frontiers in Blockchain

ORIGINAL RESEARCH
published: 20 May 2021
doi: 10.3389/fbloc.2021.627641

The Formal, Financial and Fraught Route to Global Digital Identity Governance

Malcolm Campbell-Verduyn[1,2†]* *and Moritz Hütten*[3,4†]

[1]*Käte Hamburger Kolleg Centre for Global Cooperation Research University of Duisburg-Essen, Duisburg, Germany,* [2]*Department of International Relations and International Organization, University of Groningen, Groningen, Netherlands,* [3]*Department of Economics and Center for Sustainable Economic and Corporate Policy, Darmstadt University of Applied Sciences, Darmstadt, Germany,* [4]*Department of Political Science, Amsterdam Institute for Social Science Research, University of Amsterdam, Amsterdam, Netherlands*

How can we understand the progressive, piecemeal emergence of global digital identity governance? Examining the activities of the Financial Action Task Force (FATF) - an intergovernmental organization at the center of global anti-money laundering and counter-the-financing of terrorism governance-this paper advances a two-fold argument. First, the FATF shapes how, where and who is involved in developing key standards of acceptability underpinning digital identity governance in blockchain activities. While not itself *directly* involved in the actual coding of blockchain protocols, the FATF influences the location and type of centralized modes of control over digital identity governance. Drawing on the notion of protocological control from media studies, we illustrate how centralized control emerging in global digital identity governance emanates from the global governance *of* financial flows long considered by international organizations like the FATF. Second, we suggest that governance *by* blockchains persistently shapes the ability of the FATF to stem illicit international financial flows. In highlighting both the influence of FATF on blockchain governance and blockchain governance on the FATF, we draw together two strands of literature that have been considered separately in an analysis of the formal, financial and fraught route to global digital identity governance.

Keywords: control, identity, finance, money laundering and financing terrorism, financial action task force, global governance

OPEN ACCESS

Edited by:
Andrej Zwitter,
University of Groningen, Netherlands

Reviewed by:
Jolien Ubacht,
Delft University of Technology, Netherlands
Zeynep Gurguc,
Imperial College Business School, United Kingdom

***Correspondence:**
Malcolm Campbell-Verduyn
campbell@gcr21.uni-due.de

†These authors have contributed equally to this work

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *09 November 2020*
Accepted: *04 May 2021*
Published: *20 May 2021*

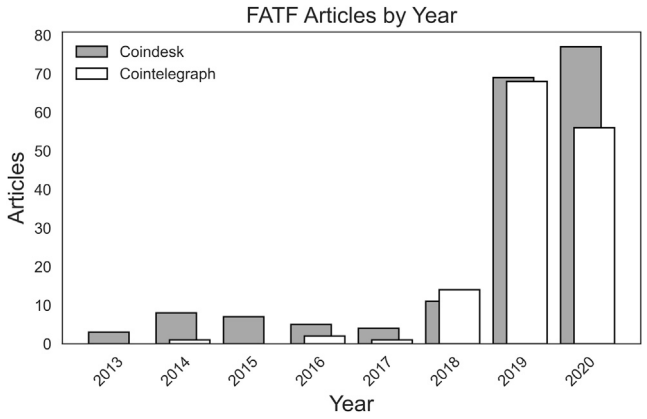
Citation:
Campbell-Verduyn M and Hütten M (2021) The Formal, Financial and Fraught Route to Global Digital Identity Governance. Front. Blockchain 4:627641. doi: 10.3389/fbloc.2021.627641

INTRODUCTION

How can we understand the on-going emergence of global digital identity governance? The seemingly ever progressing digitalization of human activities, accelerated by the Covid-19 pandemic, is not a smooth, linear and all-encompassing affair. Rather, it remains patchy and tension-filled. While activities like digital payments flourish (Boakye-Adjei, 2020; Frazier, 2020), others remain marked by longstanding conflicts. The progressive and piecemeal digitalization of identities exemplifies these broad tensions including, amongst others, user privacy and the informational needs of regulators charged with prevent exploitation, abuse and illicit activities. Blockchains and other novel technologies are continually emerging to square the circle of privacy and surveillance. Yet, their applications often merely shift the location and form of such tensions, rather than resolving them.

Analysis of emerging blockchain-based attempts to resolve these and other longstanding tensions in contemporary governance generally considers governance *by* and *of* blockchain systems

TABLE 1 | Mentions of the FATF in leading industry news outlets.



Source: Authors based on articles collected from cointelegraph.com and coindesk.com.

(Campbell-Verduyn, 2018b; Atzori, 2017; de Filipi, 2018; Herian, 2018; Hooper and Holtbrügge, 2020; Jones, 2019; Reijers et al., 2016).[1] The former stress how blockchain applications *themselves* govern an organization or process while the latter emphasize how blockchains are governed by a range of state and non-state organizations. While generating increasingly nuanced understanding, this growing literature has granted surprisingly little attention to the interplay between governance *of* and *by* blockchains. In particular, little attention has been granted to relations between informal and formal forms of blockchain governance beyond passing mentions to the likes of the International Monetary Fund (IMF) and Organization for Economic Cooperation and Development (OECD).

This article contributes to the filling of this gap by examining relations between evolving forms of governance *by* blockchains and the governance *of* blockchain emanating from the Financial Action Task Force (FATF). Attracting more industry attention than in academic studies of blockchain (**Table 1**),[2] this Paris-based intergovernmental organization is responsible for setting global standards for anti-money laundering and counter-the-financing of terrorism governance (AML/CFT). In tracing both 1) the underappreciated role of this formal organization in shaping the emergence of global digital identity governance and 2) the implications of blockchain activities on its attempts to stem illicit financial flows, this paper draws together of analysis of governance *by* and *of* blockchain. To do so, we harness and extend the notion of protocological control. Developed by media studies scholar Alexander Galloway (2004): 6–7, who built on insights from French philosophers Michel Foucault and Gilles Deleuze, the notion of protocological control helps illustrate how the embedding of specific standards of behaviour into computing protocols provide the key "standards governing the implementation of specific technologies." We show how protocols serve as key forms of governance themselves while also drawing out how the location and form of protocological control is itself shaped. In other words, we clarify the *who*, *where* and *how* of protocological control by pointing to the influence of the FATF on the location and form of protocological control in blockchain-based activities. In doing so, we show that, despite claiming to *distribute* power across the nodes in novel digital networks, applications of blockchains instead *frequently shift the location and type of actors exercising centralized contro*l.

Two central contributions are made in this article. First, we illustrate how the FATF shapes how, where and who is involved in developing key standards of acceptability underpinning digital identities. While not itself *directly* involved in the actual coding of protocols, the FATF influences *the location and type of centralized modes of control*. We stress how protocological control emerging in global digital identity governance emanates from the global governance *of* financial flows long considered by intergovernmental organizations like the FATF. In elaborating the role of this organization, we extend studies identifying the financial roots of digital identity governance beyond informal interactions between the public sector and financial technology industry at the national level (Eaton et al., 2018; Faria, 2021). Second, we suggest that governance *by* blockchains persistently shapes the ability of the FATF to stem illicit financial flows. In highlighting tensions between both the influence of FATF on blockchain governance and blockchain governance on the FATF, we draw two strands literature together in identifying both the formal and financial, as well as the fraught route to global digital identity governance.

We elaborate these arguments over three further sections drawing on primary documents, including guidance and reports of the FATF,[3] as well as secondary documents from

[1]For up-to-date overview of this fast growing literature see https://www.blockchainresearchnetwork.org/docs/blockchain-governance/.

[2]Exceptions include Campbell-Verduyn, 2018a; Naheem, 2019; Pavlidis, 2020.

[3]We manually extracted 17 documents as belonging to the topic "blockchain" from the official website of the FATF spanning the years 2013 to 2020.

TABLE 2 | Overview of the FATF 40 + 9 Recommendations (as of February 15, 2021).

Number	
	A—AML/CFT POLICIES AND COORDINATION
1	Assessing risks and applying a risk-based approach
2	National cooperation and coordination
	B—MONEY LAUNDERING AND CONFISCATION
3	Money laundering offence
4	Confiscation and provisional measure
	C—TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	Terrorist financing offence
6	Targeted financial sanctions related to terrorism and terrorist financing
7	Targeted financial sanctions related to proliferation
8	Non-profit organisations
	D—PREVENTIVE MEASURES
9	Financial institution secrecy laws
	Customer due diligence and record keeping
10	Customer due diligence
11	Record keeping
	Additional measures for specific customers and activities
12	Politically exposed persons
13	Correspondent banking
14	Money or value transfer services
15	New technologies
16	Wire transfers
	Reliance, Controls and Financial Groups
17	Reliance on third parties
18	Internal controls and foreign branches and subsidiaries
19	Higher-risk countries
	Reporting of suspicious transactions
20	Reporting of suspicious transactions
21	Tipping-off and confidentiality
	Designated non-financial Businesses and Professions (DNFBPs)
22	DNFBPs: Customer due diligence
23	DNFBPs: Other measures
	E—TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENT
24	Transparency and beneficial ownership of legal persons
25	Transparency and beneficial ownership of legal arrangements
	F—POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURE
	Regulation and Supervision
26	Regulation and supervision of financial institutions
27	Powers of supervisors
28	Regulation and supervision of DNFBPs
	Operational and Law Enforcement
29	Financial intelligence units
30	Responsibilities of law enforcement and investigative authorities
31	Powers of law enforcement and investigative authorities
32	Cash couriers
	General Requirements
33	Statistics
34	Guidance and feedback
	Sanctions
35	Sanctions
	G—INTERNATIONAL COOPERATION
36	International instruments
37	Mutual legal assistance
38	Mutual legal assistance: freezing and confiscation
39	Extradition
40	Other forms of international cooperation

Source: Adapted from FATF (2019).

blockchain industry news sites. The following section analyzes how the FATF shapes the exercise of protocological control in regards to governance *of* blockchains generally and digital identity governance specifically. A third section highlights how forms of governance *by* blockchains shaped by the FATF paradoxically undermine the objectives of this organization of reducing illicit international financial flows. A final section summarizes and offers directions for future research.

HOW SOFT INTERNATIONAL LAW SHAPES THE *LOCATION* OF HARD CODE

The FATF was established in 1989 as part of inter-state efforts by the Group of 7 (G7) countries to stem global money laundering. It promulgated an initial 40 recommendations for supporting global anti-money laundering efforts (AML) that were supplemented with 9 special counter-the-financing-of-terrorism (CFT) recommendations following the 11 September 2001 attacks (**Table 2**). The task force issues official reports and guidance on the implementation of these 40 + 9 recommendations for countering the financing of the proliferation of weapons of mass destruction (FATF, 2018) and illicit wildlife trade (FATF, 2020c), as well as extending its recommendations to virtual currencies (FATF, 2015), virtual asset service providers (FATF, 2019) and digital identities (FATF, 2020e).

Scholarly literature has long debated the origins and impacts of FATF's activities (Gutterman and Roberge, 2019: 462; Tsingou, 2010; Hülsse, 2008; Hülsse and Kerwer, 2007; Truman and Reuter, 2004). On the one hand, are critiques of its symbolic "security theatre" as providing weak attempts to show member states that it is "doing something" about international money laundering and the financing of terrorism. On the other hand, FATF activities are regarded as successfully motivating a range of state and non-state actors to prioritize AML/CFT efforts while setting the requirements for the proper monitoring of identity systems in finance. These latter accounts stress how enforcement of the FATF's non-binding, voluntary standards relies on periodic monitoring of compliance with its 40 + 9 recommendations. When what the FATF calls "strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation" is identified, the Task Force enhances its monitoring.[4] However, it lacks direct enforcement mechanisms itself. Instead, the FATF issues warnings to exercise caution to its global network of 39 official state members, as well as non-members in its wider network of some 170 associate and observer members, and related regional bodies around the world. These warnings caution state and non-state actors globally about interacting with "Jurisdictions under Increased Monitoring" (the FATF's unofficial "grey list")[5] and countries on its unofficial FATF "blacklists"[6] The effectiveness of the FATF ultimately relies on peer pressure for its members and non-members alike to sanction jurisdictions on its unofficial lists. The FATF's power is thus *indirect*: it is a standard-setter and monitor rather than an enforcer. It *shapes* global regulatory responses, but it relies on others to develop and enforce them, including its member states, who have in turn tended to "deputize" banks and other financial market actors as AML/CFT enforcers to develop and undertake Know Your Customer (KYC) procedures (Amicelle, 2011; see more generally; Avant, 2005). Such enforcement-by-proxy entails a chain of enforcement in which the FATF relies on member states who in turn rely on market actors in their jurisdictions to implement the intergovernmental organization's guidance.

In this section, we build on and extend insights into the FATF's exercise of indirect power. We show how this IO shapes the location of protocological control by tracing the financial and formal lineage of global digital identity governance. The FATF, we argue, shapes the hard code of the computer protocols underpinning blockchain-based activities through soft international law issuance of guidance and recommendations. A first sub-section considers the impacts of the FATF, 2015 guidance on virtual currencies before a second examines the 2019 guidance on virtual asset service providers. Both of these "risk-based" guidances, we argue, shaped the *market-based* location of protocological control over blockchain technology. The FATF enabled private actors to take charge of monitoring the flow of blockchain transactions and the identities of the entities undertaking them. It has done so by guiding member-states towards letting market actors exercise protocological control in the emerging governance of digital identities. Although becoming more explicit, this steering towards private-led governance is in line with this IO's longerstanding risk-based approach that, as we elaborate, attempts to weigh the costs and benefits of greater public involvement in rapidly evolving technological changes. It is also in line with the wider approach towards innovation and the knowledge economy promoted by leading international organizations like the OECD, at whose Paris headquarters the FATF's secretariat is housed (Hasselbalch, 2018; Campbell-Verduyn and Hütten, 2019).

Guiding Protocological Control by Market Forces

While always a consideration in AML/CFT discussions (see for instance FATF, 2013), technology came to the forefront of FATF activities in the past half decade as financial technologies ("FinTech") and regulatory technologies ("RegTech") gained attention globally. The FATF launched a FinTech/RegTech Forum in 2017 for stimulating more effective monitoring and compliance with its 40 + 9 recommendations. The FATF's engagement with blockchain applications began earlier, with a 2014 report weighing the potential benefits and risks from virtual currencies, which included cryptocurrencies based on blockchain technology. The report specifically highlighted identity topics. On the one hand, the FATF (2014) flagged concerns about the anonymity provided by the technology, the limited possibilities for identification and verification of network participants, as well as a lack of clarity for formal regulatory responsibilities. On the other hand, the FATF (2014) also identified legitimate benefits such as lower transaction costs and possibilities for enhancing financial inclusion. Based on this initial risk assessment formal guidance on how its members should apply its 40 + 9 AML/CFT recommendations to virtual currencies was issued in 2015.[7]

[4]http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/.

[5]See for example https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2020.html.

[6]http://www.fatf-gafi.org/countries/d-i/iran/documents/call-for-action-june-2020.html.

[7]https://www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/?hf=10&b=0&s=desc(fatf_releasedate).

The 2015 FATF guidance shaped the location and form of protocological control across emerging blockchain-based activities in two interrelated ways. First, it downplayed the growing calls for *public* authorities to apply *direct* control. Instead, it recommended letting market actors develop appropriate protocols for ensuring AML/CFT controls. This recommendation emerged at a time when formal laws were emerging to restrict blockchain-based activities in member countries like Russia and China. As outright bans on the leading application of the technology to cryptocurrencies were being imposed in prominent jurisdictions, the FATF called for looser, "light touch" regulations. It waded off calls for strong "hands on" public control by not recommending formal regulation of blockchain applications. This was despite the growing gulf between AML/CFT identity requirements and the quasi-anonymity of many cryptocurrencies. The 2015 FATF guidance did call for close monitoring of cryptocurrency exchanges by member states. Yet FATF members and non-members alike were also encouraged to *avoid* formal bans and other actions that could lead blockchain activities shifting to less regulated jurisdictions. The guidance instead called for members to "take into account, among other things, the impact a prohibition would have on the local and global level of ML/TF risks, including whether prohibiting VC [virtual currency] payments activities could drive them underground, where they will continue to operate without AML/CFT controls or oversight" (FATF, 2015: 8–9).

In toning down the growing chorus of calls for "stricter" state regulation of blockchain-based activities, the 2015 FATF guidance on virtual currencies re-enforced the longstanding roles of private actors as enforcers of AML/CFT specifically, and the market-based location of protocological control generally. The 2015 FATF guidance extended the private-led development of standards of information communication in and between blockchain activities. Rather than state authorities, a range of competing start-up technology firms like Mastercoin, Counterparty and Interledger proposed manners of connecting together various protocols building on the Bitcoin protocol. Protocological control was equally left to market actors in governing the kinds of "forks" from the Bitcoin blockchain. The market-based competition led to what was dubbed a civil war in the 2017 "hard fork" of the original computer protocol that became Bitcoin Core (BTC) and Bitcoin Cash (BCH) (Coin Idol, 2019). The latter maintained the features and transaction history of the former protocol, while also introducing a fundamental change in acceptable standards of behavior: the ability to spin-off new protocols or "forks" from an existing protocol. The new BCH protocol then itself split in two as debates over the appropriate block size for recording verified transactions on the shared ledger led to the creation of both Bitcoin Cash Satoshi Version (SV) and Bitcoin Cash Adjustable Blocksize Cap (ABC) in late 2018. Whereas the development of these multiple, overlapping protocols was left to market forces, protocological control in the Ethereum blockchain was centralized in its Foundation and founder, Vitalik Buterin. A major flaw in the protocol of The DAO, a utopian experiment with automatic management of crowdsourced funds, led to a hack and withdrawal of the equivalent to $120 million raised in 2016 before informal centralized control was exercised to repair the underlying code (Hütten, 2019). A year later, the centralized group of "core" Ethereum developers formally adopted a previously informal set of rules in standardizing interactions between the disparate applications on this blockchain (Buntix, 2017). The adoption of what is still known as the "Ethereum Request for Comment" (ERC) number 22 further illustrated how protocological control was left to be exercised by non-state actors. This episode also highlighted the relevance of the identities of the programmers shaping these protocols. Departing from the substantial efforts Satoshi Nakamoto took to remain anonymous, developers behind blockchain protocols became increasingly public figures exercising protocological control over quasi-anonymous payment systems.

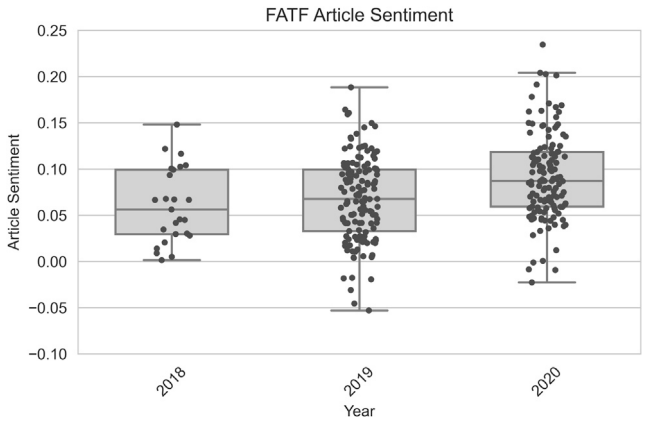
What the 2015 FATF guidance contributed to then was a *taming* of growing worldwide expectations that direct state control could, should and would be exercised over blockchain protocols in quarrels over questions of identity requirements. Key actors at the intersection of cryptocurrencies and fiat currency exchange became increasingly monitored. Yet, protocological control remained exercised by non-state actors. In the Bitcoin protocol debates of 2017 those users most able to harness computing power–the large "pools" of miners–exercised decision-making power in "forking" the original protocol. Similarly, the 2016 hack of The DAO saw a distributed community of users rally around the creator of Ethereum, then 24-year Russian-Canadian Vitalik Buterin, who undertook centralized amendment of this protocol. Both of these instances revealed the degree to which power and control remained market-based and how the FATF guidance did not *alter* non-state control but *extended* it, just as it would do again 4 years later.

Extending Protocological Control to New Markets

The 2019 FATF Guidance assembled fiat-to-cryptocurrency exchanges together with other actors linking real-world identities with the quasi-anonymous payments facilitated by blockchain protocols into a category called "virtual asset service providers" (VASPs). The FATF's guidance on extending its 40 + 9 recommendations to VASPs contained a controversial amendment to its 16th recommendation stipulating that financial institutions should collect and share customer information amongst one another.[8] The FATF specified that by June 2020 VASPs also implement the "travel rules" on customer information adhered to by other financial actors, like banks. The guidance specified that the following identity

[8]The recommendation that "financial institutions include required and accurate originator information, and required beneficial information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain". The Travel Rule's origins lie in a more than two-decades-old United States requirement that banks store and obtain customer information related to transactions above $3,000.

TABLE 3 | Industry reception of FATF guidance.



Note: Outcomes in boxplots differentiated by year illustrate general sentiments by blockchain industry actors. Sentiments are averaged of 184 articles from Coindesk and 142 articles collected from Cointelegraph. The scale ranges from -1 (most negative) to +1 (most positive) with 0 being neutral.

attributes should "travel" along the chain of transactions exceeding $1,000:

– "(i) originator's name (i.e., sending customer)
– (ii) originator's account number where such an account is used to process the transaction (e.g., the Virtual Asset wallet)
– (iii) originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth.
– (iv) beneficiary's name
– (v) beneficiary account number where such an account is used to process the transaction (e.g., the Virtual Asset wallet)" (FATF, 2019: 29)

The collection and transfer of such identity attributes stood in tension with the quasi-anonymous identity standards underpinning digital transactions in and across many blockchain protocols. As one article in the leading cryptocurrency news website *CoinDesk* put it, the extension of the Travel Rule to VASPs "goes against the grain to shoehorn an identity layer onto a technology specifically designed to be pseudonymous" (Allison, 2020a). The FATF guidance and its recommendation to extend the Travel Rule specifically was perceived by many industry actors as "excessively onerous to manage" and decried for the possibility that it "could drive the entire ecosystem back into the dark ages" (Weinberg in Hochstein et al., 2019).

Contrary to these views and critiques of the FATF's exercise of "draconian" power (Hamacher, 2019), however, the task force once again left protocological control to *markets* rather than state-controlled bodies. Notably, the FATF did not call for *public* entities to develop or enforce any set of uniform standards for identity information sharing between VASPs. Instead, the 2019 FATF guidance spurred an intense "race" between *market* players seeking to develop key standards for behavior underpinning digital identity systems that could enable VASPs comply with the Travel Rule and AML/CFT recommendations (De, 2019). Moreover, prior to the publication of the 2019 guidance, the FATF had engaged in a multi-year formal regulatory dialogue with industry actors. It gave dozens of so-called "identity start-up" firms opportunities to develop and test protocols for squaring the circle of, on the one hand, enabling VASPs to collect and transfer data on users, while on the other hand ensuring that user anonymity would remain protected (Henry et al., 2018). What we call a *protocol dialogue* involved industry-FATF deliberations on how protocols can and should be developed and applied *by blockchain start-ups and other technology companies*. The development of the FATF, 2019 guidance was summed up by the FATF Secretariat in an interview stating how "[w]e didn't want FATF to sit down and tell technical details of exactly how companies should comply with it because that would quickly become out of date." (Oki, 2019). Once again, the FATF steered protocological control towards the market rather than calling on member states themselves to develop key standards. The FATF governance *of* blockchain relied closely on governance *by* blockchain developers. **Table 3** provides an indication of how the aggregate reception of the 2019 FATF guidance grew more *positive* as fears of its "draconian" actions subsided.[9]

[9]We used automatized webscrapping with Python to collect articles mentioning the FATF from the leading blockchain media platforms CoinDesk and Cointelegraph utilizing the search feature of the respective sites. Documents were coded manually using the qualitative data analysis software NVivo 12 Plus treating the coding itself as part of the analysis (Basit, 2003). This means that we treated coding as a heuristic, more akin to an exploratory problem-solving technique (Saldana, 2009), starting with an *in vivo* approach that coded sections with a word or short phrase taken from each document. The sentiment analysis of the total 326 articles using Python TextBlob module to compare change over the three years containing the most attention to the FATF activities, 2018–2020. TextBlob assigns polarity values between −1 and 1 to certain words and word combinations in each article indicating if a sentence is more positive or more negative terms. Scores per word or word combination are predefined. For example, the word "great" receives a score of 0.8, the word "bad" scores −0.7, but a negation like "not bad" scores a 0.35. TextBlob then averages the all together for longer text and returns a total polarity value for each article (Schumacher, 2015). While a machine learning approach may yield better results, we used the data predominantly in an explorative fashion, limiting our approach to simple text processing.

A trio of caveats are necessary to clarify our central argument thus far regarding how FATF governance *of* blockchain activity through its formal guidance on virtual currency and virtual asset service providers impacted the *location* of protocological control. First, the FATF *itself* did not exercise protocological control but rather shaped the *location* where such control would be exercised. The task force did so by avoiding recommending public approaches encouraging top-down implementation of its AML/CFT recommendations. Instead, the task force sought to ensure that protocol development, implementation and control remained a more bottom-up affair with "identity" start-ups competing with one another. Second, guidance towards market- rather than government-led development of key standards of behavior to novel blockchain activities is an *extension* of the FATF's longstanding risk-based approach. The approach attempts to weigh the challenges and opportunities involved with implementing the 40 + 9 AML/CFT recommendations, recognizing that "harsher" clamp downs and even bans on certain activities may merely send illicit activities to other jurisdictions while undermining possible benefits of technological innovation. In the context of blockchains, the risk-based approach is one that weighs the risks of illicit activities with cryptocurrencies with the promises of financial surveillance offered by its underlying distributed ledger technology. Third, public actors and official policymakers were not absent, but actively encouraged private-sector standard-setting for squaring the circle of privacy and surveillance in blockchain activities. At the so called Virtual 20 (V20) event, held in parallel to the 2019 Group of 20 meeting in Japan, policymakers including ex-FATF President Roger Wilkins, Japanese Congressman Naokazu Takemoto and Taiwanese Congressman Jason Hsu were present in the signing of the national VASP industry agreement to co-develop standards for digital identities (Zmudzinski, 2019). Representatives from the United States Department of Homeland Security and Treasury Department's Financial Crimes Enforcement Network (FinCEN) were all present at the November 2019 Travel Rule Compliance Conference and Hackathon in San Francisco, California, where the Travel Rule Information Sharing Alliance (TRISA)- a private sector grouping consisting of some 50 blockchain firms and non-profits- pledged to develop "key technical solutions that include a directory of validated VASPs as well as a Certificate Authority (CA) model to ensure the public key cryptography".[10]

In summary, formal FATF guidance influenced the *location* where key standards of information communication between VASPs are developed: in the market rather than (international) state bureaucracies. The FAFT did *not* encourage either top-down or draconian enforcement of its legally non-binding standards. Rather its official guidance has recommended that key protocols and identity standards be persistently set by bottom-up *market* activities. The persistent stress on protocological control by market actors is in line with the wider spate of FATF activities and the organization's longstanding openness to private sector influence (Favarel-Garrigues et al., 2009; Amicelle, 2011; Liss and Sharman, 2015). Indeed, it has been argued that "the private sector—in particular the financial services industry and its high-level representatives—is becoming a "non-great power influencer in FATF" (Nance, 2018: 118). At the same time, former FATF personnel have joined efforts to develop "Travel Rule solutions", such as those offered by the Barbados-based Shyft Network (Allison, 2020b). What we identify as "protocol dialogue" was both present in the development of the 2019 guidance and its on-going implementation. Limits on the effective *form* of protocological control that the FATF helped steer in turn shape the intergovernmental organization's goal of preventing money laundering and the financing of terrorism.

FORM OVER FUNCTION: THE FRAUGHT EXERCISE OF PROTOCOLOGICAL CONTROL

In this section we highlight tensions between governance *of* blockchains and governance *by* blockchain. Specifically, we illustrate how the market-based *form* of protocological control the FATF has promoted fails to overcome the "pitfalls of private governance of identity" (Goanta, 2020; see more generally; Ronit and Schneider, 1999) and undermines the objectives reducing illicit finance in blockchain-based activities. While this argument can only be confirmed through analysis of events unfold over the coming years, we mobilize initial support for our position across two subsections. First, we point to the growing divide between standards of behavior in two spheres of blockchain-based activity, noting the development of *dualling identity protocols*. Second, we examine the 2020 FATF guidance on digital identities where we note a doubling down on the existing form of market-led protocological control. These trends, we contend, contribute to the fraught route towards global digital identity governance, one in which the reducing illicit activities appears increasingly unattainable.

Dualling Identity Protocols

Protocological control by market actors in blockchain activities has taken on a *dual* form undermining rather than addressing the goals of the FATF of reducing international illicit financial flows. Highly fragmented and split standards of behavior emerged for blockchain activities governed by market forces. On the one hand are protocols integrating the identity requirements of the Travel Rule. On the other hand, are protocols disregarding FATF recommendations and seeking to maintain the anonymity of their users. While both sets of protocols pledge to maintain user privacy, only the former incorporate blockchain-based activities into the identity requirements of the existing global AML/CFT regime. The latter protocols, meanwhile, push blockchain-based activities further out of the reach of formal remit of AML/CFT enforcement. This leads the very illicit activity the FATF is charged with reducing and stamping out to be progressively driven further into, rather than out of, the shadows of the "dark net". In elaborating this argument, we first detail the "dualling identity protocols" before situating their importance in the emergence of global digital identity governance.

[10]https://trisa.io/trisa-momentum-announcement/.

Protocological control is exercised by some market actors in ways that closely accord with FATF guidance. Here user identity information is collected and exchanged between and beyond VASPs in ways that closely resemble the more established forms of centralized governance that blockchains originally arose to bypass and counter. Centralized messaging platforms for "VASPs to share encrypted transmittal information with each other securely and privately" are provided by firms like Taiwan-based Sygna.[11] Other start-ups such as Coinfirm, Netki, Shyft and KYC Chain all provide similar "solutions" and are based on private or permissioned blockchain protocols with centralized gatekeepers akin to those of traditional digital systems. Even purportedly "decentralized" solutions offered by blockchain alliances and associations take-on degrees of centralized control. A prominent example is the Travel Rule Information Sharing Alliance, an association of more than 50 entities "focused on security and interoperability between the travel rule standards and protocols".[12] In December 2019, this alliance developed the Intervasp Messaging Standard 101 (IVMS-101) standard (Allison, 2020d), described as "a universal common language for communication of required originator and beneficiary information between VASP"[13]. In May 2020, InterVASP was launched as a technical standard providing a common language for communication between originator and beneficiary VASPs.[14] Such private sector-self governance closely emulates longstanding types of global associations of highly centralized financial exchanges like the World Federation of Exchanges (McKeen-Edwards, 2010).

Further steps towards "decentralized" peer-to-peer solutions being developed also contain persistent elements of centralization. For example, certificates holding transacting users' Personally Identifiable Information are maintained by centralized authorities. TransactID is overseen by California-based Netki, while the free open-source peer-to-peer VASP Address Confirmation Protocol is developed by California-based CipherTrace,[15] which sells the above type of "forensic tool" for the United States Department of Homeland Security.[16] These "blockchain forensics tools" developed to extend CFT/AML standards clearly recentralize in collaborating not only with traditional financial intermediaries, but also with governments (Nelson, 2020). The degree of such collaboration became apparent in a leaked 2019 report provided to the United States Financial Crimes Enforcement Network[17] and other financial regulators by the Cryptocurrency Indicators of Suspicion (CIOS) Working Group, a network of blockchain intelligence firms, exchanges and big banks that detailed dozens of illicit patterns of transactions on blockchain along with a "road map" for tackling them (del Castillo, 2019). Given these connections, it is not inconceivable that these firms enable the sharing of customer information not only between VASPs, but also with law enforcement and intelligence agencies, many of whom are their clients or prospective future clients. Sharing of such information would replicate the kinds of longstanding relationships between such agencies and banks (Amicelle, 2011), the latter of whom are also developing protocols such as Travel Rule Protocol developed between Dutch bank ING, British bank Standard Chartered and United States brokerage firm Fidelity (Allison, 2020e).

A parallel form of protocological control is exercised by market actors *eschewing* customer identification and information sharing requirements and pushing blockchain activity further from official regulatory remit. So-called "privacy protocols" Cashshuffle/Cashfusion,[18] Enigma,[19] Lelantus, MimbleWimble, OpenBazaar and others being tested like Lelantus (Powers, 2020a) provide enhanced standards of anonymity that do not attempt to maintain compliance with either AML/CFT or the Travel Rule customer identification and information exchange requirements. While some protocols here aim for compliance with FATF recommendations and are incorporating blockchain-based activities into formal global AML/CFT governance,[20] most protocols push blockchain-based activities further out of the reach of formal remit of AML/CFT enforcement. The FATF, 2019 guidance has affected what we label the *protocol selection* of VASPs undertaking selective, *ad hoc* compliance with AML/CFT rules. For example, fit-to-cryptocurrency exchanges have delisted cryptocurrencies whose protocols facilitate high standards of anonymity. OKEx Korea confirmed in 2019 that it would halt trading of privacy-coins Monero (XMR), Dash (DASH), Zcash (ZEC), Horizen (ZEN) and Super Bitcoin (SBTC), citing grounds of conflicts with FATF guidelines (Suberg, 2019). Nonetheless, around a third of the top 120 exchanges themselves were found in a survey to have little in the way of AML/CFT controls themselves (Palmer, 2019).

Protocol selection leads to patterns of illicit activity the FATF is charged with reducing and stamping out to be driven deeper into the shadows of the "dark net." Blockchain intelligence firm CipherTrace, for example, reported in 2020 that some 90% of suspicious transactions in cryptocurrencies were being missed by financial institutions (Haig, 2020). The FATF itself lamented these trends in a September 2020 report on "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing." This report was based on more than one hundred

[11]https://www.sygna.io/blog/types-of-fatf-r16-crypto-travel-rule-solutions/.

[12]https://trisa.io/.

[13]https://intervasp.org/.

[14]https://trisa.io/.

[15]https://ciphertrace.com/travel-rule-info-sharing-architecture/.

[16]https://ciphertrace.com/ciphertrace-announces-worlds-first-monero-tracing-capabilities.

[17]Which issued and began immediately enforcing a version of the Travel Rule for United States-based exchanges in 2019.

[18]https://github.com/cashshuffle/spec/blob/master/CASHFUSION.md.

[19]https://enigma.co/.

[20]For example the "trust framework" released by Norwegian start-up Notabene in June 2020 reportedly provides a know-your-customer (KY) through "elements of decentralized identity management to link blockchain addresses to verified profiles" (Allison, 2020c). Switzerland-based OpenVASP, to which Notabene is a member, coordinates the development of a protocol based on Ethereum that "puts privacy of transferred data at the center of its design". It suggests the use of a peer-to-peer messaging system called Whisper which "employs so-called dark routing to obscure message content and sender and receiver details to observers, a bit like anonymous web browsing Tor" (Allison, 2020a). Here identity management is undertaken by a smart contract-based "blockchain public key directory for the VASP and an IBAN-like numbering format: the virtual asset account number" (ibid).

case studies of what it noted are "indications of suspicious activities or possible attempts to evade law enforcement detection" (FATF, 2020b: 5). Meanwhile, FATF's 1 year progress survey of the status of Travel Rule extension to VASPs reported that despite "progress in the development of technological standards for use by different travel rule solutions," there was less implementation of the Travel Rule than other AML/CFT standards (FATF, 2020d: 11). The uneven outcome was blamed on a lack of "sufficient holistic technological solutions for global travel rule implementation that have been established and widely adopted." (FATF, 2020d: 12). Recognizing the "decentralisation ethos that underpins virtual assets, there appears to be a general desire for multiple potential solutions, rather than one centralised travel rule solution." (ibid.). The FATF stressed how the "usage of common standards will assist in ensuring different solutions are interoperable" (ibid.) and called upon "the VASP sector to redouble its efforts towards the swift development of holistic technological solutions encompassing all aspects of the travel rule" driving technology convergence (ibid.). Given the widely reported "struggle to implement" the non-binding "rule" around the world, a 1-year "sunrise period" review extension was granted to VASPs (Bryanov, 2020). By mid-2020, it was reported that authorities in 35 of 54 jurisdictions had implemented Travel Rule standards into domestic legislation and that another 19 had not yet done so (FATF, 2020d). The FATF doubled down on the roles of market actors and emphasized the need for "quick development of technology solutions" (FATF, 2020c: 12).

Governance *of* blockchain by the FATF shaped the *location* of protocological control in ways that allow for the persistent obscuring of identities in blockchain-based activities such as quasi-anonymous payments. Wasabi Wallet, for example, was launched in 2018 to scramble transactions and is based on "secret contracts." In contrast to the smart contracts in Ethereum, secret contracts have nodes capable of calculating data without ever "seeing" them (EC3 Cyber Intelligence Team, 2020). The Secret Network launched a bridge between its privacy-focused blockchain and Ethereum in late 2020 (Powers, 2020b). Europol cited such "privacy-enhanced wallet services" as a "top threat" in its 2020 Internet Organized Crime report.[21] Meanwhile, so-called "decentralized exchanges" (DEXs), developed largely on Ethereum protocols, expanded as increasingly important forums for users to meet and build some semblance of trust in arriving at peer-to-peer agreements to directly exchange cryptocurrency without the use of a formal intermediary or verifying of identities. While still representing a small percentage of overall cryptocurrency trading at the time of writing (around one per cent), the aggregate monthly volumes on DEXs hit records in 2020. British defense and security think-tank RUSI warned that DEXs "have the potential to weaken the role of centralized VASPs and so blunt the effect of governmental regulation" (Moiseienko and Izenman, 2019: viii). The largest DEX by value exchanged, Uniswap, had digital tokens equivalent to more than $1 billion trade in September 2020, yet neither listing rules nor KYC verification procedures (Madeira, 2020). DEXs thus stood at the same crossroad of dualling identity standards as the FATF (2021) proposed in draft guidance published in March 2021to consider them "high-risk" VASPs if they did not implement the Travel Rule standards. The draft guidance also highlighted a number of new "elements of risk," including "[e]xposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR), the Invisible Internet Project (I2P) and other darknets, capable of further obfuscating transactions or activities and inhibiting a VASP's ability to know its customers and implement effective AML/CFT measures" (FATF, 2021: 15).

In sum, the key risk is that "harsher," "hands-on," state-led restrictions on blockchain activities have the potential to merely *shift* rather than *reduce* illicit activities has emerged in part due to the FATF's shaping of private-sector led exercise of protocological control. While risks pertain to any and all forms of governance, the risks of bottom-up governance strategies are well known now more than a half decade into the FATF's governance *of* blockchain. Calls began to emanate in 2020 for "developing entirely new approaches to manage money laundering and terrorist financing risks" by key industry players (Sian Jones quoted in Allison, 2020f). Without tabling a completely new approach, the FATF (2021) did nevertheless propose some substantial changes in draft guidance published in 2021 that suggested self-regulatory bodies were insufficient for VASP supervision and only "competent authorities" (FATF, 2021: 5) could act as supervisors. The draft guidance proposed in March 2021 also suggested new Principles of Information-Sharing and Co-operation Amongst VASP Supervisor that "[g]iven the pseudonymous, fast-paced, cross-border nature of VAs [Virtual Assets], international co-operation is all the more critical between VASP supervisors." It called for a more "proactive" roles for supervisory authorities rather than self-regulatory industry organizations (FATF, 2021: 94). Even though the six principles the FATF outlined were general and the proposed guidance emphasised in bold that they are non-binding, the draft guidance proposed in March 2021 marked a shift in the FATF's emphasis on closer international cooperation between public supervisors. This shift was emphasized by its guidance, issued just a year earlier, for digital identity (DID) systems. A May 2020 report on how "effective authentication of customer identity for authorizing account access" can enhance "certain elements of customer due diligence (CDD) under FATF Recommendation 10" (FATF, 2020a: 5–7), had still largely called for market-based exercise of protocological control. It recommended member states to leave standard setting to non-state actors, even when using the standards for their own government backed DIDs.[22]

[21]https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

[22]Government authorities should be "supporting the development and implementation of reliable, independent digital ID systems by auditing and certifying them against transparent digital ID assurance frameworks and technical standards, or by approving expert bodies to perform these functions. Where authorities do not audit or provide certification for IDSPs themselves, they are encouraged to support assurance testing and certification by appropriate expert bodies so that trustworthy certification is available in the jurisdiction" (FATF, 2019: 6).

Government authorities were also recommended to remain "flexible" and merely monitor "the rapid evolution of digital ID technology" in order to "help promote responsible innovation and future-proof the regulatory requirements," as well as to support "the development and implementation of reliable, independent digital ID system" along with "assurance testing and certification by appropriate expert bodies."[23] The thrust of the May 2020 guidance persistently focused on ensuring "multi-stakeholder" solutions through constructs such as regulatory "sandboxes" where government authorities monitor private sector trials rather than lead them in any meaningful way. The March 2021 proposed guidance suggesting greater public supervisory cooperation marked a departure from the longstanding emphasis on market-based governance. Future research will have to determine whether the former proposals were mere blips in the longer trend emphasizing the latter.

CONCLUSION: PERSISTENT FORM AND UNACHIEVABLE OUTCOMES?

How can we understand the progressive, piecemeal emergence of global digital identity governance? This paper advanced a two-pronged argument that highlighted the need to consider interactions between governance *of* and *by* blockchains. First, formal governance by the FATF has shaped the "financial route" to global digital identities. Building on its governance *of* financial flows, the FATF has extended its risk-based approach to digital identity. Second, this model of leaving the reins of governance to blockchain developers and start-up firms is fraught with problems. The persistent encouragement of a reliance on market actors in developing blockchain protocols has led to the development of what we identified as dualling identity protocols, or the situation in which some activities are underpinned by standards of activity adhering to AML/CFT rules while others are not at all in accordance with such standards. The persistence of the latter, we argued, undermines FATF goals of reducing rather than just shifting illicit international financial flows. Tensions thus exist and persist between governance *by* and *of* blockchains. Blockchain studies, and emerging literatures on digital identity governance, need to consider the interplay between both forms of governance and how they interact in (un)predictable manners in order to come to a clearer understanding of the roots and evolving forms of digital identity governance.

Future studies should maintain a critical focus on the activities of the FATF and other international organizations, particularly those that have become increasingly vocal about using blockchain to "fight fire with fire," (Lagarde in Wilmoth, 2018) as the former IMF Managing Director Christine Lagarde put it in a 2018 speech. The shaping of protocological control by formal standard-setting organizations is essential to investigate in relation to informal modes of control in developing more nuanced understandings of global digital identity governance. The 2020 "Global Standards Mapping Initiative" of the World Economic Forum and Global Blockchain Business Council, for instance, flagged digital identity as one of the five main areas where overlapping standards have led to gaps in other places (World Economic Forum, 2020). The formal activities of IOs like the International Standards Organization (ISO) require much further attention going forward, especially regarding its various blockchain working groups.[24] Further scholarship would identify whether and how these IOs influence the location and forms of protocological control. They should provide normative assessments of the shifting forms, impacts and limits such forms of control have on actually stemming illicit activity, as well as on socio-economic development more widely. Finally, the extent to which the forms of protocological control shaped by the FATF and other global north rich country clubs can also be effectively contested and challenged by actors in the global south deserves further investigation. In sum, there are promising and pressing research pathways for future studies to explore at the intersection of governance *by* and *of* blockchains.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

MH benefited from funding by the Hans-Böckler-Stiftung, Project number 2017-437-2.

ACKNOWLEDGMENTS

We thank Oskar Gstrein for the invitation to contribute to these debates. We are also grateful for feedback from Gary Robinson, as well as participants in workshops "Anticipatory Global Governance: International Organisations and Political Futures" held at the EISA European Workshop in International Studies, Kraków, June 2019, and "Algorithmic Knowledge in Culture and Media" held at the Open University of Israel, Tel Aviv, October 2019. The usual disclaimers apply.

[23]https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf.

[24]https://www.iso.org/committee/6266604.html.

REFERENCES

Allison, I. (2020b). Binance Throws Weight behind Shyft Network in 'Travel Rule' Standards Race. Available at: https://www.coindesk.com/binance-throws-weight-behind-shyft-network-in-travel-rule-standards-race (Accessed November 6, 2020).

Allison, I. (2020d). Crypto Firms Establish Messaging Standard to Deal with FATF Travel Rule. Available at: https://www.coindesk.com/crypto-firms-establish-messaging-standard-to-deal-with-fatf-travel-rule (Accessed November 6, 2020). doi:10.1515/9780822377245

Allison, I. (2020f). *FATF Needs Entirely New Approach to Regulating Crypto, Says V20 Summit*. New York City, NY: Coindesk.

Allison, I. (2020c). Identity Startup Notabene Launches Exchange Tool for FATF Travel Rule Compliance. Available at: https://www.coindesk.com/crypto-identity-startup-notabene-launches-trust-framework-for-fatf-travel-rule (Accessed November 6, 2020). doi:10.1515/9780822377245

Allison, I. (2020e). In Banking First, ING Develops FATF-Friendly Protocol for Tracking Crypto Transfers. Available at: https://www.coindesk.com/in-banking-first-ing-develops-fatf-friendly-protocol-for-tracking-crypto-transfers (Accessed November 6, 2020). doi:10.1515/9780822377245

Allison, I. (2020a). Inside the Standards Race for Implementing FATF's Travel Rule. Available at: https://www.coindesk.com/inside-the-standards-race-for-implementing-fatfs-travel-rule (Accessed November 6, 2020).

Amicelle, A. (2011). Towards a 'new' Political Anatomy of Financial Surveillance. *Secur. Dialog.* 42 (2), 161–178. doi:10.1177/0967010611401472

Atzori, M. (2017). Blockchain Technology and Decentralized Governance: Is the State Still Neccesary? *J. Govern. Regul.* 6, 1–62. doi:10.22495/jgr_v6_i1_p5

Avant, D. (2005). *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press. doi:10.1017/cbo9780511490866

Basit, T. (2003). Manual or Electronic? the Role of Coding in Qualitative Data Analysis. *Educ. Res.* 45 (2), 143–154. doi:10.1080/0013188032000133548

Boakye-Adjei, N. Y. (2020). Covid-19: Boon and Bane for Digital Payments and Financial Inclusion. Available at: https://www.bis.org/fsi/fsibriefs9.pdf (Accessed November 6, 2020).

Bryanov, K. (2020). Slow but Steady: FATF Review Highlights Crypto Exchanges' Struggle to Meet AML Standards. Available at: https://cointelegraph.com/news/slow-but-steady-fatf-review-highlights-crypto-exchanges-struggle-to-meet-aml-standards (Accessed November 6, 2020).

Buntix, J. P. (2017). ERC20 Token Standard Officially Formalized by Ethereum Developers. Available at: https://themerkle.com/erc20-token-standard-has-now-been-officially-formalized-by-the-ethereum-developers/ (Accessed November 6, 2020).

Campbell-Verduyn, M. (2018b). "Towards a Block Age or Blockages of Global Governance?," in *Bitcoin and beyond: Cryptocurrencies, Blockchains, and Global Governance* (New York: Routledge), 178–197.

Campbell-Verduyn, M. (2018a). Bitcoin, Crypto-Coins, and Global Anti-money Laundering Governance. *Crime Law Soc. Change* 69 (2), 283–305. doi:10.1007/s10611-017-9756-5

Campbell-Verduyn, M., and Hütten, M. (2019). Anticipating Decentralization through Protocological Control: International Organizations and the Standardization of Blockchain Technology within Financial/Security Infrastructures," in Finance/Security Infrastructures workshop, November 13 (New York City, NY: University of Amsterdam).

Campbell-Verduyn, M., and Hütten, M. (2020). Is the Travel Rule Good or Bad for Crypto? Both. Available at: https://www.coindesk.com/is-the-travel-rule-good-or-bad-for-crypto-both (Accessed November 6, 2020). doi:10.1057/s41268-020-00198-5

De Filippi, P. (2018). "Blockchain : a Global Infrastructure for Distributed Governance and Local Manufacturing" in *The Mass Distribution of Almost Everything*. Editor T. Diez (Spain, Institute for Advanced Architecture of Catalonia). doi:10.3917/puf.filip.2018.01

De, N. (2019). CipherTrace Enters Race to Solve Crypto's FATF Compliance Headache. Available at: https://www.coindesk.com/ciphertrace-enters-race-to-solve-cryptos-fatf-compliance-headache (Accessed November 6, 2020).

del Castillo, M. (2019). Crypto's Valachi Papers. Available at: https://www.forbes.com/sites/michaeldelcastillo/2019/12/04/cryptos-valachi-papers/?sh=1a8637dd3117 (Accessed November 6, 2020).

Eaton, B., Hedman, J., and Medaglia, R. (2018). Three Different Ways to Skin a Cat: Financialization in the Emergence of National E-ID Solutions. *J. Inf. Technol.* 33, 1–83. doi:10.1057/s41265-017-0036-8

EC3 Cyber Intelligence Team (2020). Cyber Bits. Available at: https://www.coindesk.com/wp-content/uploads/2020/06/1_5096130532387848318.pdf (Accessed November 6, 2020).

Faria, I. (2021). The Market, the Regulator, and the Government: Making a Blockchain Ecosystem in the Netherlands. Finance and Society, earlyView. doi:10.1109/blockchain.2019.00067

FATF (2020d). 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (Accessed November 6, 2020).

FATF (2020e). Digital Identity. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (Accessed November 6, 2020).

FATF (2019). DRAFT GUIDANCE ON DIGITAL IDENTITY. Available at: https://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Digital%20ID-public-consultation-version.docx (Accessed March 25, 2020).

FATF (2021). Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf (Accessed March 24, 2021).

FATF (2018). FATF Guidance on Counter Proliferation Financing. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf (Accessed November 6, 2020).

FATF (2015). Guidance for a Risk-Based Approach: Virtual Currencies. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (Accessed November 6, 2020).

FATF (2020a). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Available at: www.fatf-gafi.org/recommendations.html (Accessed November 6, 2020).

FATF (2020c). Money Laundering and the Illegal Wildlife Trade. Available at: http://www.fatf-gafi.org/media/fatf/documents/Money-laundering-and-illegal-wildlife-trade.pdf ([Accessed November 6, 2020).

FATF (2013). Prepaid Cards, Mobile Payment and Internet-Based Payment Services. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf (Accessed November 6, 2020).

FATF (2020b). Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf (Accessed November 6, 2020).

FATF (2014). Virtual Currencies - Key Definitions and Potential AML/CFT Risks. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (Accessed November 6, 2020).

Favarel-Garrigues, G., Godefroy, T., and Lascoumes, P. (2009). *Les sentinelles de l'argent sale au quotidian: Les banques aux prises avec l'antiblanchiment*. Paris: La Decouverte. doi:10.3917/dec.favar.2009.01

Frazier, L. (2020). Already Leaning towards Digital Money, Covid-19 Pushes More People towards Contactless Payments. Available at: https://www.forbes.com/sites/lizfrazierpeck/2020/08/21/already-leaning-towards-digital-money-covid-19-pushes-more-people-towards-contactless-payments/?sh=70317e13012a (Accessed November 6, 2020). doi:10.2172/1763531

Galloway, A. R. (2004). *Protocol: How Control Exists after Decentralization*. Cambridge, Massachusetts: MIT press. doi:10.7551/mitpress/5658.001.0001

Goanta, C. (2020). The Private Governance of Identity on the Silk Road. *Front. Front. Blockchain.* 3, 4. doi:10.3389/fbloc.2020.00004

Gutterman, E., and Roberge, I. (2019). "The Financial Action Task Force: Fighting Transnational Organised Crime, Money Laundering, and the Limits of Experimentalist Governance," in *In* Handbook Of Organised Crime And Politics. Editors F. Allum and S. Gilmour (Northampton, Massachusetts: Edward Elgar Publishing Limited)), 455–467. doi:10.4337/9781786434579.00043

Haig, S. (2020). Banks Failing to Identify up to 90% of Suspicious Crypto Transactions. Available at: https://cointelegraph.com/news/banks-failing-to-identify-up-to-90-of-suspicious-crypto-transactions (Accessed November 6, 2020).

Hamacher, A. (2019). CipherTrace and Shyft Unveil a Fix for Draconian FATF Anti-terrorism Rules. Available at: https://news.yahoo.com/ciphertrace-shyft-unveil-fix-draconian-131045661.html (Accessed November 6, 2020). doi:10.1007/978-3-662-59008-9

Hasselbalch, J. A. (2018). Innovation Assessment: Governing through Periods of Disruptive Technological Change. *J. Eur. Publ. Pol.* 25 (12), 1855–1873. doi:10.1080/13501763.2017.1363805

Henry, C. S., Huynh, K. P., and Nicholls, G. (2018). Bitcoin Awareness and Usage in Canada: An Update. Available at: https://www.bankofcanada.ca/wp-content/uploads/2018/07/san2018-23.pdf (Accessed November 6, 2020).

Herian, R. (2018). *Regulating Blockchain: Critical Perspectives in Law and Technology*. London: Routledge. doi:10.4324/9780429489815

Hochstein, M., De, N., and Baydakova, A. (2019). Beyond KYC: Regulators Set to Adopt Tough New Rules for Crypto Exchanges. Available at: https://www.coindesk.com/beyond-kyc-global-regulators-appear-set-to-adopt-tough-new-rules-for-crypto-exchanges (Accessed November 6, 2020).

Hooper, A., and Holtbrügge, D. (2020). Blockchain Technology in International Business: Changing the Agenda for Global Governance. *Ribs* 30 (2), 183–200. doi:10.1108/ribs-06-2019-0078

Hülsse, R. (2008). Even Clubs Can't Do without Legitimacy: Why the Anti-money Laundering Blacklist Was Suspended. *Regulation & Governance* 2 (4), 459–479. doi:10.1111/j.1748-5991.2008.00046.x

Hülsse, R., and Kerwer, D. (2007). Global Standards in Action: Insights from Anti-money Laundering Regulation. *Organization* 14, 5625–5642. doi:10.1177/1350508407080311

Hütten, M. (2019). The Soft Spot of Hard Code: Blockchain Technology, Network Governance and Pitfalls of Technological Utopianism. *Global Network* 19 (3), 329–348. doi:10.1111/glob.12217

Idol, Coin. (2019). Hard Fork: Motivations Fueling Bitcoin Civil War. Available at: https://coinidol.com/bitcoin-civil-war/ (Accessed March 25, 2021).

Jones, K. (2019). Blockchain in or as Governance? Evolutions in Experimentation, Social Impacts, and Prefigurative Practice in the Blockchain and DAO Space. *Ippologia* 24 (4), 469–486. doi:10.3233/ip-190157

Liss, C., and Sharman, J. C. (2015). Global Corporate Crime-Fighters: Private Transnational Responses to Piracy and Money Laundering. *Rev. Int. Polit. Econ.* 22 (4), 693–718. doi:10.1080/09692290.2014.936482

Madeira, A. (2020). The Rise of DEXs: Fueled by DeFi and Ready to Disrupt the Status quoAccessed. Available at: https://cointelegraph.com/news/the-rise-of-dexs-fueled-by-defi-and-ready-to-disrupt-the-status-quo (Accessed November 6, 2020).

McKeen-Edwards, H. (2010). "World Federation of Exchanges" in *Handbook of Transnational Economic Governance Regimes*. Editors C. Tietje and A. Brouder (Leiden: Martinus Nijhoff Publishers), 489–500.

Moiseienko, A., and Izenman, K. (2019). *From Intention to Action - Next Steps in Preventing Criminal Abuse of Cryptocurrency*. London, United Kingdom: RUSI Occasional Paper.

Naheem, M. A. (2019). Exploring the Links between AML, Digital Currencies and Blockchain Technology. *Jmlc* 22 (3), 515–526. doi:10.1108/jmlc-11-2015-0050

Nance, M. T. (2018). The Regime that FATF Built: an Introduction to the Financial Action Task Force. *Crime Law Soc. Change* 69, 109–129. doi:10.1007/s10611-017-9747-6

Nelson, D. (2020). Inside Chainalysis' Multimillion-Dollar Relationship with the US Government. Available at: https://www.coindesk.com/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government (Accessed November 6, 2020).

Oki, H. (2019). 'Not Everyone Is Happy but We Have to Move on,' Some Challenges to the FATF's New Guidance. Available at: https://cointelegraph.com/news/not-everyone-is-happy-but-we-have-to-move-on-some-challenges-to-the-fatfs-new-guidance (Accessed November 6, 2020).

Palmer, D. (2019). A Third of Crypto Exchanges Have Little or No KYC, Says CipherTrace. Available at: https://www.coindesk.com/a-third-of-crypto-exchanges-have-little-or-no-kyc-says-ciphertrace (Accessed March 25, 2021). doi:10.1136/bmjspcare-2019-huknc.60

Pavlidis, G. (2020). International Regulation of Virtual Assets under FATF's New Standards. *J. Invest. Compl.* 21 (1), 1–8. doi:10.1108/JOIC-08-2019-0051

Powers, B. (2020a). *Secret Network Launches Bridge to Bring Transactional Privacy to Ethereum*. New York City, NY: Coindesk.

Powers, B. (2020b). Zcoin Employs Burn-And-Redeem Privacy Model, Offering Alternative to Coinjoins. Available at: https://www.coindesk.com/privacycoin-zcoin-burn-redeem-testnet (Accessed November 6, 2020).

Reijers, W., O'Brolcháin, F., and Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledge* 1, 134–151. doi:10.5195/ledger.2016.62

Ronit, K., and Schneider, V. (1999). Global Governance through Private Organizations. *Governance* 12, 243–266. doi:10.1111/0952-1895.00102

Saldana, Johnny. (2009). *The Coding Manual for Qualitative Researchers*. Thousand Oaks, California: Sage Publications ltd.

Schumacher, A. (2015). TextBlob Sentiment: Calculating Polarity and Subjectivity. Available at: https://planspace.org/20150607-textblob_sentiment/ (Accessed November 6, 2020). doi:10.1007/978-3-658-10702-4

Suberg, W. (2019). OKEx Korea Delists Monero, Dash, Privacy-Cryptos over FATF Demands. Available at: https://cointelegraph.com/news/report-okex-delisting-monero-dash-privacy-cryptos-over-fatf-demands (Accessed November 6, 2020).

Truman, E. M., and Reuter, P. (2004). *Chasing Dirty Money: Progress on Anti-money Laundering*. Washington: Institute for International Economics.

Tsingou, E. (2010). Global Financial Governance and the Developing Anti-money Laundering Regime: what Lessons for International Political Economy? *Int. Polit.* 47 (6), 617–637. doi:10.1057/ip.2010.32

Wilmoth, J. (2018). 'Fight Fire with Fire': IMF Chief Lagarde Calls for Blockchain-Powered Bitcoin Regulation. Available at: https://finance.yahoo.com/news/fight-fire-fire-imf-chief-185347015.html (Accessed March 25, 2021).

World Economic Forum (2020). Global Standards Mapping Initiative: An Overview of Blockchain Technical Standards. Available at: http://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf (Accessed November 6, 2020).

Zmudzinski, A. (2019). Group of Digital Asset Trade Associations to Establish Global Cryptocurrency Association. Available at: https://cointelegraph.com/news/group-of-digital-asset-trade-associations-to-establish-global-cryptocurrency-association (Accessed November 6, 2020).

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright © 2021 Campbell-Verduyn and Hütten. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

DuEPublico

Duisburg-Essen Publications online

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

ub universitäts bibliothek

This text is made available via DuEPublico, the institutional repository of the University of Duisburg-Essen. This version may eventually differ from another version distributed by a commercial publisher.

DOI: 10.3389/fbloc.2021.627641
URN: urn:nbn:de:hbz:465-20220314-120629-0

This work may be used under a Creative Commons Attribution 4.0 License (CC BY 4.0).