tender Status 29

ii. Anonymity (?) 30

iii. Lack of Fundamental or Intrinsic Value 32

iv. Vulnerability to a “51% attack” 36

v. Easy and Cheap International Transmissibility 37

vi. No Centralized Institutions 38

C. EU Case Law 38

IV. AML/CFT Regulation of Blockchain-Based Virtual Currency Under EU Law 44

A. The Current Situation 44

i. The European Commission 44

ii. The European Parliament 47

iii. The European Central Bank 49

iv. Financial Action Task Force 50

B. The Problem and a Proposed Solution 51

i. The Problem 51

ii. A Proposed Solution 57

V. Conclusion 60

Bibliography and Cases 61

Summary

Virtual currency based on blockchain technology represents an innovation many have likened to the “next Internet” in terms of its “disruptive potential.” While the implications in the financial sphere are still unclear, the same can be said for what it all may mean for anti-money laundering (AML) and counter-financing of terrorism (CFT) regulation. Because key features of existing virtual currencies such as Bitcoin, including near-anonymity and disintermediation, are anathema to the foundations of AML/CFT regulation both in the EU and internationally, the EU will need to adopt a comprehensive AML/CFT regulatory approach to virtual currencies that goes beyond simply trying to extend the Fourth Anti-Money Laundering Directive.

The following thesis examines the current status of AML/CFT regulation of virtual currencies in the EU and makes recommendations as to how to reconcile what would otherwise be two incompatible systems. After presenting a factual overview, the thesis discusses the Fourth Anti-Money Laundering Directive, outlines features of existing blockchain-based virtual currencies that present AML/CFT difficulties, discusses *Skatteverket v. David Hedqvist*, a case referred for a preliminary reference to the ECJ from Sweden that represents the first virtual currency related-case decided by the CJEU, and then discusses the current status of AML/CFT regulation of virtual currency in the EU. The thesis concludes by presenting the problems posed by the EU’s incremental regulatory approach as well as a proposed regulatory solution that balances the need to avoid stifling innovation with the need to preserve AML/CFT regulatory goals.

Preface

Not many American lawyers get the opportunity to step outside of the U.S. legal system mid-career and study the law from another perspective, one that is sometimes strangely foreign yet other times deeply familiar. I am grateful for the opportunity to have done just that. My sincere thanks to the law faculty at Lund University for what has been a fascinating and insightful master's program. Thank you to Henrik Norinder, my master's thesis advisor who has graciously offered his guidance and support throughout the research and writing process. Particular gratitude goes to Hans Henrik Lidgard and Justin Pierce, from whom I learned an awful lot in a short time. Back home in North Carolina, Donald Strickland, Karen Rabenau, Donald Beskind, and Steven L. Schwarcz have my sincere respect and thanks. But most of all thank you to my dear wife Jackie for supporting me throughout.

Abbreviations

4th AMLD	Fourth Anti-Money Laundering Directive
AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CDA	Communications Decency Act of 1996
CDD	Customer Due Diligence
CFT	Counter-Financing of Terrorism
CJEU	Court of Justice of the European Union
DLT	Distributed Ledger Technology
EBA	European Banking Authority
ECB	European Central Bank
ECJ	European Court of Justice
ECON	Committee on Economic and Monetary Affairs
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IMCO	Committee on the Internal Market and Consumer Protection
ISIS/ISIL	Islamic State of Iraq and Syria/Islamic State of Iraq and the Levant
TFEU	Treaty on the Functioning of the European Union
VAT	Value Added Tax

I. Introduction

A. *The "Next Internet"?*

First, a personal anecdote. The author recalls visiting the so-called "World Wide Web" for the first time in early 1994 and being deeply unimpressed: there was almost no content. The several thousand websites then in existence[1] were almost exclusively the pet projects of a limited number of hobbyists and academics and were largely devoid of interesting material. While the "Internet" was a groundbreaking concept, the then-current form was undeveloped, and the idea of it one day becoming indispensable would have struck most at the time as bizarre and improbable. Even email had limited use since few individuals had email addresses or knew how to use what was then a cumbersome and awkward technology.

More than twenty years later, we know how everything turned out, and in retrospect the inevitability of the internet's transformation from almost useless to a fundamental part of daily life seems preordained. This is of course nonsense.[2] We forget quickly how humble and unassuming the beginnings of the internet actually were, particularly when the outcome has been anything but.

The purpose of this reminiscing is that virtual currency and its underlying blockchain technology is frequently described in terms reflecting the state of the internet twenty-plus years ago. Phrases such as "nascent stage" and "niche phenomenon"[3] would be just as apt to describe the internet during its early years, before the dot-com explosion, as the current state of virtual currency.[4] (The PR problems faced by virtual currency also have parallels from the

[1] *See* statistics at http://stuff.mit.edu/people/mkgray/net/web-growth-summary.html.

[2] To illustrate, Steve Case, the co-founder and former CEO and chairman of internet giant AOL, stated that the "conventional wisdom was that the [internet] market would always be limited to hackers/hobbyists" and that in the early 1990s, "given that we [AOL] had been in business 7 years and had less than 200,000 users, most were skeptical" there would ever be a wider market. In addition, after the dot-com meltdown in the early 2000s, "[m]ost people thought the Internet as a passing phase." *See* Steve Case, *The Complete History of the Internet's Boom, Bust, Boom Cycle*, Business Insider (Jan. 14, 2011), available at http://www.businessinsider.com/what-factors-led-to-the-bursting-of-the-internet-bubble-of-the-late-90s-2011-1?IR=T.

[3] Marcin Szczepański, European Parliamentary Research Service Briefing Paper, *Bitcoin: Market, economics and regulation*, p. 5 (11/04/2014), available at http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf.

[4] Others have had similar thoughts in the virtual currency/blockchain context and have drawn similar parallels, even pointing out that what seems obvious about the internet in retrospect was not obvious at the time of its development:

> Predicting the future in the face of technological change is almost certainly a fool's errand. . . Looking back, it seems obvious that Amazon would push out not only the small local bookstore but also the megabookstore chains and many other brick-and-mortar shops that sell a wide range of products. But it was not so obvious at the time. The Internet was neat. It made it easier to chat with loved ones and find new friends. However, it was difficult to imagine in the late 1990s all the ways in which it would touch our day-to-day lives in the future—let alone which companies would come to dominate the landscape. Much the same might be said about the future of digital payments today.

William J. Luther, *Bitcoin and the Future of Digital Payments*, 20 The Independent Review 3, p. 400 (Winter 2016)(emphasis added).

Similarly, venture capitalist Marc Andreessen of the firm Andreessen Horowitz – which has invested tens of millions in virtual currency/blockchain-related startups – has analogized the present stage of virtual currencies to the internet in 1993 and made the point that the retrospective obviousness of a technology's transformative nature is not necessarily so obvious at the beginning:

internet's formative years, when the scams, pornography, and get-rich-quick schemes that abounded gave the internet an unsavory reputation in some quarters.[5])

As a quick primer, virtual currency and blockchain technology use a decentralized, peer-to-peer distributed network and cryptologic technology to allow users to send value (or digital representations of value) quickly, reliably, safely, and pseudo-anonymously across international borders and to store value electronically outside of traditional banking systems.[6] The most (in)famous virtual currency is currently Bitcoin, but there are at present some 500 or more others vying for users' attention. Virtual currency and blockchain technology could not exist but-for the internet and computers having reached sufficiently advanced stages, but these innovations, though wholly dependent upon their predecessor technologies, are something entirely new. While virtual currency (as currently conceptualized) relies on blockchain technology, blockchain technology can also power other innovations, such as electronic identification verification, e-voting via smartphone apps, proof of intellectual property ownership, auditing of financial transactions, settlement of securities transactions, and tracking valuable commodities.[7] Another non-virtual currency application of blockchain technology is so-called "smart contracts," contracts that rely on computer programming to self-execute according to preset "if-then" rules.[8]

The potential transformative nature of virtual currency and blockchain as analogous to the beginnings of the internet is widely recognized. It is in fact so widely recognized that it has become a trendy-to-the-point-of-trite thing to say. For example, a headline in The Telegraph proclaimed, "Bitcoin revolution could be the next internet, says Bank of England."[9] The title of an article on the Hewlett Packard Enterprise website similarly mused

> A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers. Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it. On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it. Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start. What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014.

Marc Andreessen, *Why Bitcoin Matters*, New York Times – Dealbook (Jan. 21, 2014), available at http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (emphasis added). Wim Raymaekers, writing in the Journal of Payments Strategy & Systems, similarly remarked that "[o]ne should therefore look beyond today's state and uses of Bitcoin, recalling the internet in the early 1990s, when it was a set of user-unfriendly hypertext pages pointing to a few newsgroups." Wim Raymaekers, *Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities*, Journal of Payments Strategy & Systems Volume 9 Number 1 (December 8, 2014).

[5] *See* Sam Kessler, *The Future of Bitcoin: A Rocky Path to Currency*, Harvard Political Review (January 19, 2016), at http://harvardpolitics.com/covers/covers-winter-2015/future-bitcoin-rocky-path-currency/ (stating that "Fabio Federici of Coinalytics compares Bitcoin to the early days of the Internet, arguing to the [Harvard Political Review] that the state of Bitcoin is 'just like we saw with the Internet where the first uses were things like pornography and gambling'").

[6] Virtual currency and blockchain technology are described in more detail in Chapter III, below.

[7] Mike Montgomery, *Bitcoin is Only the Beginning for Blockchain Technology*, Forbes (Sep. 15, 2015), available at http://www.forbes.com/sites/mikemontgomery/2015/09/15/bitcoin-is-only-the-beginning-for-blockchain-technology/#11728fb86f04.

[8] *See, e.g.*, Chris DeRose, *'Smart Contracts' are the Future of Blockchain*, American Banker (Jan. 8, 2016), available at http://www.americanbanker.com/bankthink/smart-contracts-are-the-future-of-blockchain-1078705-1.html; for examples of websites offering smart contract technology, *see* http://smartcontract.com/ and https://www.ethereum.org/.

[9] Peter Spence, *Bitcoin revolution could be the next internet, says Bank of England*, The Telegraph (25 February 2015), available at http://www.telegraph.co.uk/finance/currency/11434904/Bitcoin-revolution-could-be-the-next-internet-says-Bank-of-England.html.

about the "disruptive potential" of virtual currency technology as the "next internet."[10] An online presentation hosted by LinkedIn's presentation channel SlideShare proclaimed "Blockchain is a lot like the Internet in the '90s: No one understands it, but it's about to be huge."[11] An article in The Economist asked if the blockchain is the "next big thing."[12] Others, such as Mercator Advisory Group which provides research and advisory services to the finance and banking industry, have countered that this sort of talk is "misguided."[13] But talk there nonetheless is. And plenty of it.

But there is not just talk. Like the internet boom, the potential for great wealth to once again be made has not been lost on serious actors. The real interest is not in participating on an operational level such as through speculative trading in virtual currency, "mining," or running exchanges where virtual currencies can be bought and sold, but from innovation – moving the core technology away from a cool idea that appeals to a small self-selecting audience of early adopters to something actually useful for everyone else. Here is how one commentator put it:

> When it comes to paying for everyday items, the masses do not want a virtual currency that is difficult to understand, fluctuates wildly and operates in the shadows. . . To build on it, the major players will have to come together and merge existing technologies, not only to make the system more widely available but more efficient. [14]

Similar to what Google did for search engines and what Amazon and eBay did for online marketplaces, if virtual currency and blockchain technology are to become mainstream then extensive investment and smart development will be required. This is already happening. According to Jakob von Weizsäcker, a German Member of the European Parliament who authored a draft report on virtual currencies discussed later in this paper, "[t]here are many investors out there who have very high hopes that a particular application of this technology will be what they call a killer application."[15] This has led to a gold rush of sorts. As summarized by an article in Forbes:

> 2015 has proven to be the year that venture capital and Wall Street bet on the blockchain. . ., with companies ranging from Goldman Sachs to American Express, from Nasdaq to Kleiner Perkins, investing in such ventures, and VC investment in the sector totaling $314 million according to Pitchbook[.][16]

Swiss Bank UBS has shown interest in adapting blockchain technology to create a new

[10] https://www.hpematter.com/issue-no-6-fall-2015/next-internet-disruptive-potential-bitcoin-and-blockchain.

[11] http://www.slideshare.net/LinkedInPulse/don-alex-tapscott-weekend-essay-blockchain-revolution-bitcoin-finance-money

[12] The Economist, *Blockchain – the Next Big Thing (or is it?)*, (May 9, 2015), available at http://www.economist.com/news/special-report/21650295-or-it-next-big-thing

[13] https://www.mercatoradvisorygroup.com/Press_Releases/Mercator_Advisory_Group_Identifies_How_VC_Investments_Could_Cripple_Bitcoin/

[14] Ross Gerber, *Why Apple Pay And Dollars Are Killing Bitcoin*, Forbes (Jan. 29, 2015), available at http://www.forbes.com/sites/greatspeculations/2015/01/29/why-apple-pay-and-dollars-are-killing-bitcoin/#1c7e007db4b6.

[15] European Parliament News, *Virtual currencies: what are the risks and benefits?* (26 January 2016), available at http://www.europarl.europa.eu/news/en/news-room/20160126STO11514/Virtual-currencies-what-are-the-risks-and-benefits.

[16] Lauran Shin, *Should You Invest In Bitcoin? 10 Arguments In Favor As Of December 2015*, Forbes (Dec 11, 2015), available at http://www.forbes.com/sites/laurashin/2015/12/11/should-you-invest-in-bitcoin-10-arguments-in-favor-as-of-december-2015/#36908490540e.

settlement system for banking transactions,[17] while according to the international consulting firm Accenture, capital-market specific blockchain investment was $75 million in 2015, more than double from the previous year. [18] This figure is expected to more than quadruple by 2019.[19] CNN Money gives even more impressive numbers, claiming that $1 billion has been invested so far in start-up companies focused on virtual currency or blockchain technology, listing powerhouse names such as American Express, Bain Capital, Deloitte, Goldman Sachs, MasterCard, the New York Life Insurance Company, and the New York Stock Exchange as among the major investors.[20] The Wall Street Journal cites M&A advisory firm Magister Advisors as forecasting that Bitcoin would be the sixth largest reserve currency in the world by 2030.[21] Clearly something big is afoot.

B. *Criminals, Terrorists, and the Shadow of AML/CFT Regulation*

But all this enthusiasm overlooks a catch: the danger of stifling regulation. The internet lived to see adulthood because it was largely an American creation allowed to flourish mostly unregulated in the U.S. during its critical development years. Its U.S. roots were critical because they allowed the internet to fall under the rubric of "free speech" and consequent Constitutional protection under the First Amendment. For the benefit of non-U.S. readers, the First Amendment to the U.S. Constitution states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." The First Amendment applies to the states through the Fourteenth Amendment.[22] At a stage where the internet's eventual triumph was far from certain, this crucial legal protection allowed for experimentation and growth subject only to market pressure and not government rules.[23]

For example, in *Reno v. American Civil Liberties Union*[24] the U.S. Supreme Court overturned an early attempt at internet regulation, the Communications Decency Act of 1996 (CDA),[25] which criminalized making "indecent" and "patently offensive" communications available to minors. As the Supreme Court noted, under the CDA, users could have been criminally prosecuted for emailing birth control information to their 17-year old daughter,

[17] Anna Irrera, *UBS Building Virtual Coin For Mainstream Banking*, Wall Street Journal - Digits (3 Sept. 2015), available at http://blogs.wsj.com/digits/2015/09/03/ubs-building-virtual-coin-for-mainstream-banking/.
[18] *Latest Thinking: Blockchain-enabled distributed ledgers: Are investment banks ready?*, available at https://www.accenture.com/us-en/insight-blockchain-enabled-distributed-ledgers-investment-banks.
[19] *Id.*
[20] Jose Pagliery, *Record $1 billion invested in Bitcoin firms so far*, CNN Money (November 3, 2015), available at http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/.
[21] Paul Vigna, *Bitcoin's Volatility Reflects a Work in Progress — BitBeat*, The Wall Street Journal (Nov. 5, 2015), at http://blogs.wsj.com/moneybeat/2015/11/05/bitcoins-volatility-reflects-a-work-in-progress-bitbeat/.
[22] *See Gitlow v. People of State of New York*, 268 U.S. 652, 45 S. Ct. 625 (1925).
[23] *Cf.* Misha Tsukerman, *The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 Berkeley Tech. L.J. 385, 1130 (2015) (arguing that "[p]reventing and mitigating [virtual currency's] risks will require smart, flexible, and active regulation. This regulation must be balanced against concerns over stifling innovation. As with the internet, regulators must strike a balance between protecting the public from Bitcoin's bad actors, while allowing people to experiment with, and develop the technology"). *See also* Mohit Kaushal & Sheel Tyle, *The Blockchain: What it is and Why it Matters*, Brookings Institution (January 13, 2015), available at http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal (cited by Tsukerman, 1130 n.33)(arguing that "[h]ad we over-regulated the Internet early on, we would have missed out on many innovations that we can't imagine living without today. The same is true for the Blockchain. Disruptive technologies rarely fit neatly into existing regulatory considerations, but rigid regulatory frameworks have repeatedly stifled innovation").
[24] 521 U.S. 844, 117 S.Ct. 2329 (1997).
[25] 47 U.S.C. § 223(a)(1)(B) & § 223(d) (1994 ed., Supp. II).

using any of the seven "Filthy Words" from the classic George Carlin radio monologue from 1973 that was the subject of another Supreme Court free speech case, *FCC v. Pacifica Foundation*,[26] or even discussing the Carnegie Library card catalogue (which almost certainly contains offensive titles).[27] Thankfully, the First Amendment did not allow such an abridgement of free speech. If it had been allowed to survive, the CDA would have inevitably chilled the speech of internet content providers and indeed ordinary users,[28] with obvious destructive consequences for the direction of the internet: it is no exaggeration that the internet that we now take for granted would not have been possible under the CDA.

Free speech considerations and strong First Amendment traditions thus protected the internet when it was most vulnerable. Virtual currency and blockchain technology, however, are not typically classed as "speech," despite being constructed out of computer code.[29] They are instead considered a form of payment technology, a currency or at least something currency-like, or maybe a security or something security-like but always something essentially financial.[30] This financial categorization means virtual currency and its enabling blockchain technology are prime candidates for regulation under anti-money laundering (AML) and counter financing of terrorism (CFT) (collectively AML/CFT) regulatory regimes that have taken shape internationally in just the past few decades. These regulatory regimes conceptualize the free transfer of money as paradoxically both necessary to the global economy and inherently threatening to national and international security. Tension arises because constraints on the free movement of capital are viewed as both posing a danger to the efficient functioning of the mechanisms of capitalism while at the same time indispensable to counter organized crime, terrorism, public corruption, proliferation of weapons of mass destruction, and other major threats.

The irony of course is that the channels of free speech enabled by the internet's development have facilitated all the above evils and then some.[31] One reaction in the U.S. and in part of the EU has been the surveillance state.[32] But unlike openly-repressive regimes in other parts of the world, the Western surveillance state mostly monitors online speech without heavy-handedly regulating or constraining whole platforms for expression. Private vigilante collectives like Anonymous and Ghost Security Group have had to fill in this gap by attacking sites that allow online expression to be abused, though with unclear results.[33] There are counterexamples. For instance, against the backdrop of their nation's unique historical

[26] 438 U.S. 726, 98 S.Ct. 3026 (1978).

[27] *See* 521 U.S. at 878.

[28] *See id.* at 870 – 874.

[29] *But see Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir.2001)(finding that while "computer code, and computer programs constructed from code can merit First Amendment protection" as "speech," "content-neutral regulation with an incidental effect on a speech component" is allowed if the regulation "serve[s] a substantial governmental interest, . . . [is] unrelated to the suppression of free expression, and . . . [does] not burden substantially more speech than is necessary to further that interest").

[30] *See* Seth Litwack, *Bitcoin: Currency or Fool's Gold?: A Comparative Analysis of the Legal Classification of Bitcoin*, 29 Temp. Int'l & Comp. L.J. 309, 311 (Fall 2015)(asking if Bitcoin is a "currency, commodity, security, payment system, or something else entirely" and stating that "[t]he characterization of bitcoin has significant implications because it determines what laws and regulations will apply"); see also Andres Guadamuz and Chris Marsden, *Blockchains and Bitcoin: Regulatory responses to cryptocurrencies*, First Monday, Volume 20, Number 12 (7 December 2015), at http://ssrn.com/abstract=2704852 ("What is [virtual currencies'] legal status? Are they a currency? Are they a commodity? Are they a security?").

[31] *See* Anita Lavorgna, *Organised crime goes online: realities and challenges*, Journal of Money Laundering Control, Vol. 18 No. 2, pp. 153-168 (2015)(stating "[t]here is a broad consensus that the Internet has offered plenty of new possibilities for all types of criminals, including organised crime").

[32] *See generally* Alex Kozinski, *Essay: The Two Faces of Anonymity*, 43 Cap. U. L. Rev. 1, 10 - 15 (2015)

[33] Katie Rogers, *Anonymous Hackers Fight ISIS but Reactions Are Mixed*, New York Times (Nov. 25, 2015), available at http://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html?_r=0.

guilt from WWII, the German government has enlisted (or forced, as the case may be) social media providers like Google, Facebook, and Twitter to monitor and censor online expression on its behalf.[34] But the point is that, with some exceptions, it is not mainstream for regulators in Western governments (or at least in the U.S.) to ponder whether they should impose onerous requirements on internet sites where speech is exchanged. Not so where the exchange of money, or its virtual cousin, is concerned. Some predictions have been dire: according to Josh Strauss, Portfolio Manager of the Appleseed Fund, "Bitcoin allows for avoidance of all AML laws. . . There's no way governments are going to allow it."[35] According to the CEO of JP Morgan Chase, Jamie Dimon: "Virtual currency. . . that's going to be stopped. No government will ever support a virtual currency that goes around borders and doesn't have the same controls [as the U.S. dollar]. It's not going to happen."[36] The key in all this is that the risk of substantial regulation is far more real for virtual currency and blockchain than it was for the internet because one falls into the "finance" category while the other is "speech."

Realistically, it may be hard to avoid regulation – not that regulation would necessarily be a bad thing if done intelligently. One of the major difficulties in arguing against it is that the most famous manifestation of virtual currency/blockchain technology, Bitcoin, has a well-earned reputation problem, as it keeps making the news as a key accessory to crime and perhaps even terrorism. There are numerous examples. The best known is "Silk Road," the massive marketplace for illicit drugs operating on the "dark web" in which trades were facilitated by Bitcoin – thanks to its relative anonymity and transmissibility outside normal banking channels.[37] Its founder and operator, the Dread Pirate Roberts, was a Bitcoin aficionado, stating Bitcoin "will be looked back on as an epoch in the evolution of mankind" because of how it enabled individual control on the flow of money to be protected from the coercive power of the state.[38] Though the state soon thereafter captured and convicted Dread Pirate Roberts, a.k.a. Ross William Ulbricht,[39] as well as other cohorts in crime,[40] a newer iteration of Silk Road, Silk Road 3.0, lives on, as do other online illicit marketplaces using Bitcoin to enable illegal trades.[41] In fact, according to one scholar, most internet black markets currently in operation use virtual currencies.[42]

Besides the drug trade enabled by Bitcoin, "ransomware" extortion using Bitcoin as the payment method has become a recent trend, empowered by Bitcoin's potential for anonymity. The trend has become so extreme it has been characterized as a "ransomware

[34] *See, e.g.*, Anthony Faiola, *Germany springs to action over hate speech against migrants*, Washington Post (Jan. 6, 2016), available at https://www.washingtonpost.com/world/europe/germany-springs-to-action-over-hate-speech-against-migrants/2016/01/06/6031218e-b315-11e5-8abc-d09392edc612_story.html.

[35] David Z. Morris, *Does Western Union need to watch out for bitcoin?*, Fortune (Feb. 10, 2014), at http://fortune.com/2014/02/10/does-western-union-need-to-watch-out-for-bitcoin/.

[36] Stephen Gandel, *Jamie Dimon: Virtual Currency Will Be Stopped*, Fortune (Nov. 4, 2015), at http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/.

[37] *See, e.g.*, Andy Greenberg, *An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)*, Forbes (Aug. 14, 2013), at http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/#487bbe7365e7.

[38] *Id.*

[39] Sarah Jeong, *Jury Finds Ross Ulbricht Guilty of Running Silk Road Marketplace*, Forbes (Feb. 4, 2015), at http://www.forbes.com/sites/sarahjeong/2015/02/04/jury-finds-ross-ulbricht-guilty-of-running-silk-road-marketplace/#77da843175d2.

[40] *FBI arrest key Silk Road 'adviser' in Thailand*, BBC (Dec. 7, 2015), at http://www.bbc.com/news/technology-35025976.

[41] Joseph Cox, *Dark Web Drug Markets Are Desperately Clinging to the Silk Road Brand*, Motherboard (Oct. 22, 2015), at http://motherboard.vice.com/read/dark-web-drug-markets-are-desperately-clinging-to-the-silk-road-brand.

[42] Luther, *supra* n. 4, at 401.

nightmare."[43] The concept is simple: malware introduced into a network through phishing or other methods cryptographically locks all files on the network, rendering them inaccessible unless a virtual currency ransom is paid.[44] In one high-profile example, Los Angeles-based Presbyterian Medical Center paid $17,000 in Bitcoin in ransom to criminals in February 2016 to restore access to its computer systems rendered inoperable by a ransomware attack.[45] Another ransomware case involved the municipal computer systems of Plainfield, N.J., with the ransom again payable in Bitcoin.[46] While institutions (particularly hospitals)[47] and public authorities are often the victims,[48] non-institutional, individual internet users, such as Mac users,[49] online cheaters who used the now-defunct Ashley Madison website,[50] and visitors to major websites like the New York Times, the BBC, AOL and the NFL have also been attacked.[51] As evidence of the reach of the phenomenon, Lawyers Mutual, a major legal malpractice insurer in North Carolina, has issued an online malpractice alert about ransomware to the law firms it insures, under the clever title, "Put Your Hands in the Air and Give Me Your Bitcoin."[52] The ransomware "industry" has been estimated to generate $100 million a year in extortion profits,[53] facilitated in large measure by Bitcoin.[54]

Bitcoin has made the news for facilitating money laundering as well. For example, in January 2016 police in the Netherlands arrested 10 people for their alleged involvement in an international money laundering operation that relied on Bitcoin sales.[55] In July 2015, the

[43] Thomas Fox-Brewster, *As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin*, Forbes (Feb. 18, 2016), at http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#3880f17675b0.

[44] Department of Homeland Security, U.S. CERT, Alert (TA16-091A) Ransomware and Recent Variants (March 31, 2016).

[45] Danny Yadron, *Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers*, The Guardian (February 18, 2016), at http://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center.

[46] Matt Zapotosky and Ellen Nakashima, *These hackers can hold a town hostage. And they want ransom — paid in bitcoin*, The Washington Post (March 21, 2016), at https://www.washingtonpost.com/world/national-security/these-hackers-can-hold-a-town-hostage-and-they-want-ransom--paid-in-bitcoin/2016/03/18/1a2e2494-eba9-11e5-bc08-3e03a5b41910_story.html.

[47] *See, e.g.*, Niam Yaraghi, *A Health Hack Wake-Up Call*, U.S. News & World Report (April 1, 2016), at http://www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call; *U.S., Canada issue joint alert on 'ransomware' after hospital attacks*, The Telegraph (April 1, 2016), at http://www.telegraph.co.uk/technology/2016/04/01/picpub-us-canada-issue-joint-alert-on-ransomware-after-hospital/; Carolyn Y. Johnson and Matt Zapotosky, *Under pressure to digitize everything, hospitals are hackers' biggest new target*, Washington Post (April 1, 2016), at https://www.washingtonpost.com/news/wonk/wp/2016/04/01/under-pressure-to-digitize-everything-hospitals-are-hackers-biggest-new-target/.

[48] Annie Sneed, *The Most Vulnerable Ransomware Targets Are the Institutions We Rely On Most*, Scientific American (March 23, 2016), at http://www.scientificamerican.com/article/the-most-vulnerable-ransomware-targets-are-the-institutions-we-rely-on-most/.

[49] Andrea Peterson, *This devastating type of malware has basically ignored Mac users. Until now.*, The Washington Post (March 7, 2016), at https://www.washingtonpost.com/news/the-switch/wp/2016/03/07/this-devastating-type-of-malware-has-basically-ignored-mac-users-until-now/?tid=a_inl.

[50] http://krebsonsecurity.com/2015/08/extortionists-target-ashley-madison-users/

[51] Alex Hern, *Major sites including New York Times and BBC hit by 'ransomware' malvertising*, The Guardian (March 16, 2016), at http://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising.

[52] http://myemail.constantcontact.com/MALPRACTICE-ALERT--Beware-of-Ransomware.html?soid=1118263556714&aid=dDQFDjT06cI

[53] Johnson and Zapotosky, *supra* n. 47.

[54] *Cf.* U.S. CERT Alert (suggesting that payment in Bitcoin or other virtual currency is a common feature of ransomware attacks).

[55] *Ten arrested in Netherlands over bitcoin money-laundering allegations*, The Guardian (Jan. 20, 2016), at http://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy.

federal government brought money laundering related charges against two Florida men accused of running an illicit Bitcoin exchange called Coin.mx.[56] In January 2014, the vice chairman of the Bitcoin Foundation and former CEO of Bitcoin exchange BitInstant, Charlie Shrem, was charged with conspiracy to commit money laundering in connection with Silk Road-related activities.[57] Three men in New York state were recently charged (in March 2016) by the U.S. federal government with Bitcoin-related crimes, including money laundering and unlawfully operating an unlicensed money transmitting business.[58] The U.S. Attorney's Office for the Western District of New York, who brought the charges, recently summed up well the Bitcoin-as-criminal-tool narrative in its press release on the case:

> Bitcoin is not inherently illegal. However, its anonymity has popularized it as a payment form of choice in black markets for illegal goods and services. Virtual currencies such as Bitcoin have created a shadow banking system for criminals who use Internet-based black markets. Bitcoin has been a preferred method of payment for leading dark web markets such as Silk Road. In the same way that the Internet revolutionized consumer commerce (for lawful purposes), an anonymized global payment system on an anonymized global black market has paved the way for people to access with ease a world's array of contraband with the click of a button, rather than having to find and go to a drug dealer on a street corner.[59]

Across the Atlantic, Europol's head, Rob Wainwright, sounded the alarm on the use of virtual currencies for money laundering, indicating that law enforcement in the EU lacked sufficient investigatory powers to unmask criminals using virtual currencies to launder money relatively anonymously.[60]

Making matters worse are spectacular disasters like Mt. Gox exchange implosion, which introduce regulatory concerns beyond just AML/CFT. Tokyo-based Mt. Gox was the world's largest and best-known Bitcoin exchange until a massive meltdown forced it into bankruptcy.[61] Some 850,000 Bitcoins – worth over $450 million at the time and around $355 million in March 2016 – were stolen or "lost."[62] While the exact mechanisms underlying Mt. Gox's collapse are debated – including by those in revered position in the Bitcoin hierarchy, such as Cameron Winklevoss – some possible explanations include insider fraud, theft via hackers, technical vulnerabilities with the Bitcoin code called "transaction malleability," and/or mismanagement (such as accidentally making the Bitcoins inaccessible).[63] In August

[56] FBI New York Field Office, Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange (July 21, 2015), at https://www.fbi.gov/newyork/press-releases/2015/manhattan-u.s.-attorney-announces-charges-against-two-florida-men-for-operating-an-underground-bitcoin-exchange.

[57] Emily Flitter, *Prominent Bitcoin entrepreneur charged with money laundering*, Reuters (Jan. 27, 2014), at http://www.reuters.com/article/us-usa-bitcoin-arrests-idUSBREA0Q15N20140127.

[58] U.S. Department of Justice – U.S. Attorney's Office for the Western District of New York, *Three Men Indicted On District's First Bitcoin-Related Case* (March 11, 2016), at https://www.justice.gov/usao-wdny/pr/three-men-indicted-district-s-first-bitcoin-related-case.

[59] *Id.*

[60] Jim Urquhart, *Police need powers to tackle virtual money laundering: Europol*, Reuters (March 24, 2014), at http://uk.reuters.com/article/us-bitcoin-europol-money-laundering-idUKBREA2N1A420140324.

[61] *See, e.g.*, Nathaniel Popper and Rachel Adams, *Apparent Theft at Mt. Gox Shakes Bitcoin World*, New York Times (Feb. 25, 2014), at http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html?_r=0; Jonathan Soble, *Mark Karpeles, Chief of Bankrupt Bitcoin Exchange, Is Arrested in Tokyo*, New York Times (Aug. 1, 2015), at http://www.nytimes.com/2015/08/02/business/dealbook/mark-karpeles-mt-gox-bitcoin-arrested.html;

[62] *Id.*

[63] *What May Have Happened at Mt. Gox*, at https://winklevosscapital.com/what-may-have-happened-at-mt-gox/.

2015, Japanese authorities charged the former CEO of Mt. Gox, with embezzling several million dollars worth of Bitcoin from the exchange before its collapse, though the fate of the remainder is still a mystery.[64]

Because the missing Bitcoins belonged to customers who used Mt. Gox as a de facto "bank," Mt. Gox's failure represents a wake-up call that an unregulated Bitcoin financial ecosystem risks not only AML/CFT compliance goals but also consumer protection. In addition to Mt. Gox, the extraordinary volatility in Bitcoin's price and the risks that Bitcoin is a financial bubble give the distinct impression that Bitcoin is a sucker's game just begging for paternalistic government regulation to deliver people from their own foolishness. While this paper does not address financial regulation from a consumer protection angle, it is clear that such concerns cannot be ignored by regulators.

But more so than protecting naïve users against financial loss, the real driving force of regulatory action vis-à-vis virtual currency is fear: fear that virtual currency is particularly well-suited to empower bad actors because of its blend of quasi-anonymity, instant international transmissibility, and uncontrollability by centralized actors. The Financial Action Task Force (FATF), a key international force in AML/CFT efforts, articulates the schizophrenic nature of the current thinking on virtual currency and blockchain technology:

> two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.[65]

Some have associated Bitcoin with every evil imaginable.[66] While perhaps over-the-top if taken to the extreme, the potential dangers are hard to dismiss as mere alarmism, especially in the security climate following the November 2015 Paris terror attacks by ISIS/ISIL extremists[67] (and the ongoing danger of additional attacks, such as occurred in Belgium in March 2016). For example, in remarks provided days after the Paris attacks, Jennifer Shasky Calvery, Director of the Financial Crimes Enforcement Network (FinCEN), U.S. Department of the Treasury, acknowledged that there were reports that ISIS/ISIL had been "promoting

[64] *See* Alex Hern, *Mt Gox CEO charged with embezzling £1.7 million worth of bitcoin*, Business Insider UK (Sept. 14, 2015), at http://uk.businessinsider.com/mark-karpeles-mt-gox-ceo-charged-with-embezzling-17m-of-bitcoin-2015-9.

[65] FATF Report, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, p. 3 (June 2014), available at http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. *See also* Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 Ind. L.J. 441, 447 (Winter 2014)(stating "Bitcoin's image within the United States is polarized. Some view it as a tool used by criminals to commit crimes, whereas others view it as a tool for a legal system of currency that is free from unlawful government interference").

[66] *See* Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox*, 20 RICH. J.L. & TECH. 13, 2 (2014), who writes:

> Due primarily to their anonymity, virtual currencies have been linked to numerous types of crimes, including facilitating marketplaces for: assassins, attacks on businesses, the exploitation of children (including pornography), corporate espionage, counterfeit currencies, drugs, fake IDs and passports, high yield investment schemes (Ponzi schemes and other financial frauds), sexual exploitation, stolen credit cards and credit card numbers, and weapons.

[67] *See* Jonathan Chester, *How Questions About Terrorism Challenge Bitcoin Startups*, Forbes (Dec. 14, 2015), at http://www.forbes.com/sites/jonathanchester/2015/12/14/is-bitcoin-the-currency-of-terrorism/#4f41efb65e7c; Jasper Hamill, *ISIS owns small fortune in Bitcoin, claim Anonymous supporters - now Europe could ban virtual currency*, Mirror (Nov. 19, 2015), at http://www.mirror.co.uk/news/technology-science/technology/isis-owns-small-fortune-bitcoin-6860698.

the use of bitcoin and virtual currencies as a means of moving and raising funds," but denied that the CFT risks from virtual currency were greater than traditional methods of terrorist financing and money laundering.[68] On the other hand, Europol, the EU's law enforcement agency, has largely dismissed as unconfirmed third-party reports that ISIS/ISIL have used anonymous virtual currencies (particularly Bitcoin) to fund terrorist activities.[69]
Even so, Rand Corporation, the prominent U.S. national security think-tank, summarizes the debate in the following terms:

> The national security–policy implications of the rise of virtual-currency technology is the subject of much debate as of late. There has been a particular focus on the potential anonymity of VCs such as Bitcoin as well as the potential for terrorist or insurgent group usage in a manner resilient against efforts by local and global law enforcement, military, and intelligence organizations (including those of the United States) to survey.[70]

C. *The European Union Takes Notice*

In the European Union, the fear that virtual currencies can be used to anonymously facilitate the funding of terrorism or allow criminals to launder money has strengthened calls for regulation. An early source of alarm was the European Banking Authority (EBA), an independent EU Authority whose "objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector,"[71] which went so far as to warn consumers in December 2013 – in a perhaps not-so-veiled attempt at dissuading the use of virtual currencies entirely – that the possible use of virtual currencies for money laundering could prompt closure of exchange platforms, leaving consumers cut off from their virtual currency holdings.[72] The EBA released a comprehensive opinion on virtual currencies in July 2014, identifying numerous risks that they posed and recommending regulation, including that in the short-term "national supervisory authorities discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling VCs, thereby 'shielding' regulated financial services from VCs" and that virtual currency exchanges be deemed "obligated entities" required to comply with EU AML/CFT laws.[73]

The European Central Bank (ECB) has released reports on virtual currencies twice, once in October 2012[74] and again in February 2015.[75] Unlike the EBA, however, the ECB appears to be undecided about the need for regulation, concluding in its most recent report that virtual currencies pose risks but also could present advantages over existing payment systems.[76]

[68] Ian Mckendry, *ISIL May Be Using Bitcoin, Fincen's Calvery Says*, American Banker, Vol. 180, Issue 176 (11/17/2015).

[69] Europol, *Changes in modus operandi of Islamic State terrorist attacks*, p. 7 (The Hague, Jan. 18, 2016), available at https://www.europol.europa.eu/content/changes-modus-operandi-islamic-state-terrorist-attacks.

[70] Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz, RAND Corporation, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, p. ix (2015), *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf.

[71] EBA website, at http://www.eba.europa.eu/about-us;jsessionid=533E304F5947116C08E0B7A810CABD6B.

[72] EBA, *Warning to Consumers on Virtual Currencies*, EBA/WRG/2013/01, p. 3 (12 December 2013).

[73] EBA, *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08, p. 44 (4 July 2014).

[74] ECB, *Virtual Currency Schemes*, (October 2012), available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. As discussed below in footnote 205, this report included discussion of the virtual gaming currency Linden dollar in addition to Bitcoin.

[75] ECB, *Virtual Currency Schemes – A Further Analysis*, (February 2015), available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[76] *Id.* at 33.

In addition, the European Parliament's Committee on Economic and Monetary Affairs recently issued a February 23, 2016 draft report on virtual currencies[77] which is both balanced and insightful. Acknowledging the "transformational capacity" of what it calls "distributed ledger technology" or "DLT" (e.g., blockchain) in the context of virtual currencies and fintech (e.g. financial technology), the Committee's draft report discusses, on the one hand, the many potential benefits promised by DLT and the large-scale investments in DLT that have already been made (which it puts at over €1 billion), and on the other hand, and the risks that DLT-driven virtual currencies pose for of money laundering, terrorist financing,[78] and tax fraud.[79] As will be discussed later, the Committee recommended "smart" regulation, while stating explicitly that "[p]re-emptive and heavy-handed regulation that would stifle growth should and can be avoided."[80] The draft report took pains to make clear that smart regulation did not mean "light touch" regulation though, insisting that "rapid and forceful regulatory measures need to be part of the toolkit in order to address risks before they become systemic if and when appropriate."[81] But like the *bon mot* that there is "such a fine line between stupid and clever,"[82] the question whether this divide between smart regulation and either stifling overregulation or "light touch" regulation will be so clear in real life remains to be seen.

For its part, the European Commission has kept an open mind on virtual currencies so far, considering both the benefits of virtual currency and the need for regulation. For example, the Commission sponsored a one day "Blockchain and Digital Currencies Workshop" in Brussels in April 2015 which featured talks with titles like "Investment Opportunities in the Bitcoin Space," "Future of Cryptocurrencies and Blockchain Technology in the context of the Capital Markets," and "How banks in Europe are joining with cryptocurrencies" and asked questions like "Could blockchain become the underlying infrastructure of the future Capital Markets Union?".[83] On the other hand, in a press release on February 2, 2016 the Commission announced an "Action Plan to strengthen the fight against the financing of terrorism" in which it proposed amending the Fourth Anti-Money Laundering Directive (4th AMLD)[84] to require (among other things) that AML customer due diligence and "know your customer" rules apply to virtual currency exchange platforms.[85]

Fortunately, the Commission, like the European Parliament's Committee on Economic and Monetary Affairs and also, as discussed later, the Committee on the Internal Market and Consumer Protection, appears to recognize that the obvious disadvantage of overregulation of virtual currency and blockchain at an early stage in the technology's development is that a prodigy may be strangled in its crib. This would obviate any future danger, of course, though it would also kill the many benefits that would have been otherwise realized if the technology were allowed to mature. The Commission's language about its Action Plan suggests that it is largely taking a "wait-and-see" approach, with minimal

[77] 2016/2007(INI), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-575.277%2B01%2BDOC%2BPDF%2BV0%2F%2FEN.

[78] A risk that it states is not confirmed by law enforcement to have ever happened yet, citing Europol's report on the Islamic State cited above in footnote 69.

[79] *Id. at* p. 4-6.

[80] *Id.* at p. 8.

[81] *Id.* at p. 8-9.

[82] From the classic 1984 mockumentary "This is Spinal Tap."

[83] https://ec.europa.eu/digital-single-market/news/blockchain-and-digital-currencies-workshop.

[84] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

[85] http://europa.eu/rapid/press-release_IP-16-202_en.htm.

regulation as its starting point. In a Q&A-style "fact sheet"[86] released the same day as the Action Plan, the Commission characterized the dangers of virtual currency in somewhat equivocal terms, suggesting that it was not convinced the threat was significant enough to warrant extreme countermeasures. Phrases like "[t]here seems to be a risk" presented by virtual currency because it "may be used by terrorist organisations" (emphasis added) appear to signal agnosticism if not indecisiveness about whether the problem is even real. In addition, perhaps concerned that it would be criticized by opponents as irresponsible or ineffectual for not just making virtual currency illegal, the Commission preemptively defended itself in response to the self-generated question, "Why not just ban virtual currencies?" by citing their potential usefulness for international payments and remittances, the to-date relative insignificance of the size of the virtual currency market despite its innovative nature (e.g. 70,000 daily transactions at a total volume of €40 million), and the lack of bans in other jurisdictions, even those that have warned about their potential risks.[87]

Virtual currency and blockchain technology are unlikely to remain insignificant for much longer, though. They are rapidly evolving and are likely to be subject to exponential growth in the same way that the internet grew from thousands of users to millions to billions. Already Bitcoin has a March 2016 market capitalization in the $6 billion U.S. dollar range, up approximately 1,000 times its market capitalization of just five years ago in March 2011.[88] Bitcoin hit a peak market capitalization of almost $12 billion U.S. dollars in November 2013, with its notorious price volatility largely driving the peaks and valleys in recent years. Even despite this volatility, Bitcoin's market capitalization has not fallen below $2.3 billion U.S. dollars since October 2013.[89] Bitcoin's current market capitalization is hardly a small number or an insignificant increase in only half a decade.

To put things in perspective, though, the U.S. M1 money supply was in the $3 trillion range as of February 2016,[90] the Euro-area M1 money supply was around €6.67 trillion in January 2016,[91] and the value of all mined gold in the world is worth around $6.85 trillion in March 2016 prices (of $1,250 an ounce).[92] Bitcoin is currently small relative to financial giants, and is not in danger of replacing them any time soon. On the other hand, compared to existing payment remission services, Bitcoin has already arrived: its market capitalization now beats the market capitalization of Western Union, MoneyGram, and Euronet.[93] And compared to "minor" sovereign currencies, Bitcoin is already a "player": according to the Economist, Bitcoin's market capitalization exceeds that of all Paraguayan guaraníes in use.[94]

Once virtual currency and blockchain truly hit the bigtime, it is hard to envision that they will be regulated in the EU only as an afterthought. Instead, in regulating (or not

[86] European Commission - Fact Sheet, *Questions and Answers: Action Plan to strengthen the fight against terrorist financing*, available at http://europa.eu/rapid/press-release_MEMO-16-209_en.htm.

[87] *Id.*

[88] *See* chart at http://www.coindesk.com/data/bitcoin-market-capitalization/.

[89] *Id.*

[90] U.S. Federal Reserve Bank of St. Louis, Federal Reserve Economic Data, M1 Money Stock, available at https://research.stlouisfed.org/fred2/series/M1SL.

[91] European Central Bank, Statistical Data Warehouse, at http://sdw.ecb.europa.eu/reports.do?node=1000003478.

[92] *See* Warren Buffett, *Warren Buffett: Why stocks beat gold and bonds*, Fortune, (Feb. 9, 2012), available at http://fortune.com/2012/02/09/warren-buffett-why-stocks-beat-gold-and-bonds/, in which Warren Buffett estimated in 2012, at the then-current price of $1,750 per ounce, that the value of all mined gold in the world was worth $9.6 trillion.

[93] Rob Wile, *Bitcoin Can Be the New Western Union*, Business Insider (Dec. 5, 2013), at http://www.businessinsider.com/bitcoin-can-be-the-new-western-union-2013-12?IR=T.

[94] *The Magic of Mining*, The Economist (Jan. 10, 2015), at http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic.

regulating) virtual currency and blockchain, the EU will need to grapple with fundamental questions about liberty, security, efficiency, technological innovation, competition, and, increasingly, its own credibility and relevance in the eyes of its self-proclaimed citizenry.[95] The EU Parliament's Committee on Economic and Monetary Affairs has already begun that process, though it is hard to predict exactly where it will all end.

D. *Thesis Outline and Sources and Methodology*

The purpose of what follows is to consider the regulation of virtual currency and blockchain technology from an AML/CFT perspective in an EU law context, both where things are currently and where they are headed (or, rather, should be headed) in the future. This paper will consider blockchain technology in the context of virtual currency, but will not seek to address other, non-virtual currency applications for blockchain, such as smart contracts. Before looking at the two together, it will be necessary to address the basics: what is AML/CFT regulation, what is virtual currency (and what is blockchain technology), and what features do they have that impact AML/CFT regulations. Once these fundamentals have been laid out, the ensuing discussion turns to AML/CFT regulation of virtual currency/blockchain under EU law and argues that early regulation to channel the acceptable development of the technology in light of AML/CFT norms will be necessary to avoid later catastrophe – assuming that AML/CFT laws are not simply dispensed with in the virtual currency context.

A brief word on sources and methodology. Regarding sources, both primary legal sources, including case lase of the CJEU and materials from the Commission and other EU officials, as well as secondary sources, including law review articles, journal and periodical articles, articles from the business, financial, technology, and internet media, newspaper articles, and books, form the basis of the paper's discussion and conclusions. Because of the nature of the topic, some non-traditional sources, including even internet discussion forums and bloggers, are also cited where appropriate. With regard to method, this paper mainly follows the legal dogmatic method, along with an historical and comparative method, in order to describe the current state of AML/CFT regulation in the EU vis-à-vis virtual currency/blockchain. Because the historical, societal, and political-economical context of virtual currency and blockchain are inextricably intertwined with the development of the AML/CFT regulatory response, this context is detailed and described throughout, under the driving conviction that law cannot be understood as a sterile, closed system divorced from the wider world – especially when the law seeks to regulate an emergent, transformative technology that is less than a decade old and that may still be mostly unfamiliar to many readers.

Ultimately, this paper does not just describe what is but actively takes sides in the debate, as it identifies the problem that must be solved by any regulatory regime: unless virtual currency and blockchain development can be channeled to conform with AML/CFT norms, then one or the other will eventually be forced aside. Since both have an important role to play in the 21st century global economy, it is vital that any incompatibility between the two be addressed and solved decisively, before it is too late.[96]

[95] *See Schulz warnt vor „Implosion der EU,"* Frankfurter Allgemeine (April 11, 2016)(quoting President of European Parliament Martin Schulz as stating "Wir sind in Europa seit geraumer Zeit auf einer abschüssigen Bahn. Das Vertrauen vieler Menschen in Institutionen insgesamt, egal ob national oder europäisch, ist verloren gegangen," and fearing "the implosion of the EU"). *See also Många vill rösta om EU-medlemskap*, Svenska Dagbladet (May 9, 2016), at http://www.svd.se/manga-vill-rosta-om-eu-medlemskap/i/senaste.

[96] *See* Robert Stokes, *Virtual money laundering: the case of Bitcoin and the Linden dollar*, Information & Communications Technology Law, Vol. 21, No. 3, October 2012, 221–236, 232 ("if these virtual currencies

E. *Related Literature*

Before going further, it is worth noting that there has been an explosion of articles in recent years addressing the AML/CFT implications of virtual currencies and blockchain. Other papers that have tackled the general topic include an article by University of Texas law student Kavid Singh appearing in Northwestern Journal of Technology and Intellectual Property;[97] an article appearing in the online journal First Monday;[98] an article by Brooklyn Law School law student Nicholas Ajello appearing in Brooklyn Law Review;[99] an article appearing in the journal Information & Communications Technology Law written by Liverpool Law School senior lecturer Robert Stokes;[100] an article by Indiana University Maurer School of Law law student Danton Bryans appearing in Indiana Law Journal;[101] an article by Lawrence Trautman appearing in Richmond Journal of Law and Technology;[102] an article by Sheng Zhou, a law student at American University's Washington College of Law, which appeared in the Journal of Law and Cyber Warfare;[103] a master's dissertation for coursework at Utica College;[104] an article appearing in European Journal of Legal Studies by Sergii Shcherbak;[105] a working paper published by the SWIFT Institute;[106] an article by law student Michael Bombace at Washington and Lee University School of Law appearing in the Journal of Virtual Worlds Research;[107] an article appearing in the Journal of Money Laundering Control;[108] an article by law student Mitchell Hyman St. Thomas School of Law appearing in St. Thomas Law Review;[109] an article published by the North Carolina Banking Institute;[110] an article by Quinnipiac University School of Law law student Sarah Gruber

become more popular, the ability to launder criminal funds using Bitcoin. . . will increase accordingly. It would be preferable from an anti-money laundering perspective that pre-emptive attention is given to these facilities before their use becomes widespread")

[97] Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network,* 13 Nw.J. TECH. *&* INTELL. PROP. 37 (2015).

[98] Guadamuz and Marsden, *supra* n. 30.

[99] Nicholas J. Ajello, *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination,* 80 Brook. L. Rev. 435 (2014-2015).

[100] Stokes, *supra* n. 96.

[101] Bryans, *supra* n. 65.

[102] Trautman, *supra* n. 66.

[103] Sheng Zhou, *Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet*, 3 J.L. & Cyber Warfare 103 (2014).

[104] Berkley A. Pamplin, *Virtual Currencies and the Implications for U.S. Anti-Money Laundering Regulations,* Utica College dissertation (August 2014).

[105] Sergii Shcherbak, *How Should Bitcoin be Regulated*, European Journal of Legal Studies, 2014, Vol. 7, No. 1, pp. 45-91.

[106] Peggy Valcke, Niels Vandezande, Nathan Van de Velde, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4,* SWIFT Institute Working Paper No. 2015-001 (September 23, 2015).

[107] Michael Bombace, *Blazing Trails: A New Way Forward for Virtual Currencies and Money Laundering*, Journal of Virtual Worlds Research, Volume 6, Number 3 (July 2013).

[108] Angela S.M. Irwin Jill Slay Kim-Kwang Raymond Choo Lin Lui, *Money laundering and terrorism financing in virtual environments: a feasibility study*, Journal of Money Laundering Control, Vol. 17 Iss 1 pp. 50-75 (2014).

[109] Mitchell Hyman, *Bitcoin ATM: A Criminal's Laundromat for Cleaning Money*, St. Thomas Law Review, Vol. 27 Issue 2, p 287-308 (Summer 2015).

[110] Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws,* 18 N.C. Banking Inst. 529 (March 2014).

appearing in Quinnipiac Law Review;[111] an article in Yale Journal on Regulation;[112] an article in Washington Law Review;[113] an article in appearing in ECIS 2015 Proceedings at AIS Electronic Library (AISeL);[114]and others. Many of the above-cited papers address the question of AML/CFT regulation of virtual currencies under U.S. law, while a few look at the issue under EU law, including the articles by Stokes, Shcherbak, and Valcke *et al*. The implications of virtual currency and blockchain for EU AML/CFT regulation appear to be underexplored in the literature, however, and it is hoped that this paper will add to the scholarship on this highly-salient topic.

[111] Sarah Gruber, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion*, 32 Quinnipiac L. Rev. (2013).

[112] Sarah Jane Hughes and Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 Yale J. on Reg. 495 (Summer 2015).

[113] Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 Wash. L. Rev. 271 (August 2014).

[114] Christian Brenig, Rafael Accorsi, and Günter Müller, *Economic Analysis of Cryptocurrency Backed Money Laundering*, ECIS 2015 Completed Research Papers, Paper 20 (2015), at http://aisel.aisnet.org/ecis2015_cr/20.

II. AML/CFT Regulation in the EU

A. *Fundamentals*

The Fourth Anti-Money Laundering Directive (4th AMLD), the most current AML/CFT legislation in the EU and the one that virtual currencies should be compared against, was adopted May 20, 2015 and has a transposition deadline of June 26, 2017 for the Members States. Its avowed purpose is to prevent the EU's financial system from being used to launder money or finance terrorism.[115] Under the Directive, Member States must prohibit "money laundering" and "terrorist financing," as specifically defined.[116] They must do so primarily by requiring trusted intermediaries, called "obligated entities," to follow a number of customer due diligence and other monitoring and reporting requirements when carrying out financial transactions on behalf of clients, some of which will be discussed in more detail below. The Directive sets minimum AML/CFT standards that Member States must adopt, and Member States are free to enact stricter rules than those set forth.[117]

First, the definition of money laundering. According to Article 1(3) of the Directive, money laundering consists of any of the following intentional acts:

> (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
>
> (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
>
> (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
>
> (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Two words or phrases in the definition of "money laundering" are themselves defined elsewhere in the Directive and should be highlighted. The first, "criminal activity," is of particular importance, since funds must be derived from "criminal activity" (or from participation in "criminal activity") to trigger any of the definitions of "money laundering." The Directive defines "criminal activity" as "any kind of criminal involvement" in various terrorism offenses, illegal drug manufacturing and trafficking offenses, organized crime, serious fraud affecting the EU's financial interests, corruption, and all other offenses (including tax crimes) punishable by a maximum prison sentence of more than one year (or a minimum of more than six months in Member States having minimum sentences).[118] This definition means that most serious crimes are covered by the Directive, including financing derived from terrorism (such as kidnapping and ransom). In addition, an actor's role in any

[115] Article 1(1).

[116] Article 1(2).

[117] Article 5.

[118] Article 3(4).

particular criminal offense need not be central to qualify as "criminal activity," since "any kind of criminal involvement" will suffice. Coupled with subsection (d) of Article 1(3), discussed below, the effect is to cast the net widely as to when funds become tainted. There is furthermore extraterritorial reach: under Article 1(4), the activities which created the property being laundered may occur in another Member State or in a third country for "money laundering" to take place.

The second word in the definition of "money laundering" that is defined elsewhere is "property." "Property" is defined as: "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets."[119] Property therefore is either an "asset" (in the broadest possible sense) or it is a "legal document" or an "instrument" (in any form) evidencing title to or an interest in an "asset." The key, though, is that "property" depends on there being an underlying "asset." "Asset" is itself not further defined by the Directive, but the words "of any kind" coupled with the clause "whether corporeal or incorporeal, movable or immovable, tangible or intangible" suggests the intention to cover anything that might have or embody value, regardless of form or legal character. As will be discussed later in this paper, this broad definition of "property" should include virtual currencies.

Several points about the definition of "money laundering" stand out. First, one might normally assume that "concealment" and/or "disguise" are necessary elements of the offense of money laundering, since "laundering" (e.g. cleaning dirty money) implies an effort to hide the illicit origin of the involved funds or to distance the funds from the underlying criminal activity or the criminals that generated them. While true under subsections (a) and (b), this assumption, however, is incorrect under subsection (c): merely knowingly possessing or using criminally-derived funds (or other property) is "money laundering," even if done without concealment or disguise. The definition, therefore, is broad enough to cover all funds known to be "dirty," without also requiring any steps be taken to "clean" the funds. Which only makes sense, since it would hardly be a workable AML system if transacting with criminally-derived funds were permitted if done openly.

In addition, under all subsections the funds in question must be "dirty" from the outset: they must be "derived from criminal activity" or from "an act of participation in criminal activity." Literally, then, under the Directive it is not "money laundering" to take "clean" funds – money generated by legal activities – and divert them to fund criminal activity. Whether this is a deliberate policy choice is unclear from the text.

Further, indirect or vicarious involvement in money laundering qualifies as money laundering. Under subsection (d), various ways of assisting others in committing the offense also constitute money laundering. This includes, at one end of the spectrum, more "hands-on" involvement such as participation in and association to commit the offense, while at the other end of the spectrum offering advice as to how to commit money laundering counts the same as direct participation. While much of subsection (d) makes logical sense, there are some harsh consequences if the definition is tested: for instance, it would literally be money laundering to counsel one's innocent client who is selling his home to accept the buyer's funds if it were known that they derived from participation in criminal activity.

In addition to defining "money laundering," the Directive defines "terrorist financing." This definition appears straightforward: "the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out" any of the various terrorism

[119] Article 3(3).

offenses defined in Articles 1 to 4 of Council Framework Decision 2002/475/JHA.[120] Interestingly, however, the definition employs the term "funds" (not explicitly defined elsewhere in the Directive) rather than the broader, defined term "property," which as discussed above encompasses anything having value (e.g. an "asset" or the right to an "asset"). The question is what is meant by "funds." While "funds" is not expressly defined in the 4th AMLD, other related EU legislation does define the term, including Regulation (EU) 2015/847 of the European Parliament and of the Council,[121] the Funds Transfer Regulation. The definition of funds in Regulation (EU) 2015/847 refers though to yet another definition elsewhere: "'funds' means funds as defined in point (15) of Article 4 of Directive 2007/64/EC."[122] A look at that Directive, commonly called the Payment Services Directive,[123] gets us closer to a final definition of funds: "'funds' means banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC." The final piece in the definition of funds is the definition of "electronic money" from Directive 2000/46/EC[124]: "monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer."

There is some evidence in the 4th AMLD itself that this definition of "funds" is the one intended: the Directive employs the phrase "transfer of funds" in Article 11(b)(2), which it defines by reference to "point (9) of Article 3 of Regulation (EU) 2015/847," the Funds Transfer Regulation. Because the definition of "transfer of funds" in the Funds Transfer Regulation necessarily requires reference to the defined term "funds" (which is defined immediately before "transfer of funds" in the Regulation), the definition of "funds" arguably finds its way through this circuitous route into the Directive.

The use of "funds" rather than "property" in the definition of "terrorist financing" is potentially problematic, both generally and in reference specifically to virtual currencies. That is because unless an asset is physical cash or coins, monetary balances in a bank account (e.g. scriptural money), or electronic money (as narrowly defined), then it may not be not "funds." According to the ECB, virtual currency is not "electronic money" because it is not "issued on receipt of funds of an amount not less in value than the monetary value issued."[125] Virtual currency is also not "banknotes and coins" and is not "scriptural money." Virtual currency may therefore not be "funds," and if not it would literally not be "terrorist financing" under the 4th AMLD for a party to donate Bitcoin to ISIS/ISIL. Then again, it would also not be "terrorist financing" under the Directive for to donate 1 million shares of Apple stock to ISIS/ISIL, since stock shares would not be "funds" either. This is unless, of course, "funds" can be interpreted differently, which, as shown in Chapter III, it could be.

Turning aside from this potentially problematic definition of "terrorist financing," many have noted that money laundering and terrorist financing are mirror opposites of sorts: in the former, dirty money is made clean, and in the latter, (often) clean money is diverted for nefarious purposes. The common element though is that the free flow of money represents a threat, not only because serious crime and terrorism are themselves evils but because of the

[120] Article 1(5).

[121] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

[122] Article 3(8).

[123] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

[124] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.

[125] ECB, *Virtual Currency Schemes*, p. 43 (2012).

subversive danger posed to the mechanisms of capitalism supporting the cornerstone of the EU, the internal market. As the 4th AMLD states in the recitals:

> Flows of illicit money can damage the integrity, stability and reputation of the financial sector, and threaten the internal market of the Union as well as international development. . . The soundness, integrity and stability of credit institutions and financial institutions, and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates to disguise the origin of criminal proceeds or to channel lawful or illicit money for terrorist purposes.[126]

This threat justifies requiring trusted intermediaries, known as "obligated entities," to act as unpaid agents of the state to safeguard the flow of funds, something of a capitalist equivalent to the Cuban Comités de Defensa de la Revolución[127] tasked with discovering and reporting subversive threats to socialist revolutionary order. These obligated entities run the gamut of financial, business, legal, and professional actors: credit institutions, financial institutions, auditors, accountants, tax advisors, notaries or other legal professionals acting in a transactional capacity, trust and company service providers, estate agents, merchants receiving large cash payments, and gambling providers all full under the "obligated entities" definition.[128] Member States can exempt small actors with low money laundering risk and small transactions from the Directive if appropriate from a risk assessment perspective.[129] Conversely, Member States must add to the list of obligated entities whenever the evidence under the risk-based approach that Member States must adopt suggests doing so is warranted.[130]

Obligated entities bear the brunt of the AML/CFT fight. The Directive requires Member States to make obligated entities undertake AML/CFT risk assessments tailored to the customers and geographic regions they serve and products and services they offer, subject to review by regulatory authorities.[131] Obligated entities must also implement appropriate AML/CFT risk mitigation "policies, controls and procedures" approved by senior corporate management, which include numerous customer due diligence, reporting, record-keeping, employee screening, internal control, and compliance management components, subject when appropriate to independent audit.[132]

But more so than conducting risk assessments and having appropriate policies, controls, and procedures in place, obligated entities must undertake various "customer due diligence" measures in a variety of circumstances: at the start of every new business relationship; when conducting any transaction equaling or exceeding €15,000 in one or more linked steps; when transferring funds (as defined by the Funds Transfer Regulation) in excess of €1,000; if the obligated entity is a person trading in goods, when conducting transactions in goods for cash payments of €10,000 or more in one or more linked steps; if the obligated entity is a gambling services provider, when gamblers equal or exceed €2,000 or more in wagers, winnings, or transactions in one or more linked steps; whenever "there is a suspicion" of money laundering or terrorist financing; and whenever "there are doubts about the veracity or adequacy" of a customer's identification data.[133] Under any of the above circumstances, obligated entities must: identify the customer and confirm the customer's

[126] Recitals 1 and 2.

[127] http://www.pcc.cu/opm_cdr.php

[128] Article 2(1).

[129] Article 2(3) – 2(9).

[130] Article 4(1).

[131] Article 8(1) and 8(2).

[132] Article 8(3) – 8(5).

[133] Article 11.

identity from reliable documents or sources; if applicable, identify the beneficial owner and confirm the beneficial owner's identity, and in the case of legal entities such as companies, foundations, and trusts, understand who owns and controls the entity; understand the business relationship, including what it seeks to achieve and why it exists; monitor and scrutinize the business relationship on an ongoing basis to confirm that the transactions make sense in the context of the business relationship's purported nature and purpose (and that the source of funds remains consistent with the customer's known profile) while confirming that documentation remains complete and accurate; and confirming that persons claiming to be authorized to act on behalf of a person or entity are in fact authorized to do so and are otherwise who they claim to be.[134]

As the above indicates, there are several key elements to customer due diligence. The first is knowing the customer and any beneficial owner of customer that is a legal entity. There is good reason for this requirement, as AML/CFT measures cannot work if suspicious transactions cannot be traced back to the real people who carried them out because otherwise money launderers and terrorist financers would simply hide behind fake names and disappear if scrutinized. As an important adjunct, the Directive outlaws anonymous accounts or anonymous passbooks at credit and financial institutions, while requiring the Member States to "prevent misuse" of bearer shares and bearer share warrants,[135] both of which are designed to eliminate the problem of customers or beneficial owners being able to transact unidentified.

The second key element of customer due diligence, understanding and monitoring the business relationship, involves making sure that transactions taking place are consistent with the sorts of transactions that should be taking place, given the overall business context. Transaction patterns cannot be properly scrutinized without this context, since what may raise a red flag in one circumstance may be perfectly normal in another. Customer and beneficial owner identification requirements are important here as well, as it is not possible to understand and monitor business relationships accurately if the persons involved are unknown or unverified. In addition, understanding the business relationship allows obligated entities to conduct proper risk assessments, which are themselves critical to proper customer due diligence. Obligated entities may customize how the customer due diligence measures are applied on a risk-appropriate basis,[136] but must also be able to justify their choices to the appropriate authorities or self-regulated bodies.[137] On the one hand, obligated entities can determine that a particular relationship represents a lower AML/CFT risk, permitting simplified customer due diligence.[138] Conversely, anything out of the ordinary – "all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose" – should invite particular scrutiny,[139] a requirement that cannot work if obligated entities have no baseline normal from which to compare.

In addition, enhanced customer due diligence measures are required under certain specified circumstances. One is when obligated entities transact with persons or entities in "high-risk third countries," or otherwise when they transact in cases identified as "higher risk" by the risk assessments carried out by obligated entities or Member States.[140] Another is when transacting with so-called "politically exposed persons" – certain enumerated high-

[134] Article 13(1).
[135] Article 10.
[136] Article 13(2).
[137] Article 13(4).
[138] Article 15.
[139] Article 18(2).
[140] Article 18(1).

ranking governmental or quasi-governmental officials such as members of parliament, heads of state, supreme court justices, ambassadors, military leaders, leaders of state-run enterprises, directors of international organizations, central bankers, and political party heads[141] – and their family members and close associates.[142] The rationale for enhanced customer due diligence surrounding political exposed persons is that that they are at an increased risk of corruption, simply by virtue of their high position;[143] the Directive emphasizes though that politically exposed persons should not, by virtue of being designated as such, be stigmatized as involved in criminal activity or otherwise ostracized.[144] The overall idea though is whenever the risks of a particular customer or situation are higher than normal, then it is appropriate to align regulatory requirements with the increased risk, and vice versa.

Besides obligated entities, the other major players in the AML/CFT regime laid out in the Directive are "FIUs" – Financial Intelligence Units. FIUs are "operationally independent and autonomous" agencies at the Member State-level designed to collect and analyze information and intelligence about suspicious transactions and disseminate their analysis to the "competent authorities" empowered to enforce criminal laws against money laundering and terrorist financing.[145] FIUs must have proper authority and adequate resources to carry out their mission, and must be allowed to act as they consider appropriate, free from interference from other agencies.[146] FIUs are the investigative backbone of the AML/CFT effort but do not necessarily play a direct law enforcement role. Instead, FIUs compile operational information and intelligence for use by the "competent authorities" who ultimately arrest and prosecute suspected money launderers or terrorist financers.

A primary source of FIUs' intelligence is obligated entities, who are required by the Directive to inform on their customers. Under the Directive, obligated entities must to report all suspicious transactions (and attempted suspicious transactions) to the FIU in their Member State and provide all additional necessary information requested by the FIU.[147] They must file a suspicious transaction report to the FIU if they have at least "reasonable grounds to suspect" that the involved "funds" result from criminal activity or are related to terrorist financing.[148] In certain circumstances, particularly where otherwise legally-privileged information is obtained by particular types of obligated entities – e.g., auditors, external accountants, tax advisors, notaries, other independent legal professionals, and estate agents – the Member State may require the obligated entity to report the information first to the relevant profession's self-regulatory body (i.e. the bar association), which in turn is required to forward the report verbatim to the FIU[149] – a roundabout reporting scheme that amounts to little more than window dressing. If an obligated entity has more than just "reasonable grounds to suspect" a pending transaction is problematic from an AML/CFT standpoint – i.e. it knows or suspects the transaction involves criminal proceeds or terrorist financing – then it must first report to the FIU and then wait to carry out the transaction unless and until it receives particular instructions on what to do from the FIU, a requirement that does not apply if waiting would not be possible or would thwart investigative efforts.[150] An obligated entity

[141] Article 3(9).
[142] Articles 18, 20-23.
[143] Recital 32.
[144] Recital 33.
[145] Recital 37; Article 32.
[146] Article 32.
[147] Article 33.
[148] Article 33(1)(a). Whether there is any requirement to file a suspicious transaction report regarding transactions involving items that are not funds – such as (arguably) virtual currencies – is unclear from the text.
[149] Article 34.
[150] Article 35.

that reports a suspicious transaction to an FIU may not inform the customer or third parties that a suspicious transaction report is pending has been made, for obvious reasons.[151] Obligated entities have immunity from liability for suspicious transaction reports made in good faith,[152] while the involved individuals filing suspicious transaction reports are to be protected under Member State law from threats or a hostile workplace environment, particularly those originating from displeased employers.[153] Obligated entities who fail to report suspicious transactions or otherwise fail in their AML/CFT duties risk being reported to the FIU by competent authorities empowered to perform periodic monitoring and compliance checks.[154]

Besides reporting suspicious transactions to FIUs, obligated entities must maintain customer due diligence and transaction records for an extended period of time so that they are available for review by FIUs if a customer or transaction later comes under scrutiny. Obligated entities must keep customer due diligence documents and transaction records for a period of five years measured from the end of the business relationship with a customer or from the date of the customer's last transaction.[155] Member States may require obligated entities to maintain these documents and records for an additional five years, if deemed justified.[156] Obligated entities may not misuse the personal data collected for commercial purposes.[157] Obligated entities must also have in place secure systems allowing them to respond promptly, fully, and confidentially to FIU inquiries about business relationships maintained within the past five years.

Obligated entities have yet further demands placed on them by the Directive. For example, obligated entities that are part of a corporate group must implement group-wide policies and procedures pertaining to AML/CFT, including data protection and information sharing policies and procedures.[158] Obligated entities located in more than one Member State must respect the national provisions of the Directive in the Member States in which they are located.[159] Obligated entities with locations in a third country must follow the AML/CFT laws of their home Member State if the third country's laws are less strict, and must implement the AML/CFT policies and procedures required by their home Member State.[160] If this is not possible, then the obligated entity must so inform the competent authorities in their home Member State, which may in turn forbid the obligate entity from carrying out operations in the third country.[161] Obligated entities must also conduct appropriate AML/CFT employee training, maintain up-to-date information on money laundering and terrorist financing trends, and identify a member of management who is officially responsible for AML/CFT compliance.[162]

Currency exchange and check cashing operations are pinpointed for additional regulation, as are trust or company service providers and gambling service providers. They must be licensed or registered, and their managers or owners must be "fit and proper persons."[163] The Directive also requires that criminals not be allowed into management or

[151] Article 39.
[152] Article 37.
[153] Article 38.
[154] Articles 36, 48.
[155] Article 40(1).
[156] *Id.*
[157] Article 41.
[158] Article 45(1).
[159] Article 45(2).
[160] Article 45(3).
[161] Article 45(5).
[162] Article 46.
[163] Article 47.

ownership positions in obligated entities falling within the following categories: auditors, external accountants, tax advisors, notaries, other independent legal professionals, and estate agents.[164]

The requirements placed on obligated entities by the Directive are not mere moral imperatives. Failure to comply can result in sanctions, some serious. Under the Directive, Member States are to institute sanctions and measures against obligated entities that are "effective, proportionate and dissuasive."[165] It is up to the Member States to determine if those sanctions and measures are criminal or administrative in nature, or both.[166] Those sanctions and measures should reach members of an obligated entity's management as well as the actual individuals responsible for breaking the rules.[167] In addition, breaches by obligated entities of the main requirements imposed on them – those involving customer due diligence, reporting suspicious transactions, record-keeping, or internal controls – that are "serious, repeated, systematic, or a combination thereof" may result in particularly strong sanctions.[168] In such a situation, an obligated entity may face sanctions ranging from the mild and mostly symbolic, such as a public dressing down or a cease and desist order, to those that are not child's play, such as suspension of an obligated entity's authorization, a ban on particular managers in the obligated entity from acting as managers in obligated entities, and monetary penalties of at least double the benefit obtained by the obligated entity from the breach or at least €1 million.[169] Credit or financial institutions can face even worse: fines of at least €5 million or 10% of annual turnover (measured on a consolidated basis) in the case of entities, and sanctions of at least €5 million (!) in the case of natural persons.[170] Member States are free to impose additional sanctions or to increase the monetary amounts of the sanctions allowed.[171]

Besides obligated entities and FIUs, corporations and other legal entities have responsibilities under the Directive. The Directive requires these actors to maintain information on their beneficial owners and to make that information available in a central register kept in each Member State.[172] Member States must make this information available to FIUs and competent authorities on an unrestricted basis, to obligated entities for AML/CFT purposes, and to anyone else with a "legitimate interest,"[173] subject in the case of the latter to the possibility of limited exceptions against access in extraordinary circumstances (such as where the information could be useful to a potential kidnapper or other person with sinister intentions[174]). In addition, trustees of an express trust face similar information requirements regarding the identities of beneficial owners.[175]

As should stand out from the above abridged outline of the 4th AMLD, the AML/CFT system as currently envisioned cannot work without trusted intermediaries who control access to the channels of money transmission and storage. These trusted intermediaries serve many vital roles: gatekeepers, informants and sources of operational intelligence, archivists of transactions (and perhaps even scapegoats if things go wrong). Besides intermediaries, the other prerequisite of the AML/CFT system is transparency of the true identities of all

[164] Article 47(3).
[165] Article 58.
[166] *Id.*
[167] *Id.*
[168] Article 59.
[169] Article 59(2).
[170] Article 59(3).
[171] Article 59(4).
[172] Article 30.
[173] Article 30(5).
[174] Article 30(9).
[175] Article 31.

participants, including the identities of the real persons operating through corporations or other legal entities. Anonymity is anathema to the system because it thwarts traceability, and without traceability the system could not catch money launderers or terrorist financers, which is its ultimate purpose.

As will be discussed below, these two basic assumptions of the current AML/CFT regime create a huge problem in the context of virtual currencies (e.g. Bitcoin) because anonymity (or something approaching it) and lack of intermediaries (except when exchanging "real" money for virtual currencies and vice versa) are key features of Bitcoin as well as other similar virtual currencies.

B. EU Anti-Money Laundering Law in an International Context

Before going any further, it is worth emphasizing the wider context of the EU AML/CFT system. It is not an EU invention by any stretch of the imagination. Rather, it is the result of international efforts, largely spurred by the Financial Action Task Force (FATF), but with origins in the U.S. Any changes to the AML/CFT system to accommodate virtual currencies – or vice versa – will have to take this wider context into account, since without international harmonization and coordination the only safe prediction is failure.

The genesis of the current international AML regime is typically traced to the United States, and particularly the U.S. war on drugs.[176] Domestic efforts came first: the U.S.'s legal armamentarium against money laundering in the 1980s, before the internationalization of AML laws, included the Currency and Foreign Transactions Reporting Act of 1970 (a.k.a. the Bank Secrecy Act (BSA)), the Comprehensive Crime Control Act of 1984 (and derivatively, the versatile Racketeer Influenced and Corrupt Organizations (RICO) Act), the Money Laundering Control Act of 1986, and the Anti-Drug Abuse Act of 1988.[177]

Called the "cornerstone" of U.S. AML laws, the BSA[178] enabled the placing of record-keeping and reporting requirements on banks and other financial institutions.[179] These included requiring financial institutions to keep records of their customers' identities, to maintain copies of checks and other financial instruments, and to report currency transactions exceeding $10,000 to the Internal Revenue Service (IRS).[180] In addition, the BSA required persons sending or receiving currency or monetary instruments in excess of $10,000 in the aggregate across U.S. borders to report doing so to U.S. Customs.[181] The U.S. Supreme Court upheld the constitutionality of the BSA in a 1974 case, *California Bankers Association v. Shultz*,[182] allowing the law in the face of unreasonable search and seizure, self-incrimination, and freedom of speech and freedom of association concerns.

Once the 1980s came about and the war on drugs began in earnest, there were several important additions to U.S. AML laws. The Comprehensive Crime Control Act of 1984[183] added the famed RICO Act to the government's AML arsenal, making money laundering a

[176] *See, e.g.,* Annegret Flohr, *Self-Regulation and Legalization: Making Global Rules for Banks and Corporations*, p. 98, 114 (2014); Emmanuel Ioannides, *Fundamental Principles of EU Law Against Money Laundering*, p. 12 – 14 (2014).

[177] Michael J. Anderson and Tracey A. Anderson, *Anti-money laundering: history and current developments*, J.I.B.L.R. 2015, 30(10), 521-531, 523-524 (listing U.S. anti-money laundering laws).

[178] 31 U.S.C. 5311 *et seq*.

[179] Matthew S. Morgan, *Money Laundering: The American Law and its Global Influence*, 3-SUM NAFTA: L. & Bus. Rev. Am. 24, 26-27 (Summer 1997); *id*.

[180] *California Bankers Ass'n v. Shultz*, 416 U.S. 21, 94 S.Ct. 1494, 39 L.Ed.2d 812 (April 1, 1974).

[181] *Morgan*, *supra* n. 179, at 26-27.

[182] 416 U.S. 21.

[183] Pub.L. 98–473, S. 1762, 98 Stat. 1976, enacted October 12, 1984.

predicate act for RICO criminal and civil liability purposes.[184] The Money Laundering Control Act of 1986, meanwhile, made money laundering directly illegal under federal law for the first time, making it a federal crime to knowingly conduct or attempt to conduct a monetary transaction involving criminal proceeds with the knowledge that the transaction was designed to conceal or disguise one or more aspects of the proceeds or avoid state or federal transaction reporting requirements.[185] The Act also made it illegal to transport funds or monetary instruments across U.S. borders with the intent to promote illegal activity or with the knowledge that the transportation was designed to conceal or disguise one or more aspects of the proceeds or avoid state or federal transaction reporting requirements.[186] In addition, the Act made it illegal to structure transactions to avoid the reporting requirements of the BSA (e.g., by splitting a transaction exceeding $10,000 into multiple smaller transactions falling under the $10,000 reporting threshold).[187] Serious fines and prison time awaited law breakers, and financial institutions were burdened with additional internal compliance requirements.[188] Finally, the Anti-Drug Abuse Act of 1988 increased the coverage of the AML laws, requiring additional actors to act as gatekeepers and lowering the threshold for transaction reporting.[189]

The U.S., as should be apparent, went from basic, almost primordial, AML laws to fairly strict requirements in a relatively short period of time in an effort to stem the flow of drug money. Yet the drug problem became worse, and "crack" cocaine became an epidemic – and one that, undoubtedly due to the race aspects involved, caused some to demand extreme countermeasures.[190] Like, for instance, the U.S. Congressman from South Carolina, Arthur Ravenel, who suggested in 1988: "We ought to shoot down every drug-bearing plane and machine-gun the survivors. Think of the long trials we would save."[191]

At this point the story takes an international turn. In 1989, the G7 created the FATF, a now 37-member organization comprised of a "who's-who" of countries and regional organizations, to coordinate the international anti-money laundering effort.[192] The FATF's job at its inception was to define the money laundering problem (which was still primarily associated with drug trafficking), determine what had already been done to fight it, and, most importantly, figure out what remained to be done.[193] The result was the FATF's "Forty Recommendations" released in 1990. October 2001 saw the release of the "Eight Special Recommendations" aimed at terrorist financing. AML/CFT regulation was thus born, an amalgam one commentator has called a "forced marriage" that resulted from a "hasty

[184] Anderson and Anderson, *supra* n. 177, at 523.

[185] Charles Plombeck, *Confidentiality and Disclosure: The Money Laundering Control Act of 1986 and Banking Secrecy*, International Lawyer (ABA) 22 Int'l L. 69, 71-72 (1988); 18 U.S.C. § 1956(a)(1).

[186] Plombeck, *supra* n. 185, at 76; 18 U.S.C. § 1956(a)(2).

[187] Anderson and Anderson, *supra* n. 177, at 523-524; 31 U.S.C. § 5324.

[188] *Id.* at 524.

[189] *Id.*

[190] Andrew Cohen, *How White Users Made Heroin a Public-Health Problem*, The Atlantic (Aug. 12, 2015)(stating that "the harsh, punitive reaction to the crack era was the result of mythology about its use, and its users, that later turned out to be false"), at http://www.theatlantic.com/politics/archive/2015/08/crack-heroin-and-race/401015/.

[191] Sandy Grady, *Macho Congressmen: Drugbusters Inc.*, Philadelphia Daily News (June 20, 1988), at http://articles.orlandosentinel.com/1988-06-20/news/0050050021_1_carlucci-drug-defense.

[192] Eleni Tsingou, "Money Laundering," in Daniel Mügge, *Europe and the Governance of Global Finance*, p. 143 (2014); *see also* FATF: FATF Members and Observers, at http://www.fatf-gafi.org/about/membersandobservers/.

[193] FATF: History of the FATF, at http://www.fatf-gafi.org/about/historyofthefatf/ The discussion that follows draws from the facts listed in this resource.

reaction" to the 9/11 terrorist attacks.[194] Regardless of the alleged incompatibility of AML and CFT regulation, FATF revised its standards in 2003, and released its "40 + 9 Recommendations" in 2004 geared towards both anti-money laundering and counter financing of terrorism. FATF revised its standards once again in 2012.[195]

FATF's current objectives may have evolved from 1989, but standard setting and promoting international AML/CFT laws, regulations, and measures remain core to its work.[196] In carrying out its mandate, FATF must remain on top of developments impacting money laundering and terrorist financing and develop new AML/CFT standards accordingly.[197] In turn, FATF's 37 members have agreed to support and adopt FATF's recommendations and to follow FATF's official guidance.[198] The European Commission is a FATF member, as are 15 EU Member States in their own right.[199] The 2012 FATF standards are in fact an important source for the EU's 4th AMLD.[200] The relevance to virtual currencies should be apparent. Namely, any AML/CFT solution to virtual currencies in the EU will need to be coordinated with what FATF does in the area and harmonized with international AML/CFT efforts. This is not only because the European Commission and 15 Member States are committed to following FATF's lead but also because otherwise any EU "solution" could be undermined by conflicting AML/CFT regulation in other jurisdictions. Importantly, FATF has released two documents, *Guidance for a Risk-Based Approach to Virtual Currencies*[201] in June 2015 and *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* in June 2014 that should be taken into account in an EU law context. These documents are considered later in Chapter IV.

But before considering virtual currencies in an AML/CFT regulatory context, it is time to answer some basic questions: what are virtual currencies and what features do they have that make AML/CFT regulation more challenging.

[194] Gauri Sinha, *AML-CTF: a forced marriage post 9/11 and its effect on financial institutions*, Journal of Money Laundering Control Vol. 16 No. 2 (2013).

[195] Available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

[196] FATF, *Financial Action Task Force Mandate (2012-2020)*, p. 2 (April 20, 2012), at http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf.

[197] *See id.*

[198] *See id.*, p. 3.

[199] *See* FATF: FATF Members and Observers, at http://www.fatf-gafi.org/about/membersandobservers/.

[200] Recital 4. *See also* Tsingou, n. 192, at 144 ("FATF recommendations are not formally binding but are widely adopted by members and form the basis of the European Commission's money laundering directives"). Others have suggested, somewhat simplistically, that "[t]he enactment of AML legislation commences with the FATF developing and setting international standards. Then the Union adopts and complements these standards." Janös Boszörmenyi and Erich Schweighofer, *A review of tools to comply with the Fourth EU anti-money laundering directive*, International Review of Law, Computers & Technology, Vol. 29, No. 1, 63– 77, at 63 (2015).

[201] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

III. Virtual Currency and Blockchain: A Factual and Legal Primer

A. *Basic Concepts*

First, a delimitation of the subject matter. Excluded from consideration are virtual gaming currencies used as a medium of exchange within role-playing video games like the Linden dollar of Second Life or World of Warcraft Gold but that have real-world exchange potential. Virtual gaming currencies have garnered scholarly attention,[202] and have been described as "wildly successful in their respective in-game economies, they are used by millions to buy goods and services in limited virtual environments, and it has been proven that people will pay real cash to boost their online content."[203] Fascinatingly, these in-game currencies have given rise to problems such as unregulated virtual banks and virtual bank runs, leading to real-world financial losses.[204] Linden dollars even caught the attention of the European Central Bank, which emphasized the problems of Ponzi schemes, fraud, unregulated virtual financial institutions, and lack of external oversight in Second Life in its 2012 report on virtual currencies.[205] Even so, their impact outside of a community of gaming enthusiasts remains limited, unlike blockchain-based virtual currency like Bitcoin primarily meant to facilitate real-world transactions. And the technological model in-game currencies rely upon – a central issuer trading virtual tokens for "real" currency – is at base just an online version of something akin to Disney dollars.[206] Hardly transformative, disruptive, or revolutionary, in other words, even if fun for certain users.

Virtual gaming currencies aside, the origin of virtual currency – particularly Bitcoin – and the concept of the blockchain is (despite some earlier predecessors)[207] generally traced to a short paper posted on an online cryptography mailing list in 2008 by a poster going by the pseudonym "Satoshi Nakamoto," a person or group that has yet to be definitively identified.[208] The unassuming announcement accompanying the post carried little fanfare: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party."[209] The key features of this new system were summarized briefly as 1) using a

[202] *See* Clare Chambers-Jones, *Virtual Economics and Virtual Crime: Money Laundering in Cyberspace*, p. 11-12 (Edward Elgar Publishing Limited 2012). For a list of sources on the topic of virtual gaming currencies, *see* Trautman, *supra* n. 66, 5 n.13.

[203] Guadamuz and Marsden, *supra* n. 30.

[204] Chambers-Jones, p. 50-52.

[205] European Central Bank, *Virtual Currency Schemes*, p. 30-32 (October 2012).

[206] *See* https://disneyworld.disney.go.com/faq/parks/using-disney-dollars/.

[207] http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[208] *See* Tu & Meredith, *supra* n. 113, at 277-278. In a bit of recent drama, Australian Craig Wright claimed on May 2, 2016 to the BBC to be Satoshi Nakamoto and provided purported evidence that allegedly supported his claim. *Craig Wright revealed as Bitcoin creator Satoshi Nakamoto*, BBC (May 2, 2016), at http://www.bbc.com/news/technology-36168863. The Economist reacted skeptically. *Craig Steven Wright claims to be Satoshi Nakamoto. Is he?*, The Economist (May 2, 2016), at http://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin. Others provided evidence that Wright's "evidence" was fraudulent. https://dankaminsky.com/. Wright then promised "extraordinary proof" that he was Satoshi, but then was unwilling or unable to provide it. Rory Cellan-Jones, *'Bitcoin creator': I do not have the courage*, BBC (May 5, 2016), at http://www.bbc.com/news/technology-36213588. The consensus is that Wright is not, in fact, Satoshi. *Wright's wrongs*, The Economist (May 7, 2016), at http://www.economist.com/news/finance-and-economics/21698294-quest-find-satoshi-nakamoto-continues-wrightu2019s-wrongs.

[209] Other major inventions have had similarly humble inaugurations. When the telephone was invented, the first message ever transmitted was "Mr. Watson, come here, I want to see you." American Treasures of the Library of Congress, available at https://www.loc.gov/exhibits/treasures/trr002.html.

peer-to-peer network to solve the double-spending problem while eliminating centralized control; 2) creating new virtual currency through mathematical calculations called "proof-of-work" that also prevent double-spending; and 3) anonymity of users.[210]

By way of explanation, the double-spending problem is exactly what it sounds like: the same exact unit of value being illegitimately spent twice by a user.[211] Unless solved, the double-spending problem would enable a user to spend a unit of virtual currency X on Transaction A and then either pull-back unit X from the transaction once completed or regenerate unit X and then reuse the same exact unit X to undertake Transaction B (and maybe Transactions C, D, and E while he was at it). Not only would this devalue the virtual currency akin to counterfeiting a "real" currency, but it could result in defrauded transaction counterparties. Naturally, few rational people would use a virtual currency in which the double-spending problem was unsolved.

The paper itself, called "Bitcoin: A Peer-to-Peer Electronic Cash System,"[212] explains the workings of the new system in more depth – in only nine pages. Heavily mathematical and computer science-based, the paper first identifies the problems to be solved. Namely, 1) the need for trust in conventional electronic payment systems and the subsequent need that financial institutions act as trusted intermediaries, and 2) that even with these trusted financial intermediaries overseeing the system, the risk that payments will be reversed always remains.[213] Trust is always something that can be taken advantage of, in other words, increasing the amount of personal information that must be provided to counterparties, providing an incentive for fraudulent conduct, and raising transaction costs. In addition, small payments (so-called "micropayments") are impractical because of the associated transaction costs.[214]

The way around these problems is to get rid of the financial intermediary by substituting a decentralized peer-to-peer network employing sophisticated cryptologic, mathematical, and computer science techniques to approve transactions (and, by extension, to disapprove attempts at fraudulent double-spending transactions).[215] These techniques, when put together, constitute the blockchain, a public ledger constituting the agreed-upon true record of previous transactions which is used to confirm new transactions. The article's abstract explains the blockchain and its functioning in just a few sentences:

> The [peer-to-peer] network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers.[216]

What this means is that the system uses cryptographic functions (e.g. "hash-based proof-of-work" calculations) undertaken by computers not under the control of any centralized entity to create mathematical consensus about the "true" public ledger comprised of a chain containing information on all previous transactions. This cryptographic-powered mathematical consensus makes the "true" public ledger literally unassailable,[217] meaning any

[210] *Id.*

[211] For a good discussion of the "double-spending" problem, *see* Tu and Meredith, *supra* n. 113, at 280-82.

[212] https://bitcoin.org/bitcoin.pdf.

[213] *Id.* at p. 1.

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] Unless, as discussed below, 51% or more of the computing power devoted to the network is dishonest.

transaction recorded in it is thereby also “true” and irreversible. Trust is not needed because even if some of the computers in the network are dishonest and generate false entries, their attempts at subversion will be overridden and drowned-out by the majority of non-corrupted, honest computers. A central financial intermediary is also not needed because the network itself performs that function.

Under this system, a unit of virtual currency (e.g. a Bitcoin or an “electronic coin”) is defined as “a chain of digital signatures,” and transfers occur by the payor “digitally signing a hash of the previous transaction [with the payor’s private key] and the public key of the next owner and adding these to the end of the coin.”[218] Each transfer is then published to all nodes in the system, aggregated into blocks, subjected to the proof-of-work calculations described above, and validated.[219] The longest chain always wins because it represents the consensus of truth by having “the greatest proof-of-work effort invested in it.”[220] As long as the majority of computing power is honest then the true chain will grow the fastest and at a rate that will thwart subversion attempts.[221]

Providers of computing power are incentivized to participate in the necessary generation of proof-of-work calculations via a bounty system that awards new Bitcoin to the creator of each block.[222] Nakamoto compares participants to gold miners whose efforts add to the gold supply, noting that the resources used to mine Bitcoin are CPU time and electricity.[223] Over time, the incentive can become wholly transaction-fee based, with a small amount of existing value to be siphoned out of each block and provided to the block creator as compensation.[224] Ingeniously (or perhaps ingenuously) Nakamoto argues that this incentive program should keep a dishonest actor that controls a majority of the network’s computing power from subverting the currency because “[h]e ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.”[225]

B. *Attributes Important to AML/CFT Regulation*

Other key features of virtual currencies (usually Bitcoin) and blockchain are repeatedly noted in the literature, including attributes impacting AML/CFT regulatory considerations. A discussion of these attributes follows.[226]

i. Non-Legal Tender Status

One such feature is non-legal tender status and lack of governmental or private backing. This means that units of virtual currency do not represent any sort of legally-enforceable claim against an issuer. This also means that a holder of virtual currency cannot

[218] *Id.* at p. 2.
[219] *Id.* at p. 3.
[220] *Id.*
[221] *Id.*
[222] *Id.* at 4.
[223] *Id.*
[224] *Id.*
[225] *Id.*
[226] For a parallel discussion, *see* Robert Stokes, *Anti-Money Laundering Regulation and Emerging Payment Technologies*, 32 No. 5 Banking & Fin. Services Pol'y Rep. 1 (May 2013)(identifying the following features of Bitcoin as serious money laundering risks: anonymity, lack of centralized financial institutions as transaction intermediaries, and ease and speed of cross-border transmissibility).

compel a potential trading partner to accept it in an exchange, unlike legal tender currency.[227]

However, the lack of legal tender status may have less impact than commonly thought. For example, in the U.S., while larger denomination U.S. dollar bills are legal tender "for all debts, public charges, taxes, and dues" under 31 U.S.C. § 5103, a private merchant may refuse to accept them as there is "no Federal statute mandating that a private business, a person or an organization must accept currency or coins as for payment for goods and/or services."[228] In the UK, in contrast, banknotes issues by Scottish and Northern Ireland banks are not legal tender in England and Wales, but are nonetheless accepted in private transactions if the parties choose: according to the Bank of England, "[i]n ordinary everyday transactions, the term 'legal tender' in its purest sense need not govern a banknote's acceptability in transactions."[229] In addition, as discussed below, lack of legal tender status did not prove problematic to the ECJ when determining Bitcoin's VAT exemption status under EU law vis-à-vis traditional, legal tender currencies.

One disadvantage of non-legal tender status is that potential users may be wary of adopting a particular virtual currency because of the threat that government regulation could "kill" it. In the EU and the U.S., at least, it is unlikely that (except in the case of sanctions against de facto enemies like Cuba or Iran) regulators would enact regulations making it illegal to trade in a "fiat" currency issued by a sovereign government, especially in the case of major currencies. And even if such regulations were enacted, legal tender status within the boundaries of the issuing state would at least ensure that the currency could be used somewhere, even if doing so violated the laws of one's home country and raised other practical barriers. The same cannot be said for virtual currencies, where the adoption of AML/CFT regulation could make entire virtual currencies not conforming with these regulations legally unusable, with no guarantee of a "safe" territory where the currency would still be good. While illegal use of virtual currencies not meeting AML/CFT regulations could certainly continue, and while persons could seek to reroute their virtual currency transactions to offshore centers or otherwise seek to circumvent a ban, the loss of a legal way to exchange virtual currencies simply and cheaply would likely spell doom for their value and their viability as a medium of exchange.

One implication of the non-legal tender status of virtual currency such as Bitcoin is that it may not qualify as "funds" under the 4th AMLD, which as discussed above could be defined as "banknotes and coins, scriptural money and electronic money[.]" As a result, it is unclear that financing terrorism with Bitcoin would be "terrorist financing," given the definition of that term based on "the provision or collection of funds."[230] It is also unclear that there would be any duty by an obligated entity to report a suspicious transaction involving Bitcoin, since that duty is predicated on suspicion involving "funds."[231] These drafting peculiarities could be easily fixed, but the point remains that may indeed need fixing. Then again, as discussed below in connection with the *Hedqvist* case, it may be possible to interpret "funds" to include Bitcoin.

ii. Anonymity (?)

[227] U.S. Department of the Treasury FAQs, Legal Tender, at https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx.
[228] *Id.*
[229] Bank of England FAQs, Are Scottish & Northern Ireland banknotes "legal tender"?, http://www.bankofengland.co.uk/banknotes/Pages/about/faqs.aspx#sandni. This example is borrowed from Guadamuz and Marsden, *supra* n. 30, who presented it in the same context.
[230] Article 1(5).
[231] Article 33(1)(a).

Of critical importance for the AML/CFT regulatory discussion that follows, the blockchain was conceptualized by Nakamoto as permitting anonymity (or the potential for anonymity) in financial transactions. Although all transactions are necessarily published, if the public does not have any information about the owner of the public key used in a transaction, then that transaction cannot be attributed to any particular individual.[232] Since the owner of a public key would not normally publically disclose his ownership, the result is that the public will see virtual currency change "hands" without having any information about the identity of the sender or the recipient.[233] By simply using a new public key for each separate transaction,[234] users will further deter efforts to link transactions to themselves by making datamining or intelligence gathering more difficult if not impossible.[235]

Whether Bitcoin and the blockchain permit true anonymity is heavily debated, however. For example, two Russian virtual currency experts note that a single user could theoretically acquire the complete database of all transactions that have ever occurred, which could permit sophisticated datamining in order to uncover a user's identity.[236] Other researchers discovered patterns in how the blockchain updated that enabled sophisticated mapping to IP addresses and thus to real identities.[237] On the other hand, so-called "mixing services" and other advanced methods (including alternate protocols or so-called "altcoins") can allow users to thwart tracking,[238] though with uneven results.[239] Even so, user slip-ups, network analysis, the use of intermediaries, and old-fashion detective work have been cited as reasons that Bitcoin anonymity is illusory, with some commentators concluding that "Bitcoin anonymity ultimately fails because users cannot help but operate in the real world."[240] In one notable example, a Berkeley computer scientist was able to trace 29,000 Bitcoins from Silk Road to the laptop of its founder and operator, Ulbricht, using only information in the public domain.[241] In fact, Ulbricht's downfall came as a result of simple early sloppiness in drumming up business for the then-fledgling site: he posted his email address in an online forum, allowing the FBI to access all emails on that address via a search warrant and build their case.[242] Because any vestige of anonymity ends once law enforcement seizes a Bitcoin user's computer as part of an investigation, Ulbricht case demonstrates the limits of anonymity, at least if enough investigative resources and skill are devoted to a particular case.[243] And if the Dread Pirate Robert's anonymity could be defeated, so could others',

[232] *Id.* at 6.

[233] *Id.*

[234] Though the Nakamoto paper does not make this point explicitly, the number of potential public keys is practically unlimited: 2^{160} unique addresses, which translates to around 1.46 x 10^{48}. *See* https://bitcointalk.org/index.php?topic=678778.0.

[235] *See id.*

[236] Victor Dostov and Pavel Shust, *Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?*, 21 Journal of Financial Crime 3, p. 252 (2014)(citing Reid, F. and Harrigan, M., *An analysis of anonymity in the bitcoin system* (2012)), available at http://arxiv.org/abs/1107.4524.

[237] John Bohannon, *Why criminals can't hide behind Bitcoin*, Science (Mar. 9, 2016), at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[238] Aviv Zohar, *Bitcoin: Under the Hood*, 58 Communications of the ACM 9, p. 111 (Sept. 2015)(providing examples of CoinJoin and Zerocash).

[239] Bohannon, *supra* n. 237.

[240] Guadamuz and Marsden, *supra* n. 30.

[241] Andy Greenberg, *Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht's Laptop*, Wired (Jan. 29, 2015), at http://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/.

[242] Joab Jackson, *All the feds needed to do to ID Silk Road's founder was Google it*, PC World (Jan. 26, 2015), at http://www.pcworld.com/article/2875652/simple-google-search-outed-alleged-silk-road-founder.html.

[243] Greenberg, Wired (Jan. 29, 2014); *see also* Trautman, *supra* n. 66, at 103 (quoting François R. Velde, Senior Economist, Federal Reserve Bank of Chicago, as stating: "If anything, a virtual currency like Bitcoin provides traceability - if you have access to a criminal's hard drive, and therefore to his wallet information, you could prove in court that certain payments were made").

sometimes with far less investigative effort.[244]

Even so, though anonymity may not be absolutely impenetrable, it still defines in some measure both Bitcoin transactions and those of many other alternate virtual currencies now in use. But so does traceability, since all transactions are forever recorded in the blockchain. These characteristics of Bitcoin and many other current virtual currencies are of major importance in the AML/CFT regulatory discussion that follows.[245] As a preview, AML/CFT regulation must find a way to "tame" anonymity while permitting everyday privacy vis-à-vis third-parties so that a private person's purchasing habits cannot be attributed to an identifiable individual by curious internet users or hackers. Taming anonymity means that governments (i.e. FIUs and law enforcement) must have a way to determine the identities of senders and recipients on a need-to-know basis and must be allowed to perform suspicious transaction analysis on the blockchain to identify transactions requiring increased scrutiny. Otherwise, as virtual currencies become a self-contained closed system through wider adoption, relying on existing AML/CFT mechanisms enlisting private gatekeepers will fail, as increasingly those gatekeepers will no longer play any role in financial transactions. This failure would precipitate a crisis, as either AML/CFT regulation must then yield or virtual currencies that had already "succeeded" would have to be curtailed. Smart regulation that channels development in a direction compatible with AML/CFT norms can preserve the best of both worlds: privacy versus third parties and penetrable anonymity versus governments.

iii. Lack of Fundamental or Intrinsic Value

A feature of (existing) virtual currencies like Bitcoin and a serious potential problem with their use as currency is their lack of fundamental or intrinsic value. To illustrate, shares of stock have determinable fundamental value because they represent a legally enforceable claim on a portion of a corporation's assets, future earnings, and dividend payments. Government and corporate bonds have determinable fundamental value because they provide a right to an earnings stream at a defined interest rate and to the return of principal. Currency issued by governments has value because it can be used to pay tax liabilities.[246] Ownership of a unit of virtual currency allows the user to exchange or dispose of that unit, but that provides little help in determining how to value the unit, leading some to half-joke that its "speculative value is based on the spin of technological mystery – the crypto-nature of bitcoin – and the mining of these supposed to be magical crypto-numbers"[247] – concepts alien to conventional asset valuation theory.

Obviously corporations and even governments can become insolvent and stocks and bonds issued by these entities can become worthless. "Fiat" currencies issued by sovereign governments can also cease to have value, and "legal tender" status will not improve the situation. The danger with virtual currency though is that there is nothing "special" about any current particular embodiment of it, Bitcoin included, other than popularity, and nothing holding up any particular virtual currency's value other than the belief that others will also

[244] *See* Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, Forbes (Sept. 5, 2013), at http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/#14de58f089a8.

[245] Many others have identified the anonymity of Bitcoin transactions as an AML concern. *See, e.g.*, Nicholas Ajello, *Note: Fitting a Square Peg in a Round Hole—Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, 80 Brook. L. Rev. 435, 446-447 (2014-2015); Stokes, *supra* n. 96; Bryans, *supra* n. 65 at 447.

[246] *See* Luther, *supra* n. 4, at 398-399.

[247] Adrian (Wai-Kong) Cheunga, Eduardo Rocab, and Jen-Je Su, *Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices*, Applied Economics, Vol. 47, No. 23, 2348–2358, 2350 (2015).

believe that that particular virtual currency has value.[248] This is a circular, and tenuous, position to be in.[249]

As long as other users will continue to act in a way that will hold up a virtual currency's value, then all is well. However, one potential fallacy in this thinking is that the underlying protocols for Bitcoin (and other virtual currencies) are in the public domain and can be (and are) replicated or altered to form competing "alt-coins," e.g. alternate virtual currencies. According to Kenyon College Assistant Professor of Economics William J. Luther, as of July 15, 2015, there were over 500 alt-coins in circulation with a combined market capitalization of $720 million U.S. dollars.[250] One or more of these could eventually displace Bitcoin despite its "first-mover advantage" by improving on existing features or introducing new ones and thereby enjoy a "second-mover advantage."[251] Because the value of any particular virtual currency depends largely on network effects[252] – e.g., the more that people use a particular technology, the more that technology is worth using – potential competition from other virtual currencies should contribute to the high price volatility that has plagued Bitcoin[253] as no one wants to be left invested in a virtual currency that others have left, especially given the lack of inherent "specialness" of any particular virtual currency. One only need look at what happened to MySpace, the first real social media network, once Facebook became prominent. It basically died as network effects worked backwards: the more people who switched from MySpace to Facebook, the more reason for others to do so as well.

The point is that at present any particular virtual currency, Bitcoin included, faces a valuation black hole as a result of several combined factors: lack of intrinsic value, value derived solely from a collective assessment of what others assess the collective assessment of

[248] There is a counterargument: that the vast amounts of computing power that have been invested into building the Bitcoin blockchain, and in thereby making that blockchain harder to attack, imbue Bitcoin (and to a lesser extent, by the same logic, other alt-coins that have substantial histories) with value. *See* Guadamuz and Marsden, *supra* n. 30, stating that Bitcoin's "proponents claim that it has "'real' value" based on the computing power it took to mine them. Others, including the Bitcoinwiki page on Bitcoin myths, calls this false, arguing that this belief is an offshoot of the labor theory of value – a theory that is false because it might take a lot of resources and human effort to produce something utterly worthless. *See* https://en.bitcoin.it/wiki/Myths#The_value_of_bitcoins_are_based_on_how_much_electricity_and_computing_power_it_takes_to_mine_them.

[249] Like the fabled "Keynesian beauty contest in which one is required to form an expectation about what average opinion expects average option to be and so on," the result is that the determination of a virtual currency's value is wholly circular and nested: its value is completely dependent upon the collective belief about (the collective belief about) its value and its acceptability as a means of exchange. *See* Hammad Siddiqi, *The Routes to Chaos in the Bitcoin Market*, p. 2-3 (February 17, 2014), available on Social Science Research Network (SSRN) at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2396997&download=yes (noting circular nature of Bitcoin valuation and stating that "inability to be a reasonably reliable store of value has implications for the currency's effectiveness as a medium of exchange"). For additional reading on the Keynsian beauty contest, *see* Richard Thaler, *Keynes's 'beauty contest'*, Financial Times Magazine (July 10, 2015), at http://www.ft.com/intl/cms/s/0/6149527a-25b8-11e5-bd83-71cb60e8f08c.html. Put whimsically, any particular virtual currency, such as Bitcoin, has value in the same sense that Wile E. Coyote could float in midair – as soon as he looked down and realized there was no solid ground, the illusion was shattered, gravity took over, and down he went. Though the author came up with this (banal but amusing) analogy on his own, others have had similar thoughts. For instance, one blogger writes: "Like Wile E. Coyote walking off the edge of a cliff, things like tulip bulbs. . . can seem to have a great value for some period of time - but eventually people wake up and realize it is worthless." http://www.vartmp.com/blog/bitcoin.

[250] Luther, *supra* n. 4, at 399.

[251] *Id.* at 399-400.

[252] *Id.* at 398.

[253] *See* chart at http://www.coindesk.com/price/.

value to be, low barriers to entry for competitor virtual currencies,[254] and network effects that can cause price swings rather than stability. Criticisms along these lines have come from high places. Former Chairman of the U.S. Federal Reserve, Alan Greenspan, has criticized Bitcoin as lacking intrinsic value, calling it a "bubble."[255] Investor Warren Buffett has criticized Bitcoin from the same angle, adding that while the underlying blockchain technology might be an innovation, there is no reason to believe that Bitcoin itself (or any particular virtual currency) has any real worth because it the thing that has value – the method of transmitting money made possible by the blockchain – is replicable via alternate virtual currencies.[256]

The counterargument – that "intrinsic value" is meaningless as a metric because Bitcoin (and current virtual currencies) have a market capitalization in the billions of U.S. dollars, indicating that the market has accepted them regardless of what Warren Buffett or Alan Greenspan might think – ignores that financial bubbles have repeatedly followed the same pattern. Though Dutch Tulip Mania is the classic case mentioned in the context of financial bubbles,[257] a more recent example involved the stuffed animals called "Beanie Babies."[258] Fascinatingly, a number of commentators have drawn parallels between the Beanie Baby bubble and Bitcoin.[259] One article even noted that the total value of all Beanie

[254] *See* ECB, *Virtual Currency Schemes – A Further Analysis*, § 1.2 (February 2015), available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (stating "[g]iven that Bitcoin is an open-source project, it is relatively simple to launch a new [virtual currency] based on its protocol").

[255] Jeff Kearns, *Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value*, Bloomberg Business (Dec. 4, 2013), available at http://www.bloomberg.com/news/articles/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.

[256] Kashmir Hill, *Bitcoin Battle: Warren Buffett vs. Marc Andreessen*, Forbes (March 26, 2014), available at http://www.forbes.com/sites/kashmirhill/2014/03/26/warren-buffett-says-bitcoin-is-a-mirage-why-marc-andreessen-thinks-hes-wrong/#25b257722521. Buffett's take is as follows:

> Bitcoin is a mirage. It's a method of transmitting money. It's a very effective way of transmitting money and you can do it anonymously and all that. A check is a way of transmitting money, too. Are checks worth a whole lot of money just because they can transmit money?. . . I hope bitcoin becomes a better way of [transmitting money], but you can replicate it a bunch of different ways and it will be. The idea that [Bitcoin] has some huge intrinsic value is just a joke in my view.

[257] *See* Charles Mackey, *Memoirs of Extraordinary Popular Delusions and the Madness of Crowds* (London 1852), available online at http://www.gutenberg.org/ebooks/24518, which contains an oft-cited chapter on the Dutch tulip bulb bubble of the 17th century.

[258] As a brief summary, grown adults paid hundreds and even thousands of dollars for the stuffed animals, not because there was anything special about the toys (there was not) but because others were willing to buy them for even more money. The company that made the toys limited the numbers of each series produced, thereby creating both manufactured scarcity and a plausible-enough sounding cover story as to why it was not transparently insane to spend huge amounts of perfectly good money on otherwise worthless small stuffed animals. During the height of the bubble, Beanie Babies comprised 10% of eBay's sales, and the toy company's founder became a billionaire. Reality finally kicked in, though, and prices plummeted, leaving some unlucky souls with vast numbers of the toys and no money. Sadly, before it was all over Beanie Babies played starring roles in human tragedy, including bankruptcy, divorce, and even murder. *See* Mark Joseph Stern, *Why did people lose their minds over Beanie Babies?*, Slate (Feb. 3, 2015), available at http://www.slate.com/articles/health_and_science/science/2015/02/beanie_babies_bubble_economics_and_psychology_of_a_plush_toy_investment.html (writing that "[p]eople sold—and bought—some rare Beanie Babies for $5,000 each and expected others to skyrocket in value within a decade.") Anne VanderMey, *Lessons from the great Beanie Babies crash*, Fortune (March 11, 2015), available at http://fortune.com/2015/03/11/beanie-babies-failure-lessons/; Rachel Feltman, *Meet the family who lost $100,000 when the Beanie Baby bubble burst*, Quartz (August 13, 2013), available at http://qz.com/114753/meet-the-family-who-lost-100000-when-the-beanie-baby-bubble-burst/.

[259] One is the author of a recent book entitled "The Great Beanie Baby Bubble: Mass Delusion and the Dark Side of Cute," Zac Bissonnette. In a March 2015 interview with Fortune magazine, Bissonnette opined that it seemed that Bitcoin was following the same pattern as Beanie Babies, with stories of early users becoming rich

Babies at the height of the bubble in 1999 probably approximated the November 2013 market capitalization of Bitcoin of $10 billion.[260]

Outside of the intuitive suspicion some observers harbor that Bitcoin is a bubble, solid empirical evidence supports the bubble hypothesis, including a study by three Australian researchers used sophisticated financial modeling to confirm that bubble dynamics defined Bitcoin pricing.[261] Less sophisticated technical analysis also supports this conclusion.[262] There is, in other words, an identified (and real) risk that bubble dynamics are at work with Bitcoin (and potentially other virtual currencies as well).

Unless there is a solution to the widely-identified no "intrinsic value" problem, then it is questionable whether virtual currencies will succeed beyond a limited number of users. For one thing, they will remain highly-volatile, as users can never know when the value of their holdings might all come crashing down in a cascade of panic exits. Since it is never good to be last in a panic selling cascade, this hair-trigger uncertainty should contribute to constant "noise trading" – trading not on material information but on non-material "noise."[263] Empirical evidence suggests noise trading heavily influences Bitcoin pricing, in the sense that non-material non-information dominates trading dynamics.[264] Other possible reasons for the

leading to widespread interest spawned by "greed and jealousy." VanderMey, *supra* n. 258. An author for *Business Insider* drew the parallel as well in an April 2013 article, while a commentator writing for *PC Magazine* wrote in November 2014 that "I've said before that bitcoins are the new Beanie Babies, and suffice it to say that it looks, sounds, and feels like the Beanie Baby era without the TV shows that cropped up around the stupid stuffed animals." Joe Weisenthal, *Why Bitcoin Is Like No Other Bubble We've Seen Before*, Business Insider (April 3, 2013), available at http://www.businessinsider.com/why-bitcoin-is-like-no-other-bubble-weve-seen-before-2013-4?IR=T; John C. Dvorak, *Bitcoin & Beanie Babies: How to Spot a Tech Bubble*, PC Magazine (Nov. 5, 2014), available at http://www.pcmag.com/article2/0,2817,2471603,00.asp. Columnist Al Lewis in the *Wall Street Journal* was even more sardonic: "The bitcoin is a mania like tulip bulbs in the 1600s and Beanie Babies in the 1990s. Manias spread like communicable diseases. The more people talk, the more they spew nonsense on each other." Al Lewis, *Tulip Bulbs for Our Time*, Wall Street Journal, Al's Emporium—Commentary (December 8, 2013), available at http://www.wsj.com/articles/SB10001424052702304096104579240213383697076. There are yet more examples of the comparison being made between Beanie Babies and Bitcoin, both by mainstream media and non-traditional internet fora. *See, e.g.*, Gerber, *supra* n. 14; Geoff Williams, *Should You Invest in Bitcoin?*, U.S. News & World Report (May 1, 2013), available at http://money.usnews.com/money/personal-finance/articles/2013/05/01/should-you-invest-in-bitcoin; The Homeless Billionaire, *Bitcoins are the New "Beanie Babies"*, This is Why You're Broke [blog] (Feb. 23, 2014), at https://thisiswhyubroke.wordpress.com/2014/02/23/bitcoin-is-the-new-beanie-babies/.

[260] Nicholas Weaver, *Once You Use Bitcoin You Can't Go 'Back' – And That's Its Fatal Flaw*, Wired (Nov. 26, 2013), available at http://www.wired.com/2013/11/once-you-use-bitcoin-you-cant-go-back-and-that-irreversibility-is-its-fatal-flaw.

[261] Cheunga, Rocab, and Su, *supra* n. 247, at 2356-2357.

[262] *See* Jesse Colombo, *Bitcoin May Be Following This Classic Bubble Stages Chart*, Forbes (Dec. 19, 2013), at http://www.forbes.com/sites/jessecolombo/2013/12/19/bitcoin-may-be-following-this-classic-bubble-stages-chart/2/#58a9741660db.

[263] Drawing upon the concepts of late Professor Fischer Black (of the Black-Scholes option valuation model fame), "'information' is any item of data that correctly reflects a stock's fundamental value, while '"[n]oise" is any [item of] data that is not information.' Accordingly, information is useful to market participants for trading purposes, whereas noise is not useful, or worse, detrimental to profitable trading." Steven L. Schwarcz, *Temporal Perspectives: Resolving the Conflict Between Current and Future Investors*, 89 Minn. L. Rev. 1044, 1081 (April 2005)(quoting Fischer Black, *Noise*, 41 J. Fin. 529 (1986)).

[264] Michal Polasik, Anna Iwona Piotrowska, Tomasz Piotr Wisniewski, et al., *Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry*, International Journal of Electronic Commerce, Vol. 20, No. 1, p. 9-49, 36 (Aug. 31, 2015):

> [P]opularity of this cryptocurrency is one of the main factors driving the price. . . returns tend to be elevated whenever newspaper articles mention Bitcoin more frequently and whenever the number of people searching for it on Google increases. Moreover, the tone of newspaper articles also influences

high volatility of virtual currencies (again, mostly Bitcoin) are mentioned in the literature and financial press. Such factors as "experimentation" by users prompted by Bitcoin's "startup" nature,[265] a large percentage of pure speculators as users,[266] events such as the Cyprus banking crisis and the implosion of the Mt. Gox Bitcoin exchange,[267] high trading volumes driven by noise traders,[268] and even a large Russian/Chinese Ponzi scheme causing unusual price fluctuations[269] have been offered.

As will be discussed in more detail below, AML/CFT regulation could play a decisive role in fixing the "no inherent value" problem of virtual currencies, actually saving the day rather than stifling innovation. It could do so by acting as a barrier to entry, allowing only virtual currencies that use AML/CFT compliant protocols that can deanonymize trades for FIUs or law enforcement to be traded legally. Because businesses and non-criminal consumers are likely to only want to use legal virtual currencies, and because wide adoption by these actors will be necessary for a particular virtual currency to have sustained value, AML/CFT regulation could make complying virtual currencies less like tulip bulbs or Beanie Babies and more like traditional financial instruments. In addition, not regulating virtual currencies may stunt their development by making consumers and businesses wary to adopt them because of the accompanying legal uncertainty,[270] again counseling towards using AML/CFT regulation as a way to help virtual currency succeed.

iv. Vulnerability to a "51% attack"

The protocol for Bitcoin, currently the largest virtual currency, has a potentially fatal flaw: if more than half of the computing power dedicated to the mining network comes under common control, then the blockchain could be effectively hijacked and rewritten.[271] That is because "truth" of the Bitcoin blockchain is only what a majority of miners affirm it to be, a noble idea in theory but one that could come crashing down in practice. The computing and monetary resources necessary to effect a so-called "51% attack" would be enormous: $425 million in computing equipment and electricity.[272] The problem is that as the resources required to mine Bitcoin have increased substantially in recent years, mining pools have formed in which decentralized actors combine their computing resources into centralized groups. One such group, GHash.IO, actually controlled more than half of all mining

the value of Bitcoin—unfavorable mentions can have negative consequences, whereas exhortatory pieces increase the price.

[265] Timothy B. Lee, *Bitcoin's Volatility is a Disadvantage, But Not a Fatal One*, Forbes (Apr. 12, 2013), at http://www.forbes.com/sites/timothylee/2013/04/12/bitcoins-volatility-is-a-disadvantage-but-not-a-fatal-one/#6e77f95c635e.

[266] Kessler, *supra* n. 5.

[267] Nathalie Stråle Johansson & Malin Tjernström, *The Price Volatility of Bitcoin, A search for the drivers affecting the price volatility of this digital currency*, Umeå School of Business and Economics – Masters Thesis, p. 61 (Spring 2014), available at http://www.diva-portal.org/smash/get/diva2:782588/FULLTEXT01.pdf.

[268] *Id.*, p. 62.

[269] Victor Luckerson, *Here's Why Bitcoin Is So Volatile Right Now*, Fortune (Nov. 5, 2015), at http://fortune.com/2015/11/05/bitcoin-volatile/.

[270] Luther, *supra* n. 4 at 399 (citing Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, Hastings Science & Technology Law Journal 4, no. 1: 159-208 (2011)).

[271] Trautman, *supra* n. 66 at 54 (citing Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, *The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, June 10-11 2013, available at https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf.

[272] *The Magic of Mining*, The Economist (Jan. 10, 2015), at http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic.

resources in June 2014, prompting justified fear amid the Bitcoin community since it was now possible for a single entity to subvert the virtual currency.[273] While that situation has resolved, the threat remains that a group could reach the 51% threshold in the future, even if enormous resources were required.

This possibility poses AML/CFT concerns, since a group or entity with majority control could find a way to thwart any AML/CFT regulatory regime created around the particular virtual currency. Extremist groups with enough supporters and resources or even a state actor could hijack the blockchain, potentially shielding trades from AML/CFT oversight. As will be discussed below, any AML/CFT regulatory regime that involves compliant protocols must create a mechanism to protect the protocol from outside attack. Otherwise, the risk is that widespread groups of businesses and consumers will become reliant on a particular AML/CFT compliant virtual currency, only to have that virtual currency's regulatory approval later destroyed. Users of a virtual currency must be able to trust that this will not happen, or else they will be reluctant to embrace the virtual currency in the first place, given the associated "switching costs" from "fiat" currencies and the "incumbent money problem" (e.g., why switch from a perfectly good currency to something else?).[274]

v. Easy and Cheap International Transmissibility

One major potential advantage of virtual currencies/blockchain over mainstream currencies and payment systems is that the former could allow for easier and cheaper international transmission of value. According to the February 23, 2016 draft report of the European Parliament's Committee on Economic and Monetary Affairs, virtual currencies and blockchain technology offer the potential of:

> dramatically lowering transaction costs for payments and transfer of funds, quite possibly well below 1%, compared to 2% - 4% for traditional online payment systems, and to more than 7 % on average for the cross-border transfer of remittances, hence potentially reducing global total costs for remittances by up to EUR 20 billion.[275]

However, while the transactions costs of international fund transfers are lower for virtual currencies, extreme price volatility currently limits their usefulness in practice. Because Bitcoin transaction clearing times are currently around eight minutes,[276] volatility means that price of Bitcoin relative to the underlying "real" local currency of the recipient could fall significantly during that gap.[277] Even so, a more mature version of virtual currency

[273] Tim Hornyak, *One group controls 51 percent of Bitcoin mining, threatening security sanctity*, PC World (June 16, 2014), at http://www.pcworld.com/article/2364000/bitcoin-price-dips-as-backers-fear-mining-monopoly.html.

[274] *See* Luther, *supra* n. 4, at 398 (discussing switching costs and the incumbent money problem in virtual currency context).

[275] *Supra* n. 77, at p. 5 (citing https://remittanceprices.worldbank.org/sites/default/files/rpw_report_december_2015.pdf).

[276] https://blockchain.info/charts/median-confirmation-time?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

[277] *See* Alex Court, *Breaking the bank: Bitcoins hit Africa's money transfer traditions*, CNN (Feb. 17, 2015), at http://edition.cnn.com/2015/02/17/business/bitcoin-africa-unbanked/ (noting "I could send $200 worth of Bitcoin to someone, but as the price fluctuates they actually only get say $150."); Romain Dillet, *Why I Lost Faith in Bitcoin as a Money Transfer Protocol*, TechCrunch (Jan. 1, 2014), at http://techcrunch.com/2014/01/01/why-i-lost-faith-in-bitcoin-as-a-money-transfer-protocol/ (noting that "(f)ees [using Bitcoin to transfer funds internationally] were much lower, but it doesn't matter if you don't know how much money you will get on your bank account in the end").

with less volatility could permit seamless international transmission of funds – and if widely adopted could give rise to an de facto international currency that would lessen the need to convert into various local currencies.

From a AML/CFT perspective, the risks are obvious, especially when looked at with the other features of virtual currencies like Bitcoin. Cheap, easy, quick, (largely) anonymous international transmission of funds, and (potentially) without any intermediary to perform as a gatekeeper tasked with reporting suspicious transactions – these features together, simply put, undercut AML/CFT regulation. While AML/CFT regulation cannot seek to forbid the international transmissibility of virtual currencies without destroying their utility, it can ensure that mechanisms are in place to identify, trace, and stop suspicious transactions, to require registration of cross-border transmissions exceeding a certain value threshold, and to allow deanonymization by FIUs and/or law enforcement (while protecting reasonable expectations of privacy for law-abiding users). These points will be discussed later in this paper.

vi. No Centralized Institutions

Virtual currencies like Bitcoin currently lack any sort of central authorities or institutions that can watch over the system. It is true that exchanges (like the ill-fated Mt. Gox) have arisen where units of virtual currency can be both electronically stored and traded for "real" currency. As will be discussed below, these institutions can act as gatekeeper intermediaries akin to traditional money exchange service providers, permitting some degree of AML/CFT accountability and customer due diligence functionality. However, international transmission of virtual currencies occurs without any intermediaries, unlike in traditional international wire transfers which put banks or other financial institutions at the center of each transaction. In these traditional transactions, the financial institutions involved are obligated to identify their customers, report suspicious transactions, and in some cases refuse to undertake them. These key functions of AML/CFT regulation are currently not possible for virtual currencies. Another scholar writing on Bitcoin's money laundering potential referred to this as "troublesome" because the "traditional approach to thwarting money laundering is through the use of banks or other key professionals as a policing force."[278] "Troublesome" may be an understatement, since the entire AML/CFT system is built around intermediaries ("obligated entities" in the EU).

A properly-functioning AML/CFT approach to virtual currencies will need to address this problem. In addition, if virtual currency use becomes widespread, it may develop into a closed-loop system, obviating the need to exchange them for "real" currencies. If this happens, then exchanges will no longer have a significant gatekeeper role. Instead, fundamentally different approaches to AML/CFT than those that dominate the current regime will need to be created. This will be no small task.

C. *EU Case Law*

Having discussed the attributes of virtual currency that impact AML/CFT regulation, this paper now turns to a discussion of virtual currency's current status under EU law. There is one seminal EU case. The ECJ had an opportunity to weigh in on the status of Bitcoin (and, indirectly, virtual currencies in general) in October 2015 in *Skatteverket v. David Hedqvist*,[279] albeit in the limited context of a preliminary reference under Article 267 TFEU.

[278] Ajello, *supra* n. 99, at 446.

[279] Case C-264/14 *Skatteverket v. David Hedqvist* [2015] EU:C:2015:718.

In *Hedqvist*, at issue was whether a business that exchanges Bitcoin for traditional fiat currency (and vice versa) for consideration must pay value added tax (VAT) on the exchange transactions. The ECJ ruled that it did not, holding that for VAT exemption purposes exchange transactions involving Bitcoin were to be treated the same as financial transactions involving tradition currencies.[280]

A summary of the case follows. A Swedish citizen, David Hedqvist, planned to run an electronic virtual currency exchange on his company's website by buying and selling Bitcoin for Swedish kronor in response to customers' online orders.[281] He would do so for compensation via a bid-ask spread[282] but would not charge additional fees or commission. Prudently, Mr. Hedqvist sought to determine ahead of time whether his contemplated business model would be subject to VAT in Sweden. He therefore asked the Swedish *Skatterättsnämnden*, e.g. the Revenue Law Commission, for a preliminary decision (sv. *förhandsbesked*) as to his VAT liability if he carried out his planned business.[283]

The Swedish Revenue Law Commission had to decide Mr. Hedqvist's case by reference to EU law. That is because VAT liability in Sweden is determined under the Swedish version of the EU VAT Directive,[284] *mervärdesskattelagen* (1994:200), e.g. the Law on VAT,[285] which Sweden had duly transcribed into its national law.[286] Under the EU VAT Directive, Article 2 subjects sales of goods and the provision of services within the EU to VAT, subject to certain mandatory exemptions enumerated in Article 135.[287] These Article 135 exemptions include transactions involving negotiable instruments,[288] "negotiation, concerning currency, bank notes and coins used as legal tender" but not counting non-legal tender precious metal coins or other purely numismatic items,[289] and transactions involving certain securities and other debt and equity interests.[290]

The Swedish tax authority, *Skatteverket*, maintained that Bitcoin exchange transactions should be subject to VAT and opposed Mr. Hedqvist's efforts. First, the *Skatteverket* insisted that the exchange of Bitcoins did not constitute a "service" because persons who exchange non-legal tender Bitcoins for legal tender currency do not obtain any benefit that can be considered as consumption.[291] The obvious weak-point in this argument was that if these transactions entailed no benefit it would be perverse to subject them to value-added tax, but the *Skatteverket's* apparent point was to avoid application of the Article 135 exemptions by characterizing Bitcoin sales as supply of goods. Additionally, if exchange of Bitcoins for traditional currency did constitute provision of services, then the *Skatteverket* argued that the Article 135 exemptions (as applied via Swedish law) did not apply because

[280] *Id.*, ¶ 44 – 53.

[281] *Id.*, ¶ 13.

[282] Although the ECJ never used the term "bid-ask spread," this is clearly the form of remuneration contemplated. *See id.*, ¶ 13 and 28. Ultimately, however, the type of remuneration model adopted for the exchange transactions had no bearing on the court's ruling, since all that mattered was that the exchange services were provided for consideration and were not gratuitously undertaken. *See id.*, ¶ 29.

[283] *Id.*, ¶ 15.

[284] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ 2006 L 347, p. 1).

[285] *Id.*, ¶ 7 – 9.

[286] In any event, the fidelity of the Swedish version of the law compared to the original EU directive was not at issue in the case.

[287] *Hedqvist*, ¶ 3 – 6.

[288] VAT Directive, Art. 135(1)(d).

[289] VAT Directive, Art. 135(1)(e).

[290] VAT Directive, Art. 135(1)(f).

[291] *See Mervärdesskatt: Handel med bitcoins*, 2013-10-14 (dnr 32-12/I), available at http://skatterattsnamnden.se/skatterattsnamnden/forhandsbesked/2013/forhandsbesked2013/mervardesskatthandelmedbitcoins.5.46ae6b26141980f1e2d29d9.html.

Bitcoins are not legal tender.[292]

The questions for the Revenue Law Commission, then, were whether transactions involving the exchange of Bitcoins for currency were 1) sales of goods or provision of services, and 2) if the latter, whether they fell under any of the Article 135 exemptions. The Revenue Law Commission ruled that the transactions in question constituted a service,[293] citing the ECJ case *Commissioners of Customs & Excise v First National Bank of Chicago*[294] which held that foreign exchange transactions constituted services and not supply of goods. Second, the Revenue Law Commission held that an Article 135-derived exemption relating to the provision of banking, financial, and securities transaction services[295] applied to Bitcoin exchange transactions but that Article 135(1)(e), referring to transactions involving "negotiation, concerning currency, bank notes and coins used as legal tender," did not apply because Bitcoin was not legal tender.[296]

The *Skatteverket* appealed to the Swedish *Högsta förvaltningsdomstolen* (Supreme Administrative Court), which in turn referred two questions to the ECJ: 1) are commercial Bitcoin/currency exchanges "services" under Article 2 of the EU VAT Directive, and 2) if so, does an Article 135(1) exemption apply?[297] In response to the first question, the ECJ held that virtual currencies like Bitcoin are not "tangible property" because they serve "no purpose other than to be a means of payment," the same as traditional fiat currencies, accepting in effect that both virtual currencies and traditional currencies exist to facilitate transactions in goods and services. In addition, the ECJ held that selling Bitcoin for traditional currencies is a "service" akin to a traditional foreign exchange transaction, again putting virtual currencies on par with traditional ones.[298] The ECJ also determined that the bid-ask spread charged by Mr. Hedqvist constituted "consideration" for purposes of the VAT Directive.[299] As a result, the ECJ held that exchanging traditional currency for Bitcoin and vice versa for payment via a bid-ask spread constituted "the supply of services for consideration" under the VAT Directive, answering the first referred question in the affirmative.[300]

Because the ECJ answered the first referred question "yes," it had to address the second referred question: does an Article 135(1) exemption apply, and if so, which one? In responding, the ECJ first emphasized the independent EU-law nature of the Article 135(1) exemptions.[301] In addition, the ECJ emphasized the need to balance the "requirement of strict interpretation" of exemptions to VAT liability with the importance of construing the exemptions so as not to "deprive [them] of their effect."[302] The ECJ then held that the exemptions in Article 135(1)(d) of the VAT Directive applying to "deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments" "concern services or instruments that operate as a way of transferring money" but that that subsection "does not cover transactions that involve money itself," which instead fall under Article 135(1)(e).[303] Bitcoin, the ECJ held, is not any of the items listed in Article 135(1)(d), but is instead "a direct means of payment between the operators that accept it."[304] As a result,

[292] *Id.*
[293] *Hedqvist*, ¶ 16.
[294] Case C-172/96 [1998] ECR I-4387.
[295] Chapter 3, Paragraph 9, Law on VAT.
[296] *Hedqvist*, ¶ 17.
[297] *Id.*, ¶ 21.
[298] *Id.*, ¶ 24 – 26.
[299] *Id.*, ¶ 27 – 31.
[300] *Id.*, ¶ 31.
[301] *Id.*, ¶ 33.
[302] *Id.*, ¶ 34 – 35.
[303] *Id.*, ¶ 40 – 41.
[304] *Id.*, ¶ 42.

Article 135(1)(d) does not provide a VAT exemption for Bitcoin exchange transactions.[305] Article 135(1)(e), on the other hand, does. While the text of that subarticle refers to "currency [and] bank notes and coins used as legal tender," the ECJ held that the text was ambiguous as to whether only traditional (i.e. legal tender) currencies were covered or whether all currencies were, especially given the interpretation difficulties caused by the equally authentic nature of all language versions of the Directive.[306] On this point, the ECJ cited to the Advocate General's opinion containing a number of comparisons between different language versions, including German, English, Finnish, and Italian, where the take-away lesson was that the different language versions were wholly and irreconcilably inconsistent as to whether only legal tender currencies were covered by the Article 135(1)(e) exemption.[307]

Because textual analysis was therefore not possible, the language in Article 135(1)(e) with regard to "currencies" had to be interpreted "in the light of the context in which it is used and of the aims and scheme of the VAT Directive."[308] To that end, the ECJ held that the purpose of the Article 135(1)(e) exemptions was to remove "financial transactions" from the coverage of the VAT Directive.[309] The ECJ additionally held that "financial transactions" include transactions in non-traditional (e.g., non-legal tender) currencies if the parties to a transaction accept non-traditional currencies in lieu of legal tender currencies and if the non-traditional currency used has "no purpose other than to be a means of payment."[310] The ECJ also stated that the rational underlying Article 135(1)(e) – the difficulties of determining VAT and the VAT deductible in currency exchange transactions – applies equally to exchange transactions involving only traditional currencies and those also including a non-traditional currency.[311] As a result, the ECJ held that it would deprive Article 135(1)(e) of its effect to treat traditional currencies differently than non-traditional currencies under that exemption.[312] In consequence, because Bitcoin has no purpose other than to serve as a means of payment among parties willing to accept it instead of traditional currency, Article 135(1)(e) applies to exempt currency exchange transactions involving Bitcoin from VAT liability.[313] Finally, the ECJ held that Bitcoin is not a "security."[314] Therefore, Article 135(1)(f), which applied to transactions in "shares, interests in companies or associations, debentures," and certain "other securities," was not applicable.[315]

It is important to keep the *Hedqvist* ruling in perspective. It is true that the ECJ accepted that Bitcoin (and by extension other virtual currencies using blockchain) can be used as a means of payment and ruled that it was not justified to treat virtual currencies differently than traditional currencies for VAT purposes since they served the same purpose. What the ECJ did not do, however, was legitimize or "bless" Bitcoin or virtual currency. Advocate General Kokott effectively raised the same point in her opinion. Germany had argued that Bitcoin's high volatility and association with fraud justified treating Bitcoin exchange transactions differently than traditional currency exchange transactions and that as a consequence, Bitcoin exchange transactions should not receive an Article 135 VAT

[305] *Id.*, ¶ 43.
[306] *Id.*, ¶ 44.
[307] *Id.*, ¶ 46 (citing ¶ 31 – 34 of AG's opinion).
[308] *Id.*, ¶ 47.
[309] *See id.*, ¶ 48.
[310] *Id.*, ¶ 49.
[311] *Id.*, ¶ 50.
[312] *Id.*, ¶ 51.
[313] *Id.*, ¶ 52 – 53.
[314] *Id.*, ¶ 54 – 55.
[315] *Id.*, ¶ 56.

exemption.[316] In response, AG Kolkott disagreed that normative considerations had any bearing on a transaction's characterization under EU VAT law, instead maintaining that a transaction's regulatory status and its VAT status were wholly separate concepts:

> [T]he only place for considerations of this kind is the governmental supervision of the financial markets. VAT is independent of this, however. It is clear from the case-law that even if a practice is prohibited under supervisory law, its assessment for VAT purposes is unaffected. Thus, whether bitcoins constitute a "good" or a "bad" currency is irrelevant for the purpose of the present proceedings.[317]

So while the ECJ decided to give Bitcoin and traditional currency the same VAT treatment, it did not, by extension, hold that virtual currencies and traditional currencies would, henceforth, be treated the same for all purposes throughout the realm. It is also important to recall that *Hedqvist* was an Article 267 TFEU preliminary reference, and the only questions before the ECJ were the ones specifically addressed to it by the national court that referred the case. At issue was the VAT treatment of Bitcoin, and not, for instance, whether virtual currencies were in some cosmic sense "legal." Those larger questions were not addressed to the ECJ and were not answered in *Hedqvist*. Indeed, according to Professor Robby Houben at University of Antwerp, because the ECJ's focus was on the categorization of Bitcoin for VAT purposes, its ruling on Bitcoin's status "may not simply be copied in the context of financial regulation."[318]

That said, from an AML/CFT standpoint, several points from *Hedqvist* stand out. One is that it would be consistent with the ECJ's ruling to accept that Bitcoin and similar virtual currencies are "property" for purposes of the 4th AMLD. That is because Bitcoin, as a "means of payment" akin to a traditional currency, must therefore either qualify as an "asset" or "instrument[] in any form including electronic or digital, evidencing title to or an interest in" an "asset," since a "means of payment" that is not either of these would be oxymoronic. As discussed above, the definition of "property" under the Directive expansively covers all assets and instruments evidencing interest in an asset,[319] and criminally-derived "property" is the prerequisite for "money laundering." As such, *Hedqvist* should be read as supporting treating Bitcoin and other virtual currencies as covered by the Directive.

In addition, *Hedqvist* supports another interpretation of the meaning of "funds" under the Directive that differs from the analysis in Chapter II. Interpreting "funds" to encompass virtual currencies would place them within both the Directive's prohibitions against terrorist financing and its suspicious transaction reporting requirements. This would, of course, advance the purpose of the Directive, since permitting ISIS/ISIL terrorists to raise funds in Bitcoins simply because they are not traditional "coins" would be senseless. While it is logical to read the term "funds" under the Directive in a manner consistent with similar directives – which should mean that Bitcoins are not literally "funds" – the ECJ demonstrated in *Hedqvist* that it will interpret terms teleologically: "in the light of the context in which it is used and of the aims and scheme" of the directive in which the term appears, particularly when the different language versions clash. While a straight textual analysis (in English) yields the result that only collection of "funds" for terrorists constitutes "terrorist financing," looking at different language versions, such as Swedish and German, supports a different answer. The Swedish version of the Directive defines "terrorist financing" in terms of

[316] Opinion of Advocate General Kokott, delivered on 16 July 2015, ¶ 41 - 44.

[317] *Id.*, ¶ 44 (internal citation omitted).

[318] Professor Dr. Robby Houben, *The CJEU's view of whether Bitcoins are a currency: a Belgian perspective*, I.C.C.L.R. 2016, 27(3), 61-64, 64 (2016).

[319] Article 3(3).

"*insamling av medel*."[320] The key word here is "*medel*." Unlike the English word "funds," *"medel*" has a broader meaning, encompassing concepts like "resources" or "means." Recital 13 in the Directive in fact uses the term "*medel*" in place of the English word "means" – twice. Similarly, the German definition of "terrorist financing" uses the phrase "*finanzieller Mittel*" instead of "funds," which means something like "financial means" or "financial resources" – again a broader concept than "funds." Other languages, in contrast, use a word etymologically related to "funds," like the French "*fonds*," the Spanish "*fondos*," and the Italian "*fondi*."

Because textual analysis is not possible given the inconsistent terminology employed across different language versions, it is arguably incorrect to read the word "funds" in the 4th AMLD in the sense of "funds" as defined in other related directives. Rather, "funds" should be interpreted in light of what the Directive itself is trying to accomplish. Since as stated above allowing bad actors to finance terrorism with virtual currencies would undercut the objectives of the Directive, the correct reading of "funds" should be in the broadest sense of "all means of payment." Since *Hedqvist* tells us that Bitcoin (and by extension other blockchain-based virtual currencies) is a "means of payment," that case supports treating Bitcoin as falling under the term "funds" for purposes of the Directive.

Besides supporting a caselaw fix to the narrow definition of "terrorist financing" in the Directive, *Hedqvist* preempts arguments that could have created difficulty for virtual currencies in the EU. Importantly, under *Hedqvist*, Bitcoin is not a "security." While on one level this seems self-evident, there should now be no need to consider whether, despite what appeared to be obvious, virtual currencies could fall under the myriad regulations affecting securities.

Finally, it is worth noting that had the ECJ ruled otherwise in *Hedqvist* and found that exchanges of Bitcoin for traditional currency and vice versa were subject to VAT, this would have harmed the development of a legal virtual currency industry in the EU by raising transaction costs considerably. Interestingly, and in contrast to the U.S. approach which very well might have addressed the issue head on, the ECJ never appears to have weighed the economic consequences of its ruling. It is fortunate (and fortuitous) that the different language versions contained ambiguity regarding whether only legal-tender currencies fell within the VAT exemption, since otherwise the ECJ may come out quite differently.

Overall, *Hedqvist* is an important case for virtual currencies in the EU because it involved little fanfare. There was no crying or gnashing of teeth by the ECJ over what it meant for virtual currencies to be treated the same as traditional currencies. Instead, the ECJ just went ahead and did so, at least with regard to the one particular, narrow issue before it. In holding as it did, the ECJ may have allowed a revolution to continue.

[320] Article 1(5).

IV. AML/CFT Regulation of Blockchain-Based Virtual Currency Under EU Law

A. *The Current Situation*

This is an interesting time for AML/CFT regulation of virtual currencies in the EU, mostly because the 4th AMLD, like the 2012 FATF Recommendations that they are based on, failed to take them into account. At all. The phrases "virtual currency" (or "currencies"), "Bitcoin," and "blockchain" do not appear once in the Directive. Nor do those words appear in the FATF Recommendations, except once in the title of a guidance paper in a later-added annex of FATF guidance documents.

Unless something is done about this, it will be necessary for obligated entities, FIUs, Member States, and the ECJ to try to extend the Directive to areas it was not designed to go, or simply treat virtual currencies as outside the reach of AML/CFT laws and watch the experiment unfold. As mentioned at the beginning of this thesis, however, various EU bodies, including the Commission, the EU Parliament, and the ECB have begun actively thinking about how to mesh AML/CFT regulation with virtual currencies. The FATF has as well. What follows is a summary of the current situation.

i. The European Commission

As mentioned in Chapter I, the European Commission's February 2, 2016 "Action Plan to strengthen the fight against the financing of terrorism" contains several recommendations for conforming AML/CFT laws with virtual currencies. In its Action Plan, the Commission starts by reciting the usual "good news/bad news" problem of virtual currencies: financial innovation can bring benefits but can also allow terrorists to fund themselves covertly.[321] The anonymity of virtual currencies, as the Commission wisely notes, is the real issue.[322] However, according to the Commission, "[v]irtual currencies are currently not regulated at EU level," virtual currency exchange platforms do not currently fall under the Directive, and "there is no reporting mechanism [applicable to virtual currency exchange platforms] equivalent to that found in the mainstream banking system to identify suspicious activity."[323] The Commission's plan, "as a first step," is to amend the Directive to cover virtual currency exchange platforms so that customer due diligence requirements would apply whenever virtual currency is exchanged for "real" currency, and vice versa.[324] Therefore, even though virtual currency "closed-loop" transactions are anonymous, that anonymity would end whenever a virtual currency user wanted to cash in his virtual chips for real money. The Commission would also seek to apply the Payment Services Directive (PSD) licensing and supervision rules to virtual currency exchange platforms in order to have "better control and understanding of the market,"[325] though the Commission gives no further details. Virtual currency "wallet providers" might be regulated in the future as well,[326] again with no further details given. The Commission states it will present its proposed amendments by the 2nd quarter of 2016.

[321] Section 1.

[322] *Id.* ("For innovative financial tools, it is critical to be able to manage the risks relating to their anonymity, such as for virtual currencies. Critical to this question is less the forms of payment themselves, but rather whether they can be used anonymously").

[323] Section 1.2.

[324] *Id.*

[325] *Id.*

[326] *Id.*

The European Council has weighed in on the Commission's work in this area, issuing on February 12, 2016 a statement entitled "Council conclusions on the fight against the financing of terrorism."[327] The Council emphasized the "importance of achieving rapid progress on legislative actions identified by the Commission," including amending, as soon as possible, the 4th AMLD to address virtual currencies (and possibly amending the Payment Services Directive as well).

The Commission's proposed amendments to the 4th AMLD have not (at the time of writing) been released. An Inception Impact Assessment prepared by DG JUST – B Task Force Financial Crime on April 7, 2016[328] provides, however, some insight into the Commission's progress. Citing the Action Plan and the Commission's proposal to submit amendments to the Directive, the Assessment notes that one of the "main drivers, the issue and the problem to be tackled" included that it is difficult to trace virtual currency use, that terrorists could exploit this difficulty to divert funds into the EU anonymously, and admits, rather stunningly, that "[v]irtual currency transfers are currently not monitored in any way by public authorities within the EU."[329] The Assessment further cites EU-wide level of support for AML/CFT regulation of virtual currencies:

> [T]he FATF and EBA have issued recommendations that – at least - virtual currency exchange platforms should be brought within the scope of AML/CFT supervision. Nearly all EU Member States have issued warnings on the use of virtual currencies, and from the survey conducted, it appears that a significant number (27) of Member States support an EU framework on this. This initiative aims to be a first step in mitigating the recognised AML/CFT risks related to virtual currencies.[330]

The impact of regulation is naturally considered as well. The effects of the proposed regulations on virtual currency exchange platforms is assessed as "quite limited," and the effects on competitiveness and innovation are punted as "currently not clear."[331] (One gets the impression that the Commission has not given these vital points much thought yet.)

It is interesting that the Commission so readily concedes that virtual currencies do not fall under the Directive, since, as discussed above, under current definitions they should qualify as "property" capable of being laundered and may qualify as "funds" capable of contributing to "terrorist financing." So while no one thought to use the magic words "virtual currency" when drafting the Directive, the language actually used may well already encompass the concept. Additionally, the Commission assumes that virtual currency exchange platforms are unregulated under the Directive but this assumption can be challenged. The is because virtual currency exchange platforms could be "financial institutions,"[332] one of the listed "obligated entities" under the Directive.[333] A look at the definition of "financial institution" gives the following: "an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council (23), including the activities of currency exchange offices (bureaux de change)."[334] Annex I of

[327] http://www.consilium.europa.eu/en/press/press-releases/2016/02/12-conclusions-terrorism-financing/

[328] http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_just_054_amld_en.pdf

[329] *Id.* at p. 2.

[330] *Id.* at p. 7.

[331] *Id.* at 7-8.

[332] Article 3(2).

[333] Article 2(1)2.

[334] Article 3(2)(a).

Directive 2013/36/EU,[335] points (4) and (5), consist of the following activities:

> 4. Payment services as defined in Article 4(3) of Directive 2007/64/EC.
>
> 5. Issuing and administering other means of payment (e.g. travellers' cheques and bankers' drafts) insofar as such activity is not covered by point 4.

The first question, then, is whether virtual currency exchange services could qualify as "payment services" under Article 4(3) of the Payment Services Directive, which is defined as "any business activity listed in the Annex." The short answer is no. That is because none of the business activities listed in the Annex would encompass exchanging virtual currency for traditional currency or vice versa. The underlying terms in the Annex, such as "payment account," "money remittance," and "payment instrument" are too narrowly defined to capture the non-traditional, decentralized nature of virtual currencies, and it is simply not possible to plausibly read virtual currency exchange as covered by the Annex.

That said, point (5) of Annex I of Directive 2013/36/EU might work. Point (5) asks us first to determine whether the activity is covered by point (4). As argued above, it is not. Because the activity is not covered by point (4), it can be covered by point (5), *if* it consists of "[i]ssuing and administering other means of payment (e.g. travellers' cheques and bankers' drafts)." We know from *Hedqvist* that virtual currency like Bitcoin is a "means of payment." The only remaining question is whether a virtual currency exchange platform "issues and administers" virtual currency when it sells virtual currency for traditional currency. Those terms appear not to be defined, providing more leeway to argue about what they should mean. On the one hand, the examples given of travelers checks and bankers' drafts suggest that the "other means of payment" is envisioned as an obligation created by the financial institution itself, which if so would exclude virtual currencies (which the exchange platforms do not themselves create). One commentator, interpreting the UK version of point (5), takes this view in the context of Bitcoin, arguing that it is:

> intended to include payment products such as paper-based vouchers, however, it is unlikely that the scope of this provision could be extended so as to include BTCs, which are conceptually not a payment service but rather a form of currency.[336]

Under this view, only a centralized virtual currency could be "issued" by a financial institution, i.e. the financial institution that centrally creates and controls the virtual currency. On the other hand, the "e.g." suggests that those two examples were only supposed to taken as <u>examples</u> of the subset of "other means of payment" and not as limitations, and that anything that is an "other means of payment" counts, whether it is created by the undertaking or not. The query then is whether a virtual currency exchange platform "issues" virtual currency to the customer in exchange for real currency and whether it "administers" the virtual currency during the transaction. It is plausible to argue that does, if "issues" and "administers" are interpreted broadly to mean that the exchange platform provides its customers with virtual currency and in doing so takes part in the decentralized administration of the virtual currency. It is, at least, a colorable argument.

Which is to say that the Commission may have been too quick in taking the position that, in effect, virtual currency exchange platforms are not "financial institutions" that are

[335] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.
[336] Stokes, *supra* n. 96, at 228.

already "obligated entities" under the 4th AMLD. Be that as it may, however, the long and short of it is that the Commission has already taken the position that it believes that further amendments to the Directive (and possibly the Payment Services Directive) are in order to cover virtual currencies and would be hard-pressed to backtrack now. Regardless of how this particular issue plays out, however, a comprehensive AML/CFT approach to virtual currencies is still lacking from the Commission. What such an approach might look like is discussed below.

ii. The European Parliament

The European Parliament as a whole has not yet weighed in on AML/CFT regulation of virtual currencies. Two committees, however, have recently done so.

The European Parliament's Committee on Economic and Monetary Affairs (ECON) has taken an active role. ECON held a public hearing on January 25, 2016 devoted to the subject at which a number of advocates of the technology spoke.[337] Rapporteur Jakob von Wiezsäcker acknowledged the potential transformative nature of virtual currency while noting the potential for AML/CFT risks. The Committee heard from a number of speakers including Siân Jones,[338] founder of the European Digital Currency & Blockchain Technology Forum (EDCAB), Jeremy Millar, a partner with Magister Advisors, Primavera De Filippi, a permanent researcher at the National Centre of Scientific Research in Paris, and Olivier Salles, an expert at the European Commission, who acknowledged that the Commission was exploring AML/CFT regulation of virtual currencies.

Following the hearing, ECON issued the nine-page Draft Report on Virtual Currencies first mentioned in Chapter I. In the draft report, ECON accepted that the risks of money laundering and terrorist financing using virtual currencies were not mere fantasy but rather "significant," and in fact deserved increased regulatory capacity.[339] Existing regulations did not take virtual currencies into account, however, meaning additional regulation will be needed. The appropriate regulatory response should be proportional: protecting early-stage innovation "while taking seriously the regulatory challenges that the widespread use of VCs and DLT [distributed ledger technology, i.e. blockchain] might pose."[340] While ECON agreed with the Commission's plan to amend the 4th AMLD to make virtual currency exchange platforms "obligated entities," it also urged it to extend the Directive to wallet providers if the use of virtual currencies ever became a closed-loop system: i.e., if users no longer needed to convert virtual currency into traditional currencies because the use of virtual currencies became commonplace.[341] The draft report additionally called for the creation of a task force called "TF DLT" to investigate and address the need for new virtual currency regulation.[342] On April 26, 2016, ECON voted overwhelmingly in

[337] http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160125-1500-COMMITTEE-ECON

[338] In urging against AML/CFT regulation, Jones claimed that the use of virtual currencies for money laundering was insignificant, arguing that use virtual currencies accounted for "less than 100,000th of 1% of global money laundering" and that the Euro accounted for money laundering at a rate 92 times that of virtual currencies. Jones advocated for no AML/CFT regulation for virtual currencies but stated that if such regulation was considered, that it should be limited to targeting the "gateways" where the traditional financial system intersects with the virtual system and not users of virtual currencies themselves. *See* https://polcms.secure.europarl.europa.eu/cmsdata/upload/a5b25cc8-76a4-4086-bbef-f83aee1b3684/Sian%20Jones%20EDCAB%20Statement%20FINAL%20rev%2020160125-3.pdf. While Jones' position might be open to debate, the point is that the obvious AML/CFT problems that virtual currencies present are not universally acknowledged.

[339] *See* p. 5-6, 8.

[340] P. 7.

[341] *Id.*

[342] *Id.*

support of establishing the task force, with the report's author, Jakob von Wiezsäcker, explaining:

> To avoid stifling innovation, we favour precautionary monitoring instead of pre-emptive regulation. But, IT innovations can spread very rapidly and become systemic. That's why we call on the Commission to establish a taskforce to actively monitor how the technology evolves and to make timely proposals for specific regulation if, and when, the need arises.[343]

The report itself awaits a vote by the full European Parliament, and if approved (as seems likely) it will be sent to the Commission.[344]

In addition to ECON, the Committee on the Internal Market and Consumer Protection (IMCO) has entered the debate. IMCO authored an Opinion on virtual currencies[345] for the benefit of ECON on April 21, 2016. The overall tone of the report was caution: the need to make sure regulation did not displace innovation, especially given the early stage of virtual currency's development and the many economic benefits the technology could offer. In the Opinion, IMCO admitted that virtual currencies might present money laundering and terrorist financing risks but claimed, somewhat credulously, that there is "little evidence that VCs have been widely used as a payment vehicle for criminal activity."[346] IMCO called on the Commission to "to develop a coherent and comprehensive strategy at EU level."[347] Interestingly, IMCO urged the virtual currency industry to comply with AML/CFT regulations vis-à-vis virtual currency exchange platforms and other areas where the virtual and traditional currency sectors interface even though the Commission had not yet amended the 4th AMLD,[348] perhaps suggesting that waiting for official action was unwarranted. IMCO also asked the Commission to "evaluate and consider" amending the 4th AMLD to cover virtual currency exchange platforms.[349]

Interestingly, on April 19 to April 21, 2016 the European Parliament was the site of a virtual currency exhibition called "Virtual Currencies and Blockchain Technology: Europe's Future" that was hosted by MEP Syed Kamall and sponsored by The Cobden Centre and EDCAB.[350] There appears to have been dialogue between EDCAB and the IMCO report's rapporteur, Ulrike Trebesius MEP, with Trebesius even "visit[ing] EDCAB's Exhibition at the European Parliament straight after the vote on the report to discuss its outcome."[351] EDCAB has advanced the position that the money laundering and terrorist financing risks from virtual currency are negligible,[352] which given the examples of Silk Road and ransomware extortion seems unsupportable even if criminals far more frequently use ordinary, no-tech cash to launder proceeds. IMCO appears to have partially accepted this

[343] European Parliament Press Release, *Set up taskforce to oversee virtual currencies, ECON MEPs say* (April 26, 2016), at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160425IPR24684/20160425IPR24684_en.pdf

[344] *Id.*

[345] Rapporteur: Ulrike Trebesius, Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Economic and Monetary Affairs on virtual currencies (2016/2007(INI)) (21 April 2016), at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-577.006+02+DOC+PDF+V0//EN&language=EN

[346] P. 3. Given the Silk Road and ransomware examples, this is an odd claim.

[347] P. 4.

[348] P. 4-5.

[349] *Id.*

[350] http://edcab.eu/blockchain-expo/virtual-currency-blockchain-expo-in-european-parliament

[351] EDCAB, First vote on virtual currencies report passed with near unanimity in European Parliament, at http://edcab.eu/blockchain-expo/ulrike-trebesius-mep-supports-virtual-currencies-in-the-european-parliament

[352] *See* n. 338, *supra*.

position, claiming in the report that there was "little evidence" of AML/CFT misuse of virtual currencies. This misses the point, however, since the real issue is what will happen once virtual currencies become mainstream. Unless they can be adapted to AML/CFT norms, then the naïve mantra about "little evidence" of criminal misuse will fall flat.

To sum up the current European Parliament approach to virtual currencies, there is much to commend. Knee-jerk reactions to Bitcoin as a tool of terrorists and criminals has not occurred,[353] while on the other hand the AML/CFT risks have not been completely downplayed. The European Parliament appears to recognize the huge economic promise that virtual currencies offer, and has made a smart move with the creation of a dedicated, expert task force that will be positioned to offer constructive suggestions as to how to conform virtual currencies with AML/CFT regulation. The call by IMCO for a "coherent and comprehensive strategy" by the Commission is also positive, since merely attempting to regulate virtual currencies by extending existing approaches would fall short.

However, missing from the Parliament's approach, and for that matter from the Commission's, is a solid appreciation that virtual currencies, as currently designed, are uniquely suited to bypassing AML/CFT controls and undoubtedly attract criminals for that exact reason. In effect, the "incumbent money problem" raised earlier – why switch from a perfectly good fiat currency like the euro or dollar to a volatile virtual currency with bubble-like pricing characteristics – should raise red flags for lawmakers, since it suggests that there may be an alarming reason underlying what would otherwise not make much sense: i.e., why switch? Namely, the costs of switching to virtual currencies should currently outweigh the benefits, unless the benefits are intangible and ideological (e.g. libertarians who despise government-issued and controlled currency or tech-nerds who find virtual currencies cool), the purpose is financial speculation, or the purpose is being able to send and receive payments anonymously and without intermediaries – in other words, free from AML/CFT scrutiny. A cynic might even suggest that the entire point of a virtual currency that is anonymous and decentralized is to act as a workaround to the international AML/CFT system, even if the broader technology also offers other real solutions such as low-transaction cost international money transmission. There is a reason, after all, that Silk Road drug dealers and cyber-ransom gangs use virtual currency (particularly Bitcoin) – and it is not ideological. Put simply, the AML/CFT problem with virtual currencies like Bitcoin is the particular nature of their current protocols, and may unfortunately be a major reason for their ascendency.

A proposal for what a comprehensive strategy might look like for solving this problem will follow the discussion below about the recommendations from the ECB and FATF.

iii. The European Central Bank

The European Central Bank issued its latest report on "virtual currency schemes" in February 2015,[354] a follow-up to its October 2012 report on the subject. As the most recent "word" from the ECB, the February 2015 report is considered below as it relates to AML/CFT regulation. Most of the report focused on other aspects other than AML/CFT

[353] In partial contrast to the U.S. *See* Andy Greenberg, *Senator Calls For Bitcoin Ban In Letter To Financial Regulators*, Forbes (Feb. 26, 2014), at http://www.forbes.com/sites/andygreenberg/2014/02/26/senator-calls-for-bitcoin-ban-in-letter-to-financial-regulators/#3cbdaf944639; *see also* Aaron Timms, *BitLicense: Legitimacy for Digital Currencies, but Will Innovation Suffer?*, Institutional Investor (June 22, 2015)(quoting influential New York Senator Charles Schumer as deriding Bitcoin "an online form of money laundering used to disguise the source of money").

[354] https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

regulation, and covered a wide range of topics impacting the ECB's mandate, such as price stability, financial stability, and payment system stability.

Citing virtual currencies' international transmissibility, accessibility through the internet, and enhanced anonymity as factors enabling them to be used for illegal purposes, the ECB identified a number of AML/CFT risks.[355] One is that there is no centralized institution "in charge," either with regard to the proper functioning of the virtual currency or to the oversight of users. Users may transact without their true identities being traceable, even if the blockchain itself provides historical traceability of public keys. Second, the decentralized way in which transactions are "cleared" – which the ECB describes in terms of "complex infrastructures to transfer funds or execute payments involving several (not always identifiable) entities which are often spread across several countries" – makes it hard to apply AML/CFT laws. Third, the international nature of virtual currencies and the internet facilitates operating virtual currency "intermediaries" in jurisdictions beyond EU reach that do not have strong AML/CFT enforcement or laws.

While the ECB's focus in its report was not AML/CFT regulation *per se*, and the ECB noted that its own authority did not extend to developing the necessary regulations in this area, it is still worth noting that the AML/CFT risks identified by the ECB, while a short list, go to the heart of the problem: anonymity plus the absence of trusted, centralized intermediaries potentially undercuts effect AML/CFT controls.

iv. The Financial Action Task Force

As mentioned above, FATF has released two documents that influence the direction of EU AML/CFT regulation of virtual currencies. Building off its earlier *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* from 2014, FATF released *Guidance for a Risk-Based Approach to Virtual Currencies*[356] in June 2015. In the 2015 *Guidance*, FATF stated that it "recognizes financial innovation," but nonetheless noted that virtual currencies present AML/CFT risks that must be properly dealt with. In addressing those risks, FATF took an incremental approach, focusing its attention first towards the "points of intersection that provide gateways to the regulated financial system," in particular virtual currency exchange providers.[357] As the FATF continues to observe how virtual currencies evolve, it will update its approach, including cataloging "best practices" regarding AML/CFT that emerge as various jurisdictions develop regulatory approaches.[358] FATF plans to delay addressing the AML/CFT risks that cannot be mitigated by regulating virtual currency exchange providers, such as virtual currency transfers exceeding a certain value amount or user-to-user transfers that do not result in traditional currency exchange, until the "longer term."[359]

The 2015 *Guidance* noted that FATF's earlier risk assessment in its 2014 report suggested that only virtual currencies that can be exchanged for traditional currencies represent a near-term risk of money laundering and terrorist financing. As a result, FATF recommended devoting AML/CFT efforts to these virtual currencies instead of also targeting non-convertible virtual currencies. Since a virtual currency that could not be exchanged for traditional currency would naturally have minimal AML/CFT utility, this is sound, if not somewhat obvious, reasoning. Notably, and in contrast to the Commission's assumptions, FATF suggested that virtual currency exchange providers and other virtual currency-related

[355] *Id.*, p. 28.

[356] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

[357] *Id.*, p. 3.

[358] *Id.*

[359] *Id.*

businesses may already qualify as "financial institutions" as defined by FATF because they, *inter alia*, "issu[e] and manag[e] means of payment," and would therefore be subject to AML/CFT laws based on the FATF Recommendations.[360] These would, presumably, include the EU's 4th AMLD, a point FATF does not explicitly address.

FATF issued a number of AML/CFT recommendations in the 2015 *Guidance*. The Commission has largely followed FATF's approach even though the Commission's determination that amendments to the 4th AMLD are necessary to bring virtual currency exchange providers within its fold does not seem to mesh with FATF's position. Among FATF's recommendations are that jurisdictions undertake a dedicated risk assessment which, FATF suggested, would lead them to extend AML/CFT regulations to virtual currency exchange platforms.[361] In discussing the risk assessment, FATF contemplated that some jurisdictions may choose to simply ban virtual currencies, an option that FATF took no particular position on other than to warn of possible unintended consequences such as creating a black market. Other recommendations included that: national regulatory coordination be applied to AML/CFT policies towards virtual currencies; virtual currency exchange providers be licensed and regulated; cross-border wire transfer regulations be applied to virtual currency exchange providers; jurisdictions figure out how to solve the enforcement problems created by user anonymity; and international cooperation in AML/CFT enforcement be extended to virtual currencies.[362] FATF also issued several specific recommendations as to extending AML/CFT requirements to virtual currency exchange providers. These included requiring virtual currency exchange providers to undertake risk assessments, customer due diligence measures, transaction monitoring, record-keeping, and suspicious activity reporting.[363] FATF additionally encouraged the development of new technologies to facilitate AML/CFT compliance vis-à-vis virtual currencies, including third-party identification systems managed by trusted custodians, applications that limit transactions or build customer risk profiles, or even alt-coin virtual currencies specifically engineered to have AML/CFT features:

> Innovation relevant to AML/CFT compliance may take the form of improving existing VC protocols or developing entirely new VCs, built on fundamentally different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring.[364]

As will be argued below, this later solution offers particular promise, as it would keep the groundbreaking features of virtual currency while mitigating the AML/CFT problems created by the native and untamed varieties currently in the wild – including Bitcoin.

B. *The Problem and a Proposed Solution*

i. The Problem

While efforts to regulate virtual currency exchange providers as "obligated entities" subject to the 4th AMLD could, in the near term, mitigate some of the wide-open AML/CFT risks posed by Bitcoin and other virtual currencies, a comprehensive long-term solution is needed. First, a fairly obvious problem (and one which others have raised) with burdening

[360] *Id.* at 6-7.
[361] *Id.* at 9.
[362] *Id.* at 8-11.
[363] *Id.* at 12-14.
[364] *Id.* at 14.

virtual currency exchange providers, many of which are start-ups, with the costs of full-blown CDD and other AML/CFT responsibilities (i.e. suspicious activity reporting, record-keeping, risk assessments, internal controls, etc.) is that doing so could stifle innovation and growth. Forcing these entities to act as mature financial institutions may, in other words, be counterproductive if not futile, since compliance costs it could push reputable actors out of the market. But beyond this straightforward objection, the problem with allowing virtual currencies to continue to develop without a comprehensive AML/CFT regulatory solution is that without one, virtual currency use could develop in one of two ways: it could stagnate, or it could become widespread – but in the absence of a comprehensive AML/CFT regulatory solution. Either would be problematic.

First, without a comprehensive AML/CFT solution, virtual currency use could stagnate, perhaps ironically as a result of a regulatory Catch-22. *Viz.*, virtual currency use may never become widespread unless there is a comprehensive AML/CFT fix, but there may be no regulatory pressure for one unless virtual currency use first becomes widespread. For those who believe that blockchain-based virtual currency represents a major innovation, any such regulatorily-induced failure to thrive would be a sad waste of potential.

Why might the lack of a comprehensive AML/CFT approach contribute to stunted virtual currency growth? Several possible reasons. For example, continued regulatory uncertainty may deter potential (non-criminal) users and businesses from anything more than half-hearted experimental dabbling in virtual currencies, delaying full-scale adoption until it is known what a mature AML/CFT regulatory approach will look like – and whether all or just some virtual currencies will ultimately be legal and what the costs of AML/CFT compliance will be. The ensuing inertia would be unable to overcome incumbent currency problem, with the result being a never-ending holding pattern.

As another example discussed below in more length, comprehensive AML/CFT regulation that "blesses" certain virtual currencies having protocols or other technical features specially-engineered to be AML/CFT-compliant could imbue such virtual currencies with something like intrinsic value, especially if regulatory "blessing" was a difficult and costly process that could not be readily copied by free-riders. Intellectual property rights could play a key role in preventing free-riding, allowing the protocols to continue be transparent though no longer freely reproducible by alt-coins. By creating a costly barrier to entry, AML/CFT regulation aimed at requiring AML/CFT-compliant protocols could kill two birds with one stone: fixing the AML/CFT problems with virtual currencies like Bitcoin while reducing the "blessed" virtual currency's volatility and risk of collapse by making it "special" in comparison to its competitors. No longer reliant on self-referential network effects for its value, a virtual currency "blessed" because it had special, proprietary AML/CFT-compliant protocols would encourage acceptance by a wider public than fintech nerds, criminals, and other core true-believers. However, there is a flipside: if AML/CFT regulation instead follows an incremental, wait-and-see approach that focuses first on virtual currency exchange providers while delaying further regulation until developments force the issue, then the lack of intrinsic value problem highlighted above could prevent wider adoption of virtual currencies, which in turn would reduce the felt need to adopt the sorts of comprehensive AML/CFT regulations that could actually encourage wider virtual currency adoption. The end result would be a stagnant status quo.

As a final example, subjecting virtual currency exchange providers to CDD requirements without further comprehensive AML/CFT regulation would help de-anonymize users wishing to trade in Bitcoin for cash, but would still not allow scrutiny of the underlying transactions that generate the Bitcoin, especially given technical measures like mixing services/tumblers that can obfuscate tracing attempts. While CDD requirements would require virtual currency exchange providers as obligated entities to understand the business and the underlying context of its clients, it is questionable in practice how reliable or useful the information collected would be to FIUs if corrupt clients could costlessly interpose as many dummy steps in the blockchain as they wished in order to thwart meaningful CDD. The result may be that virtual currency exchange providers would generate a high volume of suspicious transaction reports (which they would have to do if they had at least "reasonable grounds to suspect" that the funds were tainted), leaving it to FIUs to sort through the mess. This continued lack of transparency could result in Bitcoin and other virtual currencies retaining the stigma of being associated with criminality, harming their attractiveness to reputable users and businesses. Financial institutions and other actors would similarly be scared off both on reputational grounds and from fear of the harsh sanctions possible for obligated entities that are too cozy with criminally-derived funds.

It is of course hard to predict whether the lack of early, comprehensive AML/CFT regulation will actually harm virtual currencies' widespread acceptance. The possibility, though, should not be discounted. Ironically, rather than stifling virtual currencies, robust AML/CFT regulation could actually be just what is needed to help them flourish. If so, the stereotypical narrative about early regulation harming new innovation would in fact be dead wrong, at least in this instance. That is, at least, an intriguing thought.

The other possibility of course is that lack of comprehensive AML/CFT regulation does not harm virtual currencies' development. If not, then bringing virtual currency exchange providers under the 4th AMLD could be a short-term solution, at least if doing so does not make them unduly unprofitable. At this early stage, virtual currency exchange providers can function as trusted intermediaries having AML/CFT responsibilities because merchants that accept virtual currency are relatively rare and exchanges of virtual currency for traditional currency are unavoidable.[365] The idea is that "because neither bitcoin nor digicash or other private currency can be used within exclusively closed-loop system, they are vulnerable to effective regulation on the periphery."[366] Bringing virtual currency exchange providers within the AML/CFT regulatory system as entities required to undertake CDD is in fact something of a panacea offered by many commentators if not the EU itself.

It is, however, a shortsighted solution. That is because as virtual currency use becomes more widespread, there will be less need for money launderers or terrorist financers to bother exchanging laundered Bitcoin or other virtual currency for cash instead of simply spending virtual currency directly on goods and services.[367] Once this happens, virtual

[365] *See* Laura Shin, *This Man Has Been Living On Bitcoin For 3 Years*, Forbes (Jan. 7, 2016), at http://www.forbes.com/sites/laurashin/2016/01/07/this-man-has-been-living-on-bitcoin-for-3-years/#2620a58c4b8f (man paid his salary solely in Bitcoin explains how he purchases items:

> I pay my roommate who pays our rent in dollars. If I'm out at a restaurant, I'll have a friend foot the bill, and then I'll pay them in Bitcoin. Also, Coinbase recently launched the Shift debit card, which allows you to spend Bitcoin anywhere that merchants accept cards, but it actually pulls Bitcoin from your Coinbase account. The merchant does not see Bitcoin. Shift sells your Bitcoin and pays that merchant dollars.)

[366] Victor Dostov and Pavel Shust, *Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?*, Journal of Financial Crime, Vol. 21 No. 3, 2014, pp. 249-263, 254.

[367] *See id.* (stating "Over time, there's going to be more of a closed loop where I receive my salary in Bitcoin, I pay someone for a good or service in Bitcoin, and they source their supplier in Bitcoin. That's when the transactional benefits of Bitcoin become apparent"). *See also* Stokes, *supra* n. 96, at 231:

> In principle, a BTC [Bitcoin] could remain in circulation indefinitely without being converted into real-world currency. This would allow BTC transfers to avoid money laundering controls if those controls were solely focused on the exchange mechanism. However, given the limited acceptance of BTCs as payment, businesses, it can be suggested, will only accept BTCs due to their ability to be exchanged for real-world currency. This allows a system of anti-money laundering regulation to

currency exchange providers will become obsolescent and will be increasingly bypassed altogether. This will precipitate an AML/CFT crisis, as a perhaps significant part of the economy will be invested in an anonymous means of international money transmission that no longer requires intermediaries. Because the current AML/CFT system requires both intermediaries acting as informants and customers whose identities (and even motives) are known, virtual currencies with Bitcoin-like protocols will be wholly incompatible with the AML/CFT system that has evolved since the 1980s. One of the other will have to go.

The survivor would likely be the international AML/CFT regime, given the current political climate, the increasing acquiesce to government monitoring of everyday life, and the (false) sense that AML/CFT laws have always been with us and are a natural component of the global financial system. Assuming that AML/CFT laws do not yield to virtual currencies, then it will be AML/CFT-incompatible virtual currencies that will be the casualties. But once AML/CFT-incompatible virtual currencies are adopted on a widespread basis, it will be too late to painlessly step back. If decentralized and anonymous virtual currencies are allowed to mature, some Member State governments or even the EU might find the AML/CFT threat they pose as closed-loop payment methods unbearable and seek to ban them unless they undergo “hard fork” protocol changes to make them acceptable from a AML/CFT standpoint, such as by embedding user identification information in public keys. But because the protocols to open-source virtual currencies like Bitcoin can only be altered by consensus, it may prove difficult if not impossible as a practical matter for governments to force a protocol change. The alternate then would be to ban their possession, use, or exchange in the EU.

Banning such virtual currencies at an advanced stage would present both economic and legal challenges, however, especially if they are allowed to reach significant market capitalizations. Rather obviously, wiping out vast amounts of stored wealth via a ban of virtual currencies would be an economic nightmare and the damage to financial innovation would be immense. It is also questionable from a legal standpoint whether such measures would be in accordance with EU law, the Treaties, and the Charter of Fundamental Rights, especially when there are better ideas that could have been considered earlier on.

While it is unclear whether a ban of Bitcoin or another anonymous virtual currency would be legally permissible in the name of AML/CFT goals, the CJEU caselaw offers some guidance. In a March 2016 preliminary ruling which interpreted the Third Anti-Money Laundering Directive,[368] *Safe Interenvios, SA v Liberbank, SA and Others,*[369] the ECJ noted that a Member State may legislate in a manner restricting the fundamental freedoms (in this case the freedom to provide services) if the restriction:

> reflects an overriding reason in the public interest and that interest is not already safeguarded by the rules to which the service provider is subject in the Member State in which he is established, and in so far as it is appropriate for securing the attainment of the aim which it pursues and does not go beyond what is necessary in order to attain that aim.[370]

The ECJ further reiterated that “preventing and combating money laundering and terrorist financing constitute a legitimate aim capable of justifying a barrier to the freedom to provide

> focus upon the BTC exchange businesses, **although the situation would be different if the BTC ever becomes universally accepted**.

(emphasis added).

[368] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

[369] Case C-235/14 *Safe Interenvios, SA v Liberbank, SA and Others* [2016] EU:C:2016:154.

[370] *See id.*, ¶ 100.

services" under Article 56 TFEU.[371] The ECJ additionally held that AML/CFT measures had to be "balanced against the protection of other interests, including freedom to provide services."[372] National AML/CFT legislation, according to the ECJ, "is appropriate for securing the attainment of the aim pursued if it helps to reduce the risk and reflects the concern to attain that aim in a consistent and systematic manner," such as "when it identifies, in accordance with an appropriate risk assessment. . . a high risk with respect to, inter alia, a type of. . . product."[373] While the Directive permits Member States to adopt stricter AML/CFT measures than those in the Directive, the measures adopted must be proportionate, especially in relation to other rights protected under EU law, including the protection of personal data under Article 8 of the Charter of Fundamental Rights, competition law, and other fundamental rights as reflected in the Charter.[374] If there are less restrictive means of obtaining the same objective, then proportionality may not be demonstrated.[375] In determining proportionality, the "level of protection" that the Member State seeks must be compared to the "identified level of risk of money laundering or terrorist financing."[376] A proper risk assessment is in fact vital to a proper proportionality analysis.[377]

In *Jyske Bank Gibraltar Ltd*,[378] a preliminary reference case cited by the ECJ in *Safe Interenvios* also involving the Third Anti-Money Laundering Directive, the ECJ stated that "the combating of money laundering, which is related to the aim of protecting public order, constitutes a legitimate aim capable of justifying a barrier to the freedom to provide services."[379] In addition, "measures which restrict the freedom to provide services may be justified by the aim which they pursue only if they are suitable for securing the attainment of that aim and do not go beyond what is necessary in order to attain it."[380] The ECJ additionally repeated recitals from the Third Anti-Money Laundering Directive that emphasized the paradox of AML/CFT: free movement of money threatens the foundations of an internal market partially based on that freedom.[381] As later restated by the ECJ in *Safe Interenvios,* because AML/CFT laws have not been completely harmonized at the EU level, Member States can enact stricter rules than those in the Directive, if these stricter rules "meet an overriding requirement relating to the public interest. . . not already safeguarded" by a service provider's home state, and if the restriction is "appropriate for securing the attainment of the aim which it pursues and does not go beyond what is necessary in order to attain it."[382] As on commentator has noted, *Jyske Bank Gibraltar* shows that the ECJ views AML/CFT laws as an EU-level interest that can justify restrictions by Member States on fundamental freedoms and human rights.[383]

On the other hand, in *Chmielewski*,[384] a preliminary reference case from Hungary

[371] *Id.*, ¶ 102, citing Case C-212/11 *Jyske Bank Gibraltar* [2013] EU:C:2013:270.
[372] *Id.*, ¶ 103.
[373] *Id.*, ¶ 104.
[374] *Id.*, ¶ 106 and 109.
[375] *See id.*, ¶ 110.
[376] *Id.*, ¶ 105.
[377] *Id.*, ¶ 106 – 108.
[378] Case C-212/11 *Jyske Bank Gibraltar* [2013] EU:C:2013:270.
[379] *Id.*, ¶ 64.
[380] *Id.*, ¶ 68.
[381] *Id.*, ¶ 63. There are perhaps slight shades of the Vietnam War-era logic of "destroying the village in order to save it" when considering AML/CFT regulation applied to the EU free movement of capital.
[382] *Id.*, ¶ 60 – 61.
[383] Sara De Vido, *Anti-Money Laundering Measures Versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice*, 16 German L.J. 1271, 1288 (2015).
[384] Case C-255/14 *Robert Michal Chmielewski v. Nemzeti Adó- és Vámhivatal Dél-alföldi Regionális Vám- és Pénzügyőri Főigazgatósága* [2015] EU:C:2015:475.

decided in 2015, the issue was the proportionality of a national measure imposing a 60% penalty on cash above €50,000 entering or leaving the EU that was not declared according to EU law.[385] Notably, the purpose of Regulation (EC) No 1889/2005 – controlling movements of cash into and out of the EU in order to prevent dirty money from entering the financial system[386] – is similar to that of the 4th AMLD. According to the ECJ, in the absence of harmonized legislation in an area, a measure is proportionate if it does not "go beyond what is necessary in order to attain the objectives legitimately pursued by that legislation."[387] While stating that competent authorities do not have to take into account individual circumstances in a case such as motive for the measures imposed to be proportionate,[388] the ECJ held that a fine of 60% of the undeclared cash was not proportionate because it did not allow for competent authorities to instead fine a lesser amount while detaining the cash pending investigation into "the provenance of that cash, its intended use and destination."[389]

The primary issue, then, is proportionality. There is no doubt that an outright ban on virtual currency would entail not only a restriction of freedom to provide services under Article 56 TFEU but also a restriction on free movement of capital under Articles 63 and 65 TFEU. Such a ban would also run into Article 17 of the Charter of Fundamental Rights, which states "No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss." That said, a ban would be touted as necessary for maintaining public order and security and meeting AML/CFT goals. Whether it could be justified as not going beyond what is necessary to achieve AML/CFT goals is the question.

There is no certain answer, especially since it is unclear what other measures could be adopted short of a ban. If the ban were coupled with a forced migration to an AML/CFT-compliant virtual currency (e.g. from Bitcoin to a "Bitcoin II" having a modified protocol) but that left everyone in as good or better position than before, then there would be a good argument for proportionality. Otherwise, though, the risk is that the ECJ might disallow a ban, even if a Member State (or potentially even the EU) determined after a thorough risk assessment that banning virtual currencies without AML/CFT-compliant protocols was the only way to ensure that the AML/CFT system itself survived. Given the ECJ's tendency towards *ipse dixit* rulings and the opacity of its reasoning process, there is no real way to gauge how it might come out if presented with the question. But from a Member State's perspective, the worst case scenario should be taken into account: that the ECJ disallows a ban as failing the proportionality test, resulting in 1) the national court forcing the Member State to instead adopt a court-created half-measure that solves little, and/or 2) the Member State facing monetary liability under *Francovich*[390] and to all persons negatively affected by their loss of property in violation of Article 17 of the Charter. Member States faced with a negative ECJ ruling could always ignore it and proceed anyway, a course of action that may go from unthinkable to tempting as the EU itself flirts with existential crisis. But barring total systemic breakdown, an ECJ ruling that forced Member States to either live with AML/CFT-non-compliant virtual currencies or buy out their holders would be an unfortunate, and avoidable, development.

To sum up, then, embracing a short-term AML/CFT solution to virtual currencies increases the risk of a medium-term disaster that could see either the end of effective

[385] Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (OJ 2005 L 309, p. 9).

[386] *Id.*, ¶ 32.

[387] *Chmielewski*, ¶ 21 – 22.

[388] *Id.*, ¶ 28 – 29.

[389] *Id.*, ¶ 30 – 33.

[390] Joined Cases C-6/90 and C-9/90 *Francovich and Others* [1991] ECR I-5357.

AML/CFT regulation or a virtual currency-centered economic crisis. This is not to say that the Commission is wrong to seek to bring virtual currency exchange providers under the 4th AMLD as an interim measure, even if the Commission's position that this will require additional legislation may be incorrect. That said, successful long-term AML/CFT regulation of virtual currencies will require a fundamental "rethink" of the basic tenants how AML/CFT regulation works. To echo IMCO, a "coherent and comprehensive strategy" will be required.

ii. A Proposed Solution

First, some underlying premises: 1) blockchain-based virtual currency really is an important innovation worth promoting, 2) AML/CFT regulation serves an essential public purpose. The problem, as repeated throughout this paper, is that anonymity and lack of intermediaries (particularly in a closed-loop virtual currency system) – features of virtual currencies like Bitcoin – clash fundamentally with the current design of the AML/CFT regulatory system. To preserve both blockchain-based virtual currency and AML/CFT regulation, both will need to be reworked to be compatible with one another.

Fortunately, there is a way: taming anonymity by permitting FIUs and law enforcement to unmask transactions and the real identities of the users behind them. As stated above, this idea was hinted at by FATF, and has been raised elsewhere by commentators. One such commentator explained:

> Using the blockchain it is possible to construct a "translucent" ID system in such a way as to partition knowledge of identities. The blockchain would in effect maintain a record of various ID credentials for an individual and act as a trusted pseudonym for someone's identity. The partition element would involve a third party who would hold the ID credentials as a kind of escrow. The details of these credentials – the real identity – would only ever be released under prescribed, specific circumstances. . . So while the Bitcoin operator might not know who owns a particular wallet (for example) it would know for sure that another regulated institution does and, more importantly, that regulators can find out if needs be.[391]

Similarly, a Seattle attorney who represents virtual currency market actors raised the prospect of a "hard fork" protocol change to Bitcoin that would embed identifying information about public key holders in the software itself, a modification which he characterized as a "large deviation" from the current protocol.[392] There has even been talk of an official government virtual currency having real identities coded into the transactions,[393] though so far this appears to be wishful thinking. On the other hand, one commentator expressed skepticism over an approach requiring re-engineering of virtual currencies to be AML/CFT compliant:

> It may be thought that the software developers could introduce changes to the software itself allowing for the monitoring of transactions and the process of de-anonymising transfers. However, since the Bitcoin software is open source and developed by the Bitcoin community generally, Bitcoin is not centrally controlled by one organisation or business.[394]

In the same vein, a Reddit thread ridiculed a suggestion that "know your customer" CDD be

[391] Gunnar Nordseth, *Will regulation be a blessing or a blow for Bitcoin?*, Banking Technology (April 14, 2016), at http://www.bankingtech.com/458622/will-the-4th-aml-directive-be-a-blessing-or-a-blow-for-bitcoin/

[392] Daniel S. Friedberg, *Hard Fork Conspiracy Treacherous* (Feb. 11, 2016), at http://www.riddellwilliams.com/blog/articles/post/hard-fork-conspiracy-treacherous.

[393] Bohannon, *supra* n. 237.

[394] Stokes, *supra* n. 96, at 230.

coded into the Bitcoin protocol, suspecting that the person who raised it was "trolling."[395] Resistance should be expected.

Without attempting to address the idea from a technical standpoint, the concept is simple enough: interpose a trusted entity, akin to the Internet Corporation for Assigned Names and Numbers (ICANN) in the internet context, tasked with issuing virtual currency public keys. The trusted entity would undertake CDD whenever it issued new public keys and would require adequate customer identification and other identity-verification measures before creating a new public key. This identifying information would be encrypted and encoded into the new public key, while the trusted entity would retain the private ID-key necessary to unlock and reveal the information. This step would require development of a virtual currency or currencies with protocols specially-engineered to be AML/CFT compliant, and it would be left to the private sector to bring these about. The trusted entity could additionally provide FIUs with the private ID-key registry, allowing FIUs to "ping" a public key to obtain the user's identification information. Legal safeguards could be built into the system, such as requiring a warrant or court order before a FIU could "ping" a public key. Private actors would of course not be able to obtain identifying information about public keys or the underlying transactions since they would not have access to the private ID-keys needed to unlock them.

Virtual currencies with AML/CFT-compliant protocols would have a competitive advantage over those lacking such protocols, beyond the obvious advantage of legality. Namely, virtual currencies with AML/CFT-compliant protocols would, as has been mentioned before, have intrinsic value, especially if intellectual property rights and compliance and certification costs created barriers to entry. Ironically, as things are currently, the ease by which new virtual currencies can be developed and the lack of barriers to entry threaten the viability of even successful virtual currencies like Bitcoin, which could be eclipsed by an alt-coin rival if popular sentiment shifts. By increasing costs on rivals, then, AML/CFT regulation requiring special protocols could narrow the field and contribute to the maturing of virtual currencies as a whole.

In addition to a trusted entity issuing public keys, a comprehensive AML/CFT regulatory approach would need to address the 51% attack problem head-on. After all, it would do no good for a virtual currency to have special and expensively-attained AML/CFT-compliant protocols if a dedicated group could seize power and do away with them. The solution could be a computer resource reserve controlled by a government entity or other trusted third-party able to step in and overwhelm any attack via a superior counterattack, much like a central bank attempting via open market operations to counter currency speculation (though hopefully with better success).

Additional AML/CFT-compliant protocol changes could include geographic identifiers added to public keys so that FIUs could monitor transfers to or from the EU surpassing a certain value threshold (either in one transactions or in a series of related transactions). Additionally, public keys could include "block" features that would allow FIUs to stop all transactions to and from a public key, providing FIUs with ammunition against known or suspected criminals or terrorists.

[395] https://www.reddit.com/r/Bitcoin/comments/3ilyav/going_full_retard_bips_proposal_for_implementing/ An excerpt follows:
"Dude, I've got an idea, let's troll the Bitcoin community by saying we're going to start a company that tracks every transaction on the blockchain!"
(swig of beer)
"No wait, hold on, even better we say we're going to introduce KYC into the core software itself!"
"Oh man, yes! Let's actually code up a BIP for it!"
"This is going to be so good, I can't wait 'til Reddit gets a hold of it. Everyone is still fried from the block size cap debacle."

Outside of the virtual currency context, state-of-the-art computer software designed for suspicious pattern recognition, risk-assessment, matching against "watch lists," and other data mining and surveillance applications are already part of obligated entities' AML/CFT toolkit, largely made necessary because of the sheer number of financial transactions that obligated entities facilitate.[396] FIUs could use these tools to monitor virtual currency transactions in near-real time, allowing FIUs to identify potentially suspicious transactions without need for reports from intermediaries. The blockchain would be a valuable data-mining tool for FIUs, since all transactions are recorded for posterity. Coupled with de-anonymising features, virtual currencies would lose their utility for money laundering or terrorist financing and would instead be one of the worst vehicles for transmitting dirty money.

In addition to intellectual property protection for AML/CFT-compliant protocols, a bounty for developing a virtual currency with such features could be offered by the EU, encouraging private sector competition. Once a virtual currency or currencies that were AML/CFT-compliant were ready for launch via a trusted entity, current users of virtual currencies such as Bitcoin could be given a grace period to migrate to the new currency, with new virtual currency issued for old non-compliant currency at a fixed exchange rate. Anyone who failed or refused to migrate would be left with holdings of virtual currency that could not be legally used in the EU, and with FATF and international cooperation and harmonization, in other jurisdictions. By premising a ban of non-compliant virtual currencies on a fair and full opportunity to first exchange them for AML/CFT-compliant virtual currencies, the EU would increase the chance that its actions would be deemed to be proportionate by the ECJ and in accordance with EU law.

While the above changes to virtual currency in the EU would certainly make them more palatable from an AML/CFT regulatory standpoint, many of their current adherents would object on ideological, political, or self-interest grounds. Ultimately, however, the point is not to make the Bitcoin community happy but to move virtual currency and blockchain technology forward while closing the gaping and perhaps intentional AML/CFT compliance problems they currently pose.

[396] *See* Boszörmenyi and Schweighofer, *supra* n. XX, at 67-68.

V. Conclusion

This paper has addressed a topic that just ten years ago would have been regarded as fanciful: AML/CFT regulation of virtual currencies and blockchain technology under EU law. While starting from the premise that early regulation of an emerging technology could impede its development, this paper concludes that in the case of virtual currency and blockchain, early comprehensive AML/CFT regulation could actually help ensure the technology's success. Even if this possibility is overstated, however, waiting until the technology becomes widespread before enacting comprehensive AML/CFT regulation could spell disaster, as it may by that point be too late to bring virtual currencies within a workable AML/CFT system.

Though the solution proposed – integrate AML/CFT into virtual currencies' protocols themselves and allow FUIs to access, on a "need to know" basis, otherwise hidden information about transactions and the real people behind them – would fix what could otherwise be an unsolvable dilemma, nothing is without risk. The prospect of FIUs having unparalleled ability to monitor private transactions should be seen as troubling, and as Boszörmenyi and Schweighofer note, the use of so-called "dataveillance" technologies under the current AML/CFT system raises fundamental rights concerns, particularly with respect to the right to private and family life under Article 7 of the EU Charter of Fundamental Rights.[397] Oversight is, however, basic to any functioning AML/CFT system, whether carried out by intermediaries or by the state itself. And anonymity may not always be such a good thing, especially when the flow of money is concerned. As stated by legal commentator and U.S. federal judge Alex Kozinski, "[s]ome scary things happen when people are – or feel to be – anonymous," a condition that brings with it some "highly antisocial aspects."[398] This is not to dismiss privacy concerns, but at a certain point it is misplaced to complain about the lack of privacy occasioned by a regulatory system deliberately designed to enforce a lack of privacy. Only a dismantling or scaling-back of AML/CFT could ensure real financial privacy – but at the cost of facilitating money laundering and terrorist financing. There are, like many things in life, no perfect solutions. It is hoped however that the EU will work towards integrating AML/CFT controls with virtual currency so that the two systems complement each other – and thereby allow the "next internet" to reach adulthood.

[397] *Id.* at 68.

[398] *See* Kozinski, *supra* n. XX, at 17.

Bibliography and Cases

Journal Articles

Nicholas J. Ajello, *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, 80 Brook. L. Rev. 435 (2014-2015).

Michael J. Anderson and Tracey A. Anderson, *Anti-money laundering: history and current developments*, J.I.B.L.R. 2015, 30(10), 521-531.

Michael Bombace, *Blazing Trails: A New Way Forward for Virtual Currencies and Money Laundering*, Journal of Virtual Worlds Research, Volume 6, Number 3 (July 2013).

Janös Boszörmenyi and Erich Schweighofer, *A review of tools to comply with the Fourth EU anti-money laundering directive*, International Review of Law, Computers & Technology, Vol. 29, No. 1, 63– 77 (2015).

Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 Ind. L.J. 441 (Winter 2014).

Adrian (Wai-Kong) Cheunga, Eduardo Rocab, and Jen-Je Su, *Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices*, Applied Economics, Vol. 47, No. 23, 2348–2358 (2015).

Sara De Vido, *Anti-Money Laundering Measures Versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice*, 16 German L.J. 1271, 1288 (2015).

Victor Dostov and Pavel Shust, *Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?*, 21 Journal of Financial Crime 3, p. 252 (2014).

Sarah Gruber, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion*, 32 Quinnipiac L. Rev. (2013).

Andres Guadamuz and Chris Marsden, *Blockchains and Bitcoin: Regulatory responses to cryptocurrencies*, First Monday, Volume 20, Number 12 (7 December 2015).

Robby Houben, *The CJEU's view of whether Bitcoins are a currency: a Belgian perspective*, I.C.C.L.R. 2016, 27(3), 61-64, 64 (2016).

Sarah Jane Hughes and Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 Yale J. on Reg. 495 (Summer 2015).

Mitchell Hyman, *Bitcoin ATM: A Criminal's Laundromat for Cleaning Money*, St. Thomas Law Review, Vol. 27 Issue 2, p 287-308 (Summer 2015).

Angela S.M. Irwin, Jill Slay, Kim-Kwang Raymond Choo, Lin Lui, *Money laundering and terrorism financing in virtual environments: a feasibility study*, Journal of Money Laundering Control, Vol. 17 Iss 1 pp. 50-75 (2014).

Sam Kessler, *The Future of Bitcoin: A Rocky Path to Currency*, Harvard Political Review (January 19, 2016).

Alex Kozinski, *Essay: The Two Faces of Anonymity*, 43 Cap. U. L. Rev. 1 (2015).

Anita Lavorgna, *Organised crime goes online: realities and challenges*, Journal of Money Laundering Control, Vol. 18 No. 2, pp. 153-168 (2015).

Seth Litwack, *Bitcoin: Currency or Fool's Gold?: A Comparative Analysis of the Legal Classification of Bitcoin*, 29 Temp. Int'l & Comp. L.J. 309, 311 (Fall 2015).

William J. Luther, *Bitcoin and the Future of Digital Payments*, 20 The Independent Review 3 (Winter 2016).

Matthew S. Morgan, *Money Laundering: The American Law and its Global Influence*, 3-SUM NAFTA: L. & Bus. Rev. Am. 24, 26-27 (Summer 1997).

Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. Banking Inst. 529 (March 2014).

Charles Plombeck, *Confidentiality and Disclosure: The Money Laundering Control Act of 1986 and Banking Secrecy*, International Lawyer (ABA) 22 Int'l L. 69, 71-72 (1988).

Michal Polasik, Anna Iwona Piotrowska, Tomasz Piotr Wisniewski, et al., *Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry*, International Journal of Electronic Commerce, Vol. 20, No. 1, p. 9-49 (Aug. 31, 2015).

Wim Raymaekers, *Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities*, Journal of Payments Strategy & Systems Volume 9 Number 1 (December 8, 2014).

Steven L. Schwarcz, *Temporal Perspectives: Resolving the Conflict Between Current and Future Investors*, 89 Minn. L. Rev. 1044, 1081 (April 2005).

Sergii Shcherbak, *How Should Bitcoin be Regulated*, European Journal of Legal Studies, 2014, Vol. 7, No. 1, pp. 45-91.

Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 Nw.J. TECH. *&* INTELL. PROP. 37 (2015).

Gauri Sinha, *AML-CTF: a forced marriage post 9/11 and its effect on financial institutions*, Journal of Money Laundering Control Vol. 16 No. 2 (2013).

Robert Stokes, *Anti-Money Laundering Regulation and Emerging Payment Technologies*, 32 No. 5 Banking & Fin. Services Pol'y Rep. 1 (May 2013).

Robert Stokes, *Virtual money laundering: the case of Bitcoin and the Linden dollar*, Information & Communications Technology Law, Vol. 21, No. 3, October 2012, 221–236.

Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox*, 20 RICH. J.L. & TECH. 13 (2014).

Misha Tsukerman, *The Block is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 Berkeley Tech. L.J. 385, 1130 (2015).

Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 Wash. L. Rev. 271 (August 2014).

Sheng Zhou, *Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet*, 3 J.L. & Cyber Warfare 103 (2014).

Aviv Zohar, *Bitcoin: Under the Hood*, 58 Communications of the ACM 9, p. 111 (Sept. 2015).

<u>Books</u>

Clare Chambers-Jones, *Virtual Economics and Virtual Crime: Money Laundering in Cyberspace* (2012).

Annegret Flohr, *Self-Regulation and Legalization: Making Global Rules for Banks and Corporations* (2014).

Emmanuel Ioannides, *Fundamental Principles of EU Law Against Money Laundering* (2014).

Charles Mackey, *Memoirs of Extraordinary Popular Delusions and the Madness of Crowds* (1852).

Eleni Tsingou, “Money Laundering,” in Daniel Mügge, *Europe and the Governance of Global Finance* (2014).

<u>Websites and Other Misc. Online Resources</u>

http://www.bankofengland.co.uk/banknotes/Pages/about/faqs.aspx#sandni

https://bitcoin.org/bitcoin.pdf

https://bitcointalk.org/index.php?topic=678778.0

https://blockchain.info/charts/median-confirmation-time?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

http://www.coindesk.com/data/bitcoin-market-capitalization

http://www.coindesk.com/price

https://dankaminsky.com/

https://disneyworld.disney.go.com/faq/parks/using-disney-dollars

http://www.eba.europa.eu/about-us;jsessionid=533E304F5947116C08E0B7A810CABD6B

https://ec.europa.eu/digital-single-market/news/blockchain-and-digital-currencies-workshop

http://edcab.eu/blockchain-expo/virtual-currency-blockchain-expo-in-european-parliament

http://edcab.eu/blockchain-expo/ulrike-trebesius-mep-supports-virtual-currencies-in-the-european-parliament

https://en.bitcoin.it/wiki/Myths#The_value_of_bitcoins_are_based_on_how_much_electricity_and_computing_power_it_takes_to_mine_them

https://www.ethereum.org/

http://europa.eu/rapid/press-release_IP-16-202_en.htm

http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160125-1500-COMMITTEE-ECON

http://www.fatf-gafi.org/about/historyofthefatf/

http://www.fatf-gafi.org/about/membersandobservers/

http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

https://www.hpematter.com/issue-no-6-fall-2015/next-internet-disruptive-potential-bitcoin-and-blockchain

http://krebsonsecurity.com/2015/08/extortionists-target-ashley-madison-users/

https://www.loc.gov/exhibits/treasures/trr002.html

https://www.mercatoradvisorygroup.com/Press_Releases/Mercator_Advisory_Group_Identifies_How_VC_Investments_Could_Cripple_Bitcoin/

http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

http://myemail.constantcontact.com/MALPRACTICE-ALERT--Beware-of-Ransomware.html?soid=1118263556714&aid=dDQFDjT06cI

http://www.pcc.cu/opm_cdr.php

https://www.reddit.com/r/Bitcoin/comments/3ilyav/going_full_retard_bips_proposal_for_implementing/

https://research.stlouisfed.org/fred2/series/M1SL http://www.riddellwilliams.com/blog/articles/post/hard-fork-conspiracy-treacherous

http://sdw.ecb.europa.eu/reports.do?node=1000003478

http://www.slideshare.net/LinkedInPulse/don-alex-tapscott-weekend-essay-blockchain-revolution-bitcoin-finance-money

http://smartcontract.com/

http://stuff.mit.edu/people/mkgray/net/web-growth-summary.html

https://thisiswhyubroke.wordpress.com/2014/02/23/bitcoin-is-the-new-beanie-babies

https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx

http://www.vartmp.com/blog/bitcoin

https://winklevosscapital.com/what-may-have-happened-at-mt-gox/

Media and Newspaper Articles

Blockchain – the Next Big Thing (or is it?), The Economist (May 9, 2015).

Craig Steven Wright claims to be Satoshi Nakamoto. Is he?, The Economist (May 2, 2016).

Craig Wright revealed as Bitcoin creator Satoshi Nakamoto, BBC (May 2, 2016).

FBI arrest key Silk Road 'adviser' in Thailand, BBC (Dec. 7, 2015).

The Magic of Mining, The Economist (Jan. 10, 2015).

Många vill rösta om EU-medlemskap, Svenska Dagbladet (May 9, 2016).

Schulz warnt vor „Implosion der EU," Frankfurter Allgemeine (April 11, 2016).

Ten arrested in Netherlands over bitcoin money-laundering allegations, The Guardian (Jan. 20, 2016).

U.S., Canada issue joint alert on 'ransomware' after hospital attacks, The Telegraph (April 1, 2016).

Wright's wrongs, The Economist (May 7, 2016).

Marc Andreessen, *Why Bitcoin Matters*, New York Times – Dealbook (Jan. 21, 2014).

John Bohannon, *Why criminals can't hide behind Bitcoin*, Science (Mar. 9, 2016).

Warren Buffett, *Warren Buffett: Why stocks beat gold and bonds*, Fortune (Feb. 9, 2012).

Steve Case, *The Complete History of the Internet's Boom, Bust, Boom Cycle*, Business Insider (Jan. 14, 2011).

Rory Cellan-Jones, *'Bitcoin creator': I do not have the courage*, BBC (May 5, 2016).

Jonathan Chester, *How Questions About Terrorism Challenge Bitcoin Startups*, Forbes (Dec. 14, 2015).

Andrew Cohen, *How White Users Made Heroin a Public-Health Problem*, The Atlantic (Aug. 12, 2015).

Jesse Colombo, *Bitcoin May Be Following This Classic Bubble Stages Chart*, Forbes (Dec. 19, 2013).

Alex Court, *Breaking the bank: Bitcoins hit Africa's money transfer traditions*, CNN (Feb. 17, 2015).

Joseph Cox, *Dark Web Drug Markets Are Desperately Clinging to the Silk Road Brand*, Motherboard (Oct. 22, 2015).

Chris DeRose, *'Smart Contracts' are the Future of Blockchain*, American Banker (Jan. 8, 2016).

Romain Dillet, *Why I Lost Faith in Bitcoin as a Money Transfer Protocol*, TechCrunch (Jan. 1, 2014).

John C. Dvorak, *Bitcoin & Beanie Babies: How to Spot a Tech Bubble*, PC Magazine (Nov. 5, 2014).

Anthony Faiola, *Germany springs to action over hate speech against migrants*, Washington Post (Jan. 6, 2016).

Rachel Feltman, *Meet the family who lost $100,000 when the Beanie Baby bubble burst,* Quartz (August 13, 2013).

Emily Flitter, *Prominent Bitcoin entrepreneur charged with money laundering*, Reuters (Jan. 27, 2014).

Thomas Fox-Brewster, *As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin*, Forbes (Feb. 18, 2016).

Stephen Gandel, *Jamie Dimon: Virtual Currency Will Be Stopped*, Fortune (Nov. 4, 2015).

Ross Gerber, *Why Apple Pay And Dollars Are Killing Bitcoin*, Forbes (Jan. 29, 2015).

Sandy Grady, *Macho Congressmen: Drugbusters Inc.*, Philadelphia Daily News (June 20, 1988).

Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, Forbes (Sept. 5, 2013).

Andy Greenberg, *An Interview With A Digital Drug Lord: The Silk Road's Dread Pirate Roberts (Q&A)*, Forbes (Aug. 14, 2013).

Andy Greenberg, *Prosecutors Trace $13.4M in Bitcoins from the Silk Road to Ulbricht's Laptop*, Wired (Jan. 29, 2015).

Andy Greenberg, *Senator Calls For Bitcoin Ban In Letter To Financial Regulators*, Forbes (Feb. 26, 2014).

Jasper Hamill, *ISIS owns small fortune in Bitcoin, claim Anonymous supporters - now Europe could ban virtual currency*, Mirror (Nov. 19, 2015).

Alex Hern, *Major sites including New York Times and BBC hit by 'ransomware' malvertising*, The Guardian (March 16, 2016).

Alex Hern, *Mt Gox CEO charged with embezzling £1.7 million worth of bitcoin*, Business Insider UK (Sept. 14, 2015).

Kashmir Hill, *Bitcoin Battle: Warren Buffett vs. Marc Andreessen*, Forbes (March 26, 2014).

Tim Hornyak, *One group controls 51 percent of Bitcoin mining, threatening security sanctity*, PC World (June 16, 2014).

Anna Irrera, *UBS Building Virtual Coin For Mainstream Banking*, Wall Street Journal - Digits (3 Sept. 2015).

Joab Jackson, *All the feds needed to do to ID Silk Road's founder was Google it*, PC World (Jan. 26, 2015).

Sarah Jeong, *Jury Finds Ross Ulbricht Guilty of Running Silk Road Marketplace*, Forbes (Feb. 4, 2015).

Carolyn Y. Johnson and Matt Zapotosky, *Under pressure to digitize everything, hospitals are hackers' biggest new target*, Washington Post (April 1, 2016).

Jeff Kearns, *Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value*, Bloomberg Business (Dec. 4, 2013).

Timothy B. Lee, *Bitcoin's Volatility is a Disadvantage, But Not a Fatal One*, Forbes (Apr. 12, 2013).

Victor Luckerson, *Here's Why Bitcoin Is So Volatile Right Now*, Fortune (Nov. 5, 2015).
Ian Mckendry, *ISIL May Be Using Bitcoin, Fincen's Calvery Says*, American Banker, Vol. 180, Issue 176 (11/17/2015).

Mike Montgomery, *Bitcoin is Only the Beginning for Blockchain Technology*, Forbes (Sep. 15, 2015).

David Z. Morris, *Does Western Union need to watch out for bitcoin?*, Fortune (Feb. 10, 2014).

Gunnar Nordseth, *Will regulation be a blessing or a blow for Bitcoin?*, Banking Technology (April 14, 2016).

Jose Pagliery, *Record $1 billion invested in Bitcoin firms so far*, CNN Money (November 3, 2015).

Andrea Peterson, *This devastating type of malware has basically ignored Mac users. Until now.*, The Washington Post (March 7, 2016).

Nathaniel Popper and Rachel Adams, *Apparent Theft at Mt. Gox Shakes Bitcoin World*, New York Times (Feb. 25, 2014).

Katie Rogers, *Anonymous Hackers Fight ISIS but Reactions Are Mixed*, New York Times (Nov. 25, 2015).

Lauran Shin, *Should You Invest In Bitcoin? 10 Arguments In Favor As Of December 2015,* Forbes (Dec 11, 2015).

Laura Shin, *This Man Has Been Living On Bitcoin For 3 Years*, Forbes (Jan. 7, 2016).

Annie Sneed, *The Most Vulnerable Ransomware Targets Are the Institutions We Rely On Most*, Scientific American (March 23, 2016).

Jonathan Soble, *Mark Karpeles, Chief of Bankrupt Bitcoin Exchange, Is Arrested in Tokyo*, New York Times (Aug. 1, 2015).

Peter Spence, *Bitcoin revolution could be the next internet, says Bank of England*, The Telegraph (25 February 2015).

Mark Joseph Stern, *Why did people lose their minds over Beanie Babies?*, Slate (Feb. 3, 2015).

Aaron Timms, *BitLicense: Legitimacy for Digital Currencies, but Will Innovation Suffer?*, Institutional Investor (June 22, 2015).

Richard Thaler, *Keynes's 'beauty contest'*, Financial Times Magazine (July 10, 2015).

Jim Urquhart, *Police need powers to tackle virtual money laundering: Europol*, Reuters (March 24, 2014).

Anne VanderMey, *Lessons from the great Beanie Babies crash*, Fortune (March 11, 2015).

Paul Vigna, *Bitcoin's Volatility Reflects a Work in Progress — BitBeat*, The Wall Street Journal (Nov. 5, 2015).

Nicholas Weaver, *Once You Use Bitcoin You Can't Go 'Back' – And That's Its Fatal Flaw*, Wired (Nov. 26, 2013).

Joe Weisenthal, *Why Bitcoin Is Like No Other Bubble We've Seen Before*, Business Insider (April 3, 2013).

Rob Wile, *Bitcoin Can Be the New Western Union*, Business Insider (Dec. 5, 2013).

Geoff Williams, *Should You Invest in Bitcoin?*, U.S. News & World Report (May 1, 2013).
Al Lewis, *Tulip Bulbs for Our Time*, Wall Street Journal, Al's Emporium—Commentary (December 8, 2013).

Danny Yadron, *Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers*, The Guardian (February 18, 2016).

Niam Yaraghi, *A Health Hack Wake-Up Call*, U.S. News & World Report (April 1, 2016).

Matt Zapotosky and Ellen Nakashima, *These hackers can hold a town hostage. And they want ransom — paid in bitcoin*, The Washington Post (March 21, 2016).

Other Sources

Latest Thinking: Blockchain-enabled distributed ledgers: Are investment banks ready?, at https://www.accenture.com/us-en/insight-blockchain-enabled-distributed-ledgers-investment-banks

Mervärdesskatt: Handel med bitcoins, 2013-10-14 (dnr 32-12/I).

Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz, RAND Corporation, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment* (2015).

Christian Brenig, Rafael Accorsi, and Günter Müller, *Economic Analysis of Cryptocurrency Backed Money Laundering*, ECIS 2015 Completed Research Papers, Paper 20 (2015).

Committee on Economic & Monetary Affairs of the European Parliament, Public hearing on virtual currencies, Statement of Siân Jones, founder, EDCAB (Jan. 25, 2016).

DG JUST – B Task Force Financial Crime, Inception Impact Assessment (Apr. 7, 2016).

EBA, *Warning to Consumers on Virtual Currencies*, EBA/WRG/2013/01 (12 December 2013).

EBA, *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08 (4 July 2014).

ECB, *Virtual Currency Schemes*, (October 2012).

ECB, *Virtual Currency Schemes – A Further Analysis* (February 2015).

European Commission - Fact Sheet, *Questions and Answers: Action Plan to strengthen the fight against terrorist financing* (Feb. 2, 2016).

European Council, *Council conclusions on the fight against the financing of terrorism* (Feb. 12, 2016).

European Parliament News, *Virtual currencies: what are the risks and benefits?* (26 January 2016).

European Parliament Press Release, *Set up taskforce to oversee virtual currencies, ECON MEPs say* (April 26, 2016).

Europol, *Changes in modus operandi of Islamic State terrorist attacks* (The Hague, Jan. 18, 2016).

FATF*, Financial Action Task Force Mandate (2012-2020)* (April 20, 2012).

FATF Recommendations (February 2012).

FATF Report, Virtual Currencies – Key Definitions and Potential AML/CFT Risks (June 2014).

FBI New York Field Office, Manhattan U.S. Attorney Announces Charges Against Two Florida Men for Operating an Underground Bitcoin Exchange (July 21, 2015).

Nathalie Stråle Johansson & Malin Tjernström, *The Price Volatility of Bitcoin, A search for the drivers affecting the price volatility of this digital currency*, Umeå School of Business and Economics – Masters Thesis, p. 61 (Spring 2014).

Mohit Kaushal & Sheel Tyle, *The Blockchain: What it is and Why it Matters*, Brookings Institution (January 13, 2015).

Berkley A. Pamplin, *Virtual Currencies and the Implications for U.S. Anti-Money Laundering Regulations*, Utica College dissertation (August 2014).

Hammad Siddiqi, *The Routes to Chaos in the Bitcoin Market* (February 17, 2014).

Marcin Szczepański, European Parliamentary Research Service Briefing Paper, *Bitcoin: Market, economics and regulation* (11/04/2014).

Rapporteur Ulrike Trebesius, Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Economic and Monetary Affairs on virtual currencies (2016/2007(INI)) (Apr. 21, 2016).

U.S. Department of Homeland Security, U.S. CERT, Alert (TA16-091A) Ransomware and Recent Variants (March 31, 2016).

U.S. Department of Justice – U.S. Attorney's Office for the Western District of New York, *Three Men Indicted On District's First Bitcoin-Related Case* (March 11, 2016).

Peggy Valcke, Niels Vandezande, Nathan Van de Velde, *The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4*, SWIFT Institute Working Paper No. 2015-001 (September 23, 2015).

Rapporteur Jakob von Weizsäcker, Committee on Economic and Monetary Affairs of the European Parliament, *Draft Report on Virtual Currencies* [Feb. 23, 2016] (2016/2007(INI)).

Legislation

U.S.

Bank Secrecy Act [31 U.S.C. 5311 *et seq.*].

Communications Decency Act of 1996 [47 U.S.C. § 223(a)(1)(B) & § 223(d) (1994 ed., Supp. II)].

Comprehensive Crime Control Act of 1984 [Pub.L. 98–473, S. 1762, 98 Stat. 1976, enacted October 12, 1984].

EU

Capital Requirements Directive IV [Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC].

Electronic Money Directive [Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions].

Fourth Anti-Money Laundering Directive [Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC].

Funds Transfer Regulation [Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006].

Payment Services Directive [Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC].

Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community].

Third Anti-Money Laundering Directive [Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing].

VAT Directive [Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax].

Cases

U.S.

California Bankers Ass'n v. Shultz, 416 U.S. 21, 94 S.Ct. 1494 (1974).

FCC v. Pacifica Foundation, 438 U.S. 726, 98 S.Ct. 3026 (1978).

Gitlow v. People of State of New York, 268 U.S. 652, 45 S. Ct. 625 (1925).

Reno v. American Civil Liberties Union, 521 U.S. 844, 117 S.Ct. 2329 (1997).

Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir.2001).

EU

Case C-255/14 *Robert Michal Chmielewski v. Nemzeti Adó- és Vámhivatal Dél-alföldi Regionális Vám- és Pénzügyőri Főigazgatósága* [2015] EU:C:2015:475.

Case C-172/96 *Commissioners of Customs & Excise v First National Bank of Chicago* [1998] ECR I-4387.

Joined Cases C-6/90 and C-9/90 *Francovich and Others* [1991] ECR I-5357.

Case C-212/11 *Jyske Bank Gibraltar* [2013] EU:C:2013:270.

Case C-235/14 *Safe Interenvios, SA v Liberbank, SA and Others* [2016] EU:C:2016:154.

Case C-264/14 *Skatteverket v. David Hedqvist* [2015] EU:C:2015:718 and Opinion of Advocate General Kokott, delivered on 16 July 2015.