

University of Groningen

Enrolling into Exclusion

Campbell-Verduyn, Malcolm; Giumelli, Francesco

Published in:
Journal of Cultural Economy

DOI:
[10.1080/17530350.2022.2028655](https://doi.org/10.1080/17530350.2022.2028655)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2022

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):
Campbell-Verduyn, M., & Giumelli, F. (2022). Enrolling into Exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure. *Journal of Cultural Economy*, 15(4), 524-543. <https://doi.org/10.1080/17530350.2022.2028655>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.



Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure

Malcolm Campbell-Verduyn & Francesco Giumelli

To cite this article: Malcolm Campbell-Verduyn & Francesco Giumelli (2022) Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure, Journal of Cultural Economy, 15:4, 524-543, DOI: [10.1080/17530350.2022.2028655](https://doi.org/10.1080/17530350.2022.2028655)

To link to this article: <https://doi.org/10.1080/17530350.2022.2028655>



© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group on behalf of Academy of Criminal Justice Sciences.



Published online: 11 Apr 2022.



[Submit your article to this journal](#)



Article views: 1464



[View related articles](#)




[View Crossmark data](#)



Citing articles: 4 [View citing articles](#)

Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure

Malcolm Campbell-Verduyn^{a,b} and Francesco Giumelli ^a

^aDepartment of International Relations and International Organization, University of Groningen, Groningen, The Netherlands; ^bKäte Hamburger Kolleg Centre for Global Cooperation Research, University of Duisburg-Essen, Duisburg, Germany

ABSTRACT

There is growing debate over whether applications of blockchain and other financial technologies ('fintechs') reinforce forms of neo-colonial extraction that perpetuate North–South inequities or help enact decolonial ambitions across the Global South. This paper expands such discussions and contributes to this special issue on 'fintech in Africa' by situating emerging African blockchain techno-experimentation within wider international infrastructural relations. We argue that blockchain-based activities in and across the African continent must be understood within those also unfolding in countries that have been subjected to financial sanctions of varying types (China, Iran, Russia, Venezuela) by the European Union, United States, and United Nations. Our analysis traces how blockchain-based applications by sanctioned countries are extending exclusions in novel and existing socio-technical relations. We conclude that blockchain-based experiments are facilitating rather than displacing a colonial finance/security infrastructure.

ARTICLE HISTORY

Received 11 July 2021

Accepted 21 December 2021



KEYWORDS

Digital finance; fintech; infrastructure; sanctions; security; technology

Introduction

Financial technologies ('fintech') generally, and the blockchain technologies underlying 'cryptocurrencies' and other forms of 'decentralized finance' (DeFi) in particular, are being carefully and critically analyzed in the pages of this journal and beyond (Dallyn 2017, Grossman 2019, Nelms 2016, O'Dwyer 2019). Nuanced cultural economy study of blockchain, however, has tended to focus on applications of this set of digital technologies mainly in the Global North, where formal regulation is rapidly evolving (Faria 2019, 2021, Faustino 2019). As part of the wider 'turn to technology' in development more generally (Bernards 2019), less formal techno-financial experimentation is rapidly expanding across the Global South. In September 2021, the *Financial Times*, for example, exclaimed that 'developing countries provide fertile ground' for cryptocurrencies (Wheatley and Klasa 2021).

Claims that, for Africa in particular, the 'future is crypto' (Dana 2020) have been materializing in both formal and informal experiments across the continent that are based, to varying degrees, on the blockchain technologies underlying cryptocurrencies. Framed as a 'liberation technology' (Levine 2020) these blockchain-based trials ostensibly seek to fulfill a 'desire for financial autonomy' (Handagama 2021a) from Senegal to Ethiopia, as cryptocurrency adoption by individuals is said to

CONTACT Malcolm Campbell-Verduyn  m.a.campbell-verduyn@rug.nl  Oude Kijk in 't Jatstraat 26, 9712 EK Groningen, The Netherlands

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group on behalf of Academy of Criminal Justice Sciences. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

be ‘blowing up’ (Handagama 2021b, Kobo 2021). Meanwhile, governments and central banks from South Africa to Tunisia have been officially exploring blockchain-based central bank digital currency (CBDC) (Michael 2021, Handagama 2021a).¹ Most prominently, the Central Bank of Nigeria launched a CBDC trial of the ‘eNaira’ on the country’s independence day in 2021 (Iyatse 2021). Widespread techno-euphoria has encouraged these and other experiments with blockchains as ‘the answer to Africa’s problems’ (AllAfrica InfoWire 2021).

Yet, despite considerable hype, the small but growing scale of blockchain-based fintech experimentation in Africa and across the Global South raises larger and longer standing questions. Do digital technologies actually contribute to decolonial ambitions? Does fintech merely reinforce forms of neo-colonial extraction and perpetuate North–South inequities as well as international power asymmetries? The launch of blockchain-based fintech projects and ‘education campaigns’ by foreign-based multinational organizations, such as the ‘pan-African’ cryptocurrency called the AFRO, which was launched by a Swiss-based organization in 2018 (Afro Foundation 2021, Wright 2021), accentuate concerns over what in an earlier pre-blockchain age Herzfeld (2002) referred to as ‘crypto-colonialism’ (see also Campbell-Verduyn *et al* 2021, Crandall 2019, Howson 2020, Jutel 2021, Scott 2016).²

This article expands existing debates over such wider concerns by situating this special issue’s focus on fintech in Africa within wider *international infrastructural relations* in and beyond the African continent. We show how the core exclusionary practice of sanctioning is being reproduced across blockchain-based fintech experiments undertaken in sanctioned countries of varying size and geographical locations. Examining unfolding blockchain-based financial activities in China, Iran, Russia, and Venezuela, we place rapidly evolving efforts to enact Africa as ‘the next frontier for cryptocurrency’ (Rao 2018) in the growing shift of blockchain experimentation from Global North to the Global South. We argue that critical cultural economy analysis of blockchain must consider the evolving conditions under which blockchain and cryptocurrencies, adoption is emerging in, in attempts to ostensibly overcome existing power asymmetries.

In 2020, the two largest sub-Saharan African economies, South Africa and Nigeria, came in at seventh and eighth, respectively, on a Top 10 list of leading ‘crypto-jurisdictions’ (Chainalysis 2020). This list revealed how growing blockchain-based fintech experimentation across the African continent is occurring in a *wider international* context being shaped by a diverse, yet very particular, grouping of countries. Ukraine, Russia, Venezuela, and China were the top four jurisdictions identified as leading cryptocurrency adoption. Despite their differences, these four countries shared three important features: first, they were each subjects of international sanctions by the United States, European Union, and United Nations; second, they are sites of systematic efforts to harness cryptocurrencies or their blockchain technologies to *escape* these international sanctions, and; third, they are themselves involved in what have been identified as neo-colonial forms of involvement in Africa’s digital fintech ‘frontier’ (Gravett 2020).

International sanctions are key political acts that punish through exclusions (Sullivan 2020, Giumelli 2011). They are designed to, for example, cut off access to the financing necessary for conducting trade. A longstanding set of practices, sanctions today exclude individuals, firms, or entire jurisdictions from international trade and credit (Giumelli 2015). They are mainly imposed on countries in the Global South by the European Union (EU) and United States (US). Yet, China and Russia also increasingly undertake these exclusionary practices, including through the very blockchain technologies that we show are being harnessed to escape sanctions. Financial sanctions are a core feature of what Marieke de Goede (2020) refers to as an international finance/security infrastructure. Elaborating the relational understandings of the term developed in Science and Technology Studies (STS), finance/security infrastructures are open and durable sets of relations between human and non-human actors. Such infrastructures are, however, neither *entirely* open nor *completely* durable: they both persistently exclude and continually change, often in ways that are poorly understood and can even remain unnoticed. As De Goede (2020) stresses, persistent colonial exclusions have been ‘hard-wired’ into finance/security infrastructures over time. Growing

blockchain-centered fintech experimentation across the Global South, this article illustrates, re-wire exclusionary set of relations in ways that *extend* rather than overcome colonial legacies of the existing finance/security infrastructure. We therefore inject skepticism into whether such techno-experimentation can contribute to African decolonial ambitions.

Our analysis proceeds across five sections. A first section elaborates the STS-informed insights informing what a second section identifies as a profoundly neo-colonial existing finance/security infrastructure. A third section then traces blockchain applications emerging in and across China, Iran, Russia, and Venezuela. We show how this international techno-experimentation is extending exclusionary possibilities and practices by sanctioned countries *themselves* who are drawing on far less open and inclusive variants of blockchain technology. A penultimate section illustrates how blockchain-based attempts to escape international exclusions by sanctioned countries are in turn prompting the US and EU to further expand longstanding exclusions and power asymmetries. A final section re-iterates our call for cultural economy analysis to consider the decolonial possibilities of fintech by scrutinizing formal techno-experimentation across the Global North in relation to what are often more informal trends in the Global South through STS-inflected notions of infrastructures.

Infrastructural relations

Infrastructures are typically regarded as closed and static ‘things’ worthy of attention mostly for their failures, both real and potential, such as electrical grids. In Science and Technology Studies (STS), by contrast, infrastructures are more dynamic and evolving sets of socio-technical *relations*. This relational conception sees infrastructure as an ‘on-going accomplishment’ (Feldman 2000) and a ‘dynamic, unfolding process’ in which *entanglements* are ‘the primary unit of analysis rather than the constituent elements themselves’ (Emirbayer 1997). These entanglements, as Rella (2020, p. 239) writes in the pages of this journal, are ‘always already cultural and symbolic artifacts animated by cultures and promises associated with their use.’ In other words, infrastructural relations must always be situated in time and place. Before elaborating on the contemporary finance/security infrastructure, we lay out four general characteristics of infrastructural relations that are essential to our analysis of decolonial possibilities of blockchain-based fintech.

First and foremost, infrastructures are characterized by *openness*. This openness is not absolute, but relative. When contrasted with, for example, the far more closed digital ‘platforms’ where specific actors are in charge of determining access (Plantin *et al* 2018), it is essential to stress that no one individual or set of actors, even hegemonic states, are ‘really in charge of infrastructure’ (Star 1999). Openness, nevertheless, entails that certain states, corporations, and other non-state actors can ‘close,’ curtail, or exclude access to infrastructural relations. What the openness of infrastructural relations means, then, is that such exclusions are never complete. As the existing finance/security infrastructure illustrates, sanctioned entities typically still have some access to alternative forms of international credit and possibilities for international trade. The key point here is that there is no one central point enabling access to the evolving sets of relations that together make up an infrastructure.

Second, infrastructures consist of *durable relations* that are not easily displaced or ‘disrupted.’ STS accounts emphasize the ‘installed base’ of infrastructures (Star 1999). Like their openness characteristic, in which exclusion remains possible, durability still entails the possibility of evolution, though less revolution, in infrastructural relations. Change in infrastructures occurs incrementally and in relation with attempts to form *new* infrastructural relations. In other words, infrastructures are never entirely static ‘forever affairs’; they evolve in unpredictable ways as attempts to establish ‘new’ relations are incorporated into existing relations. Infrastructural evolution can thereby stem from attempts to create more open alternatives. Yet, this evolution is not pre-determined: change occurs in often unanticipated manners that can either extend exclusions and undermine the openness of an infrastructure, or can expand openness

and enhance inclusions in socio-technical relations. As the case of blockchain illustrates, attempts to enact more open infrastructural relations can be re-purposed for extending exclusions in novel ways not initially considered in the founding and original development of a technology.

A third characteristic of infrastructures is their *facilitation of core activities*. This feature is typically emphasized in the more general designation of specific infrastructures as ‘critical’ by policy-makers (e.g. Organization for Economic Co-Operation and Development 2008, *Critical 5* 2014). State security concerns are central to these designations. Digital infrastructures, for example, are ‘critical’ because they make state infrastructures vulnerable to hacking and ransomware attacks. What the notion of ‘critical infrastructure’ typically downplays, however, is a stress on the profound entanglement *between* the core activities that infrastructures facilitate. Financial infrastructures, for instance, provide (in)security through practices ranging from modeling future risks to the materiality of money itself (de Goede 2012, Gilbert 2017, Kessler 2011, Lobo-Guerrero 2016). As we elaborate below, the practice of applying sanctions illustrates the entanglements of core activities in both an existing, as well as an emerging, finance/security infrastructure.

A final key characteristic of infrastructures is their *obscurity*. In STS terms, infrastructural relations are ‘black boxed,’ with the socio-technical nature of the relations they facilitate often backgrounded. Yet, just as periods of crisis can expose and reveal the operation of complex systems, infrastructural relations become foregrounded as they are (re-)constructed and (re-)constituted. This is what Pinzur (2021) refers to as ‘ongoing contributions to the web of relations and practices that comprise an infrastructure in action.’ Finance, and particularly cross-border payments, are as Rella (2020, p. 237) also writes ‘comparatively less “infrastructured” than domestic payments. Hence, the dynamics at play in the design and deployment of money infrastructures can be observed with greater clarity.’ What Rella identifies as ‘money infrastructure’ can both internationalize and digitize the exclusionary degrees of longer standing, backgrounded socio-technical relations. In foregrounding the obscure relations between human and non-human actors, the next section assesses change and continuity in the socio-technical relations that have underpinned a neo-colonial finance/security infrastructure.

A neo-colonial finance/security infrastructure

In an STS-inflected sense, then, infrastructures are open and durable sets of relations between human practices and non-human objects that facilitate certain core activities. This understanding of infrastructure can usefully situate the exclusions exemplified by the practice of sanctioning within longer and wider historical trajectories.

The extraterritorial application of sanctions, as existing scholarship has stressed, supports and extends asymmetric power relations between hegemonic and non-hegemonic countries (Rodman 1995, Mallard 2019, Matera 2020). With the often silent consent of a wider group of nation-states, represented today by the likes of the EU, sanctions by hegemonic countries such as the US contribute to and consolidate ‘neo-colonial’ legacies in relations between the Global North and Global South. Countering the tendency in sanctions literature to theorize hegemony as *distinct* from imperialism,³ however, sanctioning practices by hegemonic powers and their allies are situated here in lineages with past practices of exclusions that were formally established in the colonial period and have become ‘hard-wired’ into an increasingly digital era (de Goede 2020). The *durability* of socio-technical relations characterized infrastructural exclusions from credit under formal colonialism is a key feature of contemporary ‘postcolonial poverty finance’ (Bernards *forthcoming* 2022). Despite its *relative openness*, today’s finance/security infrastructure persistently excludes entire countries and tracks of the Global South.

Sanctions also extend exclusions as key practices in the *facilitation of core activities* by the existing finance/security infrastructure. Since secure access to credit flowed from metropolis’ of the Global North to the Global South in the colonial era, international financial relations have remained

dominated by the leading financial centers of hegemonic powers and designed ‘to keep the least risky, most profitable activities (providing remittances, lending to government, and making advances to large merchants or businesses) for the banks, while offloading risks associated with crop prices, disease, or bad weather onto smaller traders and, ultimately, onto peasant producers’ (Bernards *forthcoming* 2022). These relations of exclusion have persisted beyond the formal colonial era through activities that are typically *obscured* yet become more widely apparent in practices like sanctioning. As de Goede (2020) observes, sanctions reveal ‘the unseen technical financial payment infrastructures of global finance’ that are weaponized ‘in pursuit of particular security agendas’ as ‘the very infrastructures of payment, financial flows, and banking access are appropriated, reformed, and rerouted through sanctions.’ Rendering international payments ‘difficult, cumbersome, and expensive,’ sanctions today continue to be ‘depriving citizens and companies around the world infrastructurally’ (de Goede 2020).

Granted, the exclusions of finance/security infrastructural relations can serve to *counter* neo-colonial relations. Apartheid-era sanctions on South Africa serve as a leading example here. Our central point, however, is the very act of (dis)abling access to credit is central to the *relatively* – and never completely – open finance/security infrastructure. Sanctions highlight persistent and profound exclusions and inequalities between the Global South and Global North that have continually characterized the existing finance/security infrastructure.⁴

A final key point to emphasize before turning to the case of blockchain-based fintech is that both the enforcement and evasion of sanctions are imbedded in infrastructural relations between state, non-state actors, and technical objects. On the one hand, the socio-technical relations underpinning the existing finance/security infrastructure facilitate attempts to *enforce* international sanctions. The same banks ‘deputized’ (Amicelle 2011) by leading sanctioning countries to enforce financial exclusions are often the very ones that are caught up in breaches of sanctions. Efforts to enhance the effectiveness of international sanctions draw on technologies, like those digital algorithmic technologies making ‘Big Data’ (EY Global 2019), in seeking to ensure that banks do not process financial transactions from sanctioned entities. On the other hand, sanctioned jurisdictions also turn to digital technologies in order to escape international sanctions (Hufbauer *et al* 2020). Like infrastructures more generally, the existing finance/security infrastructure *evolves in unanticipated manners*. Technologies that identify the customers of banks and financial services firms who are required to conduct Know Your Customer (KYC) and to perform ‘due diligence’ checks on transactions and assess potential risks often have their very own blind spots. For instance, the Big Data technologies embraced by international banks have not prevented the processing of customer transactions with sanctioned entities, major oversights that have led to the levying of billion dollar fines by American regulators.⁵

In short, technologies, including the blockchains and cryptocurrencies we turn to next, can work to ‘enroll’ seemingly novel practices into existing relations by both facilitating and undermining other practices like sanctions. Importantly, however, technology on its own does little. The impacts of technological change on practices like sanctioning need to be understood as part of wider socio-technical relations underlying evolving finance/security infrastructures, including in our increasingly digital era.

Escaping yet extending exclusions

Blockchains are distributed ledger technologies enabling the peer-to-peer transaction, verification, and publication of digital objects. Experimentation with blockchain technologies, we argue, is paradoxically enabling both the escape and extension of the very exclusions and power asymmetries characterizing leading Global North countries’ restrictions of credit flows towards Global South jurisdictions. In this section, we first illustrate how the advent and evolution of blockchain technologies since 2009 has provided a range of very real *possibilities* for evading international sanctions and undertaking less exclusionary practices. We then trace the still very limited extent to which

applications of blockchain technologies in and across jurisdictions subjected to varying types of sanctions – China, Iran, Russia, and Venezuela – have actually enabled the evasion of such exclusions. Drawing on developments reported in both specialized English-language cryptocurrency and general financial media up until November 2021,⁶ we contend that the still small scales of blockchain-based sanctions evasion remain significant in their highlighting of novel extensions of exclusionary practices. To elaborate this argument, two interrelated variations on the original Bitcoin blockchain are first necessary to distinguish.

A first key variation in blockchains is in the ‘types’ of centralization and control maintained over participation in these digital networks. At one extreme are the original ‘permissionless’ blockchains open to anyone with Internet access. The Bitcoin blockchain is the most prominent example here. At the other extreme are ‘permissioned’ blockchains where a gatekeeper(s) control network access. So-called distributed ledger technologies (DLTs) are typically permissioned. Of central importance to our argument is that the latter type of blockchains are largely being drawn upon by sanctioned states. This ‘type’ of blockchain is that inherently more exclusionary than the original permissionless form.

The second key element of variation in blockchains enabling extensions of exclusion is in the varying level of anonymity offered. What analysts refer to as ‘sanctions resistance through cryptocurrency technology’ (Fanusie 2018) is enabled by the anonymity provided by cryptography underpinning blockchains. As the oft-cited author(s) of the technical specifications for developing Bitcoin argued, the privacy appeal of cryptocurrency is the ability to ‘see that someone is sending an amount to someone else, but without information linking the transaction to anyone’ (Nakamoto 2008, p. 6). To ensure such anonymity is maintained, so-called ‘mixers’ or ‘tumblers,’ like Wasabi, that seek to prevent individual identity tracking by ‘coinjoining’ transactions together into unpredictable combinations, have emerged (New Money Review Staff 2020). Other cryptocurrencies promise complete anonymity by employing further encryption techniques to fully conceal transaction histories. Monero, Zcash, and Zerocoin allow actors to ‘convert funds into crypto, anonymize it, and then cash out.’ Cashing out typically then occurs via fiat-to-cryptocurrency exchanges that typically enforce only very basic ‘Know Your Customer’ regulations, although these are growing, as we detail below. Further possibilities for maintaining anonymity include exchange via darknet markets. For example, the Russian-language darknet marketplace, Hydra (Allison 2021), as well as the Secret Network that provides a ‘bridge’ for turning cryptocurrencies developed on the second largest blockchain, Ethereum, into privacy-enhanced ‘secret tokens’ (Wright 2020b). Table 1 provides a simplified overview of key actors and objects whose relations have the potential to form alternative blockchain-based infrastructural relations.

The novel socio-technical relations enabled by blockchain technologies interact with the set of relations underpinning the existing finance/security infrastructure in several manners. Most prominently, a host of financial actors *within* sanctioned jurisdictions serve as ‘relations between socio-technical relations.’ Once wary of cryptocurrencies, banks in both sanctioned and sanctioning countries have increasingly dealt with these and other applications of blockchain technologies, serving as ‘connecting threads’ between older analog and newer digital infrastructural relations. For example, banks in the jurisdiction sanctioned by the US for the longest period, Cuba, process

Table 1. Blockchain-based privacy-enhancing products, services and processes.

Category	Description	Examples
<i>Exchanges</i>	Centralized institutions that undertake increasing but still little to no KYC	Bisq, Bitshares, Bitsquare, Coinbase
<i>Mixers</i>	Transactions bundled together in unpredictable combinations	Laundry and Bitcoin Fog, CoinJoin
<i>PrivacyCoins</i>	Further encryption conceal transaction histories	Monero, Zcash, Zerocoin
<i>Privacy Protocols</i>	Enable the build of new privacy instruments	Lelantus MimbleWimble
<i>Wallets</i>	Enable the receiving and sending of cryptocurrencies in secure manners	zkSnacks; Samourai Wallet, Wasabi Wallet, Dark Wallet

remittances in cryptocurrencies through new financial exchanges such as Fusyon, a local exchange ‘distinctively designed’ for the country (Heasman 2019), that provides a ‘lifeline’ for ordinary Cuban citizens (The Economist 2021).

Similarly, both large and small domestic firms in sanctioned jurisdictions are enrolling novel blockchain-based activities into the socio-technical relations underpinning the existing finance/security infrastructure. Efforts to harness blockchain to bypass US sanctions have been spurred by Iranian multinationals, such as the Kish Free Zone organization, which proposed local cryptocurrency mining as a manner of funding car imports (ArzDigital 2020). Smaller firms in Iran have accepted cryptocurrency payments, including the 70-year old Persian Shoes that attracted international media attention for accepting payments in Bitcoin (Barrier 2013). The manners in which attempts at developing new socio-technical relations are enrolled in the existing finance/security infrastructure is further exemplified by an Iranian blockchain-based digital currency backed by gold called PayMon. In 2019, four Iranian banks along with the exchange Iran Fara Bourse signed up to use the gold-backed cryptocurrency (Financial Tribune 2019). Cryptocurrencies have also been drawn upon to enable international investment in Iran, such as by the Swedish government, which authorized a local blockchain startup to invest in Iran through Bitcoin (Mizrahi 2017).

Facilitating Bitcoin activities in ways that enable the evasion of international sanctions to a still limited degree, blockchain-based activities in Iran are significant for the ways they reproduce a key exclusionary element of the existing finance/security infrastructure. Private sector activities of Iranian banks and other firms that had been tacitly supported by the national government began to be actively controlled by the internal and international activities of the Iranian government. Facing domestic power outages and seeking to cut down on the high energy consuming production of cryptocurrencies, the government shut down cryptocurrency mining activities (Thomson 2021). This left only a few officially registered Bitcoin production ‘farms,’ many of which are controlled by Chinese investors (Baydakova 2021a), to generate an estimated \$1 billion worth of cryptocurrency used to pay for imports via the Central Bank of Iran (Financial Tribune 2021, Robinson 2021, Sinclair 2021). Internationally, the Iranian government has proposed blockchain-based payments systems based on religious exclusion, for instance with Muslim-majority forming countries trading in an Islamic cryptocurrency. Other international activity has been based on activities between Iran and a constrained remit of countries. For example, in 2018 the heads of the Iranian parliamentary commission on economic affairs and Russian Federation Council Committee on Economic Policy emphasized the prospect of using cryptocurrencies to bypass US sanctions in enabling international commodity exchange (Tetkin 2018). This call was echoed in a 2020 statement by Iranian General Saeed Muhammad, that ‘[t]o circumvent sanctions, we must develop solutions such as the exchange of products and the use of cryptocurrencies with our partnerships [in other countries]’ (Wright 2020a). Which countries are included and excluded from such exchange was not specified. The point is that blockchains are not being harnessed in an entirely open and permissionless manner, but in their permissioned form where certain actors remain excluded. In this sense, the turn to blockchain technologies is enabling the reproduction, albeit in novel manners, of exclusions upon which the existing finance/security infrastructure is based.

Developments in Venezuela provide another example of how blockchain technologies enable a thus far limited degree of sanctions evasion, while reproducing the central exclusionary elements of the existing finance/security infrastructure. The Venezuelan government launched a cryptocurrency called the Petro in 2018 as an explicit effort to ‘overcome the [US] financial blockade’ (President Maduro cited in McDowell 2020), as well as to ‘advance in issues of monetary sovereignty, to make financial transactions and overcome the financial blockade’ (President Maduro cited in Buck 2017). The Petro was developed in a joint venture between Venezuelan and Russian officials seeking to erode sanction power and bypass the existing financial/security infrastructure (Bull and Rosales 2020). The internationalization of the Petro has been government-led, with official offers of discounts on oil purchased in Petro made to countries like India. The Venezuelan government has

also sought to attract foreign investors (Zuckerman 2018) from countries like Poland and Norway, as well as authorized the use of an app to convert Bitcoin to US dollars via partners in countries such as China (Cointelegraph 2021a) and Russia (Cointelegraph 2021b). Yet, these funds are ultimately deposited as US dollars in government-controlled bank accounts in those countries (Suberg 2019). While bypassing key elements of the existing finance/security infrastructure, this is a very limited extent effort to harness blockchain-based fintech that is also reliant on other elements of the existing finance/security infrastructure (e.g. conversion to dollars). It also reproduces the exclusionary nature of the finance/security infrastructure through the centralized control of the ‘cryptocurrency’ created and maintained by the Venezuelan government.

Blockchain activities in Russia further exemplify how hitherto limited attempts to harness blockchain technologies to escape sanctions reproduce exclusions of an existing finance/security infrastructure. The Russian government in 2017 had what a former CIA analyst framed as a second ‘Sputnik moment,’ when a domestic scientific institution successfully tested a blockchain platform that could withstand hacking from a quantum computer (Fanusie and Zilberman 2017). The aim to make the country ‘a global leader’ in the technology was tied to making Russia ‘able to withstand America’s economic sanctions tools in the future’ (Fanusie and Zilberman 2017). Yet, Russian blockchain-based sanctions evasion has yet to materialize, with attempts do so instead extending exclusions. The second largest blockchain, Ethereum, underpins a private permissioned intra-bank information exchange platform called Masterchain. This closed digital exchange network was developed by the Russian FinTech Association under the auspices of the Bank of Russia. It is positioned ‘as a part of the next-generation financial infrastructure’ (Naumoff 2016) involving a few countries selected from the Eurasian Economic Union (Milano 2018). Similarly, a digital ruble began being developed in 2018 in order to ‘settle accounts with our counterparties all over the world, with no regard for sanctions’ as economic adviser to President Putin, Sergei Glazyev, put it (cited in Cappozzalo 2018). A prototype e-ruble is slated for trial between Russian banks in a ‘mega-project’ (Baydakova 2021b) geared to becoming an ‘integral part of national settlements by 2023 or 2024’ (Partz 2021a). Granted, the Russian government has proposed several more inclusive international blockchain-based initiatives that would ‘connect some of the most promising emerging market economies stretching across Asia, Eastern Europe, Africa, and South America, via blockchain and smart contract technology by using a new multinational cryptocurrency to be collectively adopted by the BRICS and the Eurasian Economic Union (EEU) countries (Member States)’ (Ozelli 2018). Such blockchain ambitions are continually being hinted at by Russian officials. For example, a 2021 proposal called for a blockchain-based alternative to the Belgium-based Society for Worldwide Interbank Financial Telecommunications (SWIFT), the technical messaging system linking together international banks at the center of the finance/security infrastructure (Nelson 2021). While this particular alternative has yet to materialize, Russia has turned to another exclusionary set of socio-technical relations by engaging China’s Cross-Border International Payments System (CIPS). The CIPS processed \$3.77 trillion in international financial transactions in 2018. While still ‘nowhere close to rivaling SWIFT’ according to a 2019 US Congressional report (Bartholomeuw *et al* 2019 and more generally Green and Gruin 2021), the CIPS reproduces the ability to exclude entities from payments and financial access. Rather than a ‘new’ and more *open* socio-technical relation within a ‘alternative’ finance/security infrastructure, the CIPS is merely a further attempt to replace one exclusionary set of exclusions with another.

Although not yet subject to the more extensive sanctions that some of its individual members have faced (Barret *et al.* 2020), the Chinese government has been ‘prudently enthusiastic’ about blockchain (Jia and Zhang 2018). The communist government included the technology as a priority project in its Thirteenth Five-Year National Informatization Plan in 2016 (Gruin 2021). It launched a Blockchain Services Network (BSN) in March 2020 to coordinates trials of the technology within China, as well as between ‘portals’ hosted by countries like Turkey and Uzbekistan (Gkritsi 2021). These experiments have most prominently included a blockchain-based CBDC. Formally called the digital currency/electric payment (DCEP), the digital yuan has attracted a great deal of attention for

its perceived attempt to enable and enforce the country's ability to provide and access credit broadly framed under the notion of 'financial sovereignty' (Aredy 2021, Tran 2020). A reported \$9.5 billion of digital yuan transactions were conducted as of October 2021 by 140 million users, including banks and citizens in several large cities, as well as the international financial centers of Shanghai and Hong Kong. The digital yuan is enabled by the technology of several large technology firms and banks, yet remains centrally controlled by the People's Bank of China (PBoC) and its concern with enforcing 'capital controls and border monetary policy' (Avan-Nomayo 2021, Fanusie and Logan 2019, Reuters 2021). In fulfilling a broader stated aim at 'optimizing the country's cryptocurrency infrastructure' (Day 2020), the internationalization of digital yuan is at once the clearest attempt to develop a new finance/security infrastructure *and* of reproducing the exclusionary nature of the existing finance/security infrastructure. In 2021, the PBoC revealed the plans for a 'universal digital payments network' (UDPN) for enabling 'international transfers and payments with and between central bank digital currencies' (Phillips 2021). Yet, what became the Multiple Central Bank Digital Currency Bridge (m-CBDC) project has only linked Hong Kong, Thailand, and the United Arab Emirates in a wider plan to establish the DCEP as the pan-Asian payments infrastructure underpinning trade across the One Belt One Road (OBOR) initiative (Crawley 2021). Beyond Asia, meanwhile, adoption of the digital yuan in Africa is being enabled through the introduction of smartphones with hardware wallets, facilitating use of the DCEP and which build on Huawei and other Chinese technology firms' dominant position in mobile handset production and networks across the continent (Kimani 2021). There are plans to ensure that the digital yuan is only accessed through fingerprint identification technology (Pan 2021b), reflecting the persistent ability to exclude access to the CBDC, for instance, to dissidents. Once again, attempts to escape international sanctions through blockchain technology reproduce in novel digital neo-colonial form the exclusions characterizing the existing finance/security system.

In sum, despite considerable *potential*, emerging blockchain fintech applications in and across sanctioned countries have thus far led only to small scale sanctions evasion that we argue is more significant to the extent that these efforts extend exclusions characterizing existing infrastructural relations. At times hyperbolic claims about blockchain applications facilitating sanctions evasion (e.g. Barone and Masciandaro 2019, Teichmann and Falker 2021) point to both the cases that we noted here, as well as wider illicit activities being facilitated through applications of these technologies. Most prominent here is blockchain-based money laundering (Campbell-Verduyn 2018) and international attention-grabbing revelations, such as a \$250 million scheme set up by North Korea-linked actors in 2018 (Zagaris and Bannister 2020). These wider activities and still-limited attempts at evading significant international sanctions provide *possibilities* for enrolling a growing range of African blockchain-based activities into persistently exclusionary infrastructural relations. Nigeria, where cryptocurrency activity has boomed despite an official ban (Baydakova 2021c), for example, announced in 2018 a yet-to-materialize plan to establish a 'Free Crypto Currency Economic Zone' with Russia.⁷ Nigerian businesses have engaged in small scale cryptocurrency-denominated trade with China (Hertig 2020). Both Chinese and Russian firms have further facilitated the adoption of cryptocurrency and blockchain technology by mining companies operating in the Democratic People's Republic of Congo and the creation of digital platforms such as ModulTrade in Burkina Faso (Phillips 2018). Efforts to circumvent sanctions by Venezuela, meanwhile, have implicated countries like Egypt (Blockchain Tech 2018).

Ostensibly 'alternative' blockchain-based activities emerging in and across sanctioned countries, which we summarize in Table 2, *reproduce*, albeit in different manners, the exclusionary relations characterizing the very finance/security infrastructure they seek to counter. What still small-scale blockchain-enabled efforts to escape international sanctions are more importantly contributing to, then, is a *furthering* of the historical exclusions characterizing the coloniality of the existing finance/security infrastructure. While not *necessarily* neo-colonial, emerging blockchain-based efforts appear unlikely to enhance African decolonial ambitions. Varying in the extent to which they are being 'enrolled' into 'alternative' socio-technical relations, the African 'fintech frontier'

Table 2. Emergent blockchain-based infrastructural relations.

	China	Iran	Russia	Venezuela
Central Bank Activities	Digital currency/electric payment (DCEP)	National blockchain platform Borna	Digital ruble	Petro
Industry Activity	Bank trials of digital yuan, technology firm participation in creation	PayMon backed by gold and 4 banks and an exchange	Masterchain Financial messaging system	Cryptocurrency production through National Digital Mining Pool
Other government activity	Blockchain Services Network	Calls for Muslim cryptocurrency, exploration of cryptocurrency use with eight countries	Calls for Eurasian Economic Union blockchain usage	Incentives to use Petro in international oil purchases
International linkages	BRICS agreement; DCEP internationalization with Multiple Central Bank Digital Currency Bridge; investments in Iranian Bitcoin mining	2019 trilateral blockchain cooperation agreement with Russia and Armenia	BRICS agreement; Shanghai Cooperation Organisation blockchain research	Russian government involvement in Petro development

risks extending exclusions characterizing a digitizing yet still neo-colonial finance/security infrastructure. This is most prominently illustrated by the growing blockchain-based infrastructural relations between Chinese and African firms in settling a still very small degree of international trade in cryptocurrency (Hertig 2020). While still limited in scope, these developments point to how African fintech ambitions are becoming enrolled into persistently exclusionary socio-technical relations. They are also significant in the extent to which have sparked wider concern in American national security think tanks about ‘how China seized the initiative on blockchain’ (Murray 2021). As the next section proceeds to detail, emerging blockchain-based attempts to *escape* sanctions are not only reproducing exclusions themselves, but are spurring further efforts to draw on this technology in *extending* exclusionary practices underpinning the existing finance/security infrastructure.

Enforcing and extending exclusions

Finance/security infrastructures, like all infrastructures, are not static. The open, permanent ledger of transactions originally provided by blockchain technologies offer means not merely for *evading* international sanctions, but also of *enforcing* them. These twin possibilities are materializing hand-in-hand. Efforts to escape sanctions through blockchain have instigated attempts at enforcing these exclusions in official experimentation with the technology across the Global North. While relatively small-scale, blockchain-based sanctions evasion has instigated growing uses of this very same set of evolving technologies for *extending* the exclusions at the core of the existing neo-colonial finance/security infrastructure. The manners in which blockchains are underpinning exclusionary socio-technical relations in the existing finance/security infrastructure is most prominently reflected by the development and expansion of an international blockchain intelligence industry.

A flurry of ‘data analytics’ firms have arisen since 2015 that harness blockchains to develop profiles of illicit cryptocurrency transactions and users. These profiles and tracking services are sold to sanctioning governments, intergovernmental police organizations, and multinational firms, including most of the large international banks. The blockchain intelligence industry consists of both small start-ups (Table 3), as well as larger and longer existing multinational firms (Table 4) whose activities and personnel are tightly interlinked with its governmental, corporate, and international security services clients. Like other areas of financial governance, there is considerable overlap as well as a ‘revolving door’ between the blockchain intelligence industry and sanctioning governments. This overlap was revealed in a 2019 report provided to the U.S. Financial Crimes Enforcement Network⁸ and other financial regulators that a Cryptocurrency Indicators of Suspicion (CIOS) Working Group consisting of blockchain intelligence firms, exchanges, big banks had

Table 3. Selected blockchain intelligence industry start-ups.

Company & Headquarters	Selected Products and Services	Selected Clients and Partners
Bitfury, Amsterdam, Netherlands	<i>Crystal</i> , connecting virtual wallets to real-world identities	Police; FICO
Blockchain Intelligence Group, Canada	<i>Qualitative Law Enforcement Unified Edge</i> 'enables investigators to quickly and visually follow the virtual money' ¹⁵	US Department of Homeland Security Illicit Finance and Proceeds Crime Unit
Chainalysis, Switzerland	<i>Rumker</i> blockchain transaction tracing, real-time suspicious cryptocurrency transaction alert system, boasting capacity to trace most 'privacycoin' transactions	Barclays, Europol, US Department of Homeland Security, Department of Justice, OFAC
CipherTrace, California, USA	<i>Armada</i> cryptocurrency transaction tracing ($n = 700$) & user deanonymization	Canada Revenue Agency, Malta Financial Services Authority
Coinfirm, London, UK	Real-time cryptocurrency monitoring and investigative tools identifying transaction patterns	Ripple
Elliptic, London, UK	<i>Discovery</i> targeted for bank compliance teams to identify flows of funds on crypto assets	FBI, banks like Santander, Internet Watch Foundation
Guardtime, Switzerland	<i>Black Lantern</i> AML/CTF Platform,	KPMG
Netki, California, USA	<i>OnboardID</i> automated facial recognition	IBM
Scorechain, Luxemburg	<i>Scorechain Artificial Intelligence (SCai)</i> makes a prediction about entity types when it is related to Darkweb marketplaces	HSBC, RBC, ING, BNP Paribas

detailed dozens of illicit patterns of transactions on blockchain along with a 'road map' for tackling them (del Castillo 2019). Another illustration of the overlapping relations between regulators and industry personnel was the April 2021 appointment to Acting Director of the Financial Crimes Enforcement Network of the United States Department of the Treasury (FinCen) of the previous Chief Technical Counsel of Chainalysis (FinCEN 2021). That same month, new international sanctions were imposed by the US Treasury on a number of Bitcoin, Zcash and other cryptocurrency addresses used by Pakistan-based SecondEye Solution to be paid around \$2.5million in some 27,000 digital currency transactions in order to create false identities for members of a Russian organization accused of US election interference and other cyberattacks (De 2021). The 2021 FinCen measures built on a growing litany of activities by other offices at the US Treasury (see Rella 2020). In particular, the Office of Foreign Assets Control (OFAC) in February 2021 fined Atlanta-based Bitpay more than half a million US dollars for facilitating over 2,100 transactions with individuals in sanctioned countries that included Cuba, North Korea, Iran, and Sudan (U.S. Department of Treasury 2021). OFAC had earlier, in 2018, sanctioned two Iranian individuals for their alleged involvement in the Bitcoin ransomware scheme SamSam. This was the first time that OFAC publicly attributed cryptocurrency addresses to designated individuals for what the U.S. Department of Treasury (2018) described as helping 'exchange digital currency ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims' (Young 2021b).

These measures were seen by many in the cryptocurrency and blockchain industries as a harbinger of further official actions. The OFAC's Office of Global Targeting in 2021 indicated that it would

Table 4. Selected blockchain intelligence services of large and longstanding firms.

Category	Companies	Products and Services
Accounting/Audit Firms	Deloitte	Eduscript
	EY	Blockchain Analyzer
	KPMG	Chain Fusion
	PricewaterhouseCoopers	Halo
Asset Managers	Fidelity	Sherlock
Financial Exchanges	NASDAQ	SMARTS
Information technology firms	IBM	Various products used by U.S. Department of Defense
	LexisNexis	World Compliance
	Thomson Reuters	BlockoneID

enhance its use of blockchain surveillance tools offered by Chainalysis (Singer 2021, Young 2021b). A few months later OFAC announced sanctions on cryptocurrency exchange Suex following investigations by Chainalysis (2021) that the firm's Moscow and St. Petersburg branches had facilitated the transfer of \$160 million in Bitcoin from ransomware payments and darknet markets. In October 2021, OFAC (2021) published guidance declaring that its sanctions 'apply equally to transactions involving virtual currencies and those involving traditional fiat currencies.'

These developments illustrate how relations of exclusion at the heart of existing finance/security infrastructure are extended via blockchains to counter the very attempts at harnessing this set of technologies to evade international sanctions. Growing blockchain-based efforts across the Global South are instigating the expansion of restrictions by leading actors in the Global North through blockchain applications. Both the US⁹ and the EU¹⁰ are contemplating the development of their own Central Bank-backed Digital Currencies (CBDCs) that are being tested by the central banks of central banks, the Bank for International Settlements (BIS) (Tassev 2021). Based, to varying extents, on permissioned blockchains, CBDCs seek, amongst other objectives, to extend real-time overview of transactions that can more clearly highlight transactions that may be in breach of international sanctions. Even the SWIFT, which has long been reliant on legacy technologies from the 1970s,¹¹ has experimented with permissioned blockchains (Zmudzinski 2019, De Meijer 2017) and in early 2021 initiated a joint venture with the PBOC (Pan 2021a). The double edged sword of technology entails opportunities for both escaping and enforcing sanctions, as the US and European countries turn to the very CBDCs being embraced in China, Russia, and Venezuela and sanctioned jurisdictions (Meredith 2021).

Official experimentation across the Global North with less inclusive 'permissioned' forms of blockchain technologies and emerging within a growing intelligence industry are extending 'global banking surveillance' as part of a widening formal, legal, and regulatory 'compliance infrastructure' (Mallard and Hanson 2021). Exclusionary practices have included targeted prohibitions of specific activities enabled by blockchain technology, such as bans of Iranian-based cryptocurrency exchange customers by countries like Finland. Further restrictive measures on uses of the technology were imposed by the Council of the European Union in 2020 on Chinese and Russian individuals allegedly involved in cyber-attacks that had demanded cryptocurrencies for ransoms. Restrictions were also undertaken in the US's 2018 Blocking Iran Illicit Finance Act, which expanded sanctions to any financial institution engaging in the sale, supply, holding, or transfer of the Iranian digital currency (Alexandre 2018). A March 2018 executive order also specifically banned U.S. citizens from buying the Petro, an order that led exchanges around the world, such as Hong-Kong based Bitfinex, to delist the Venezuelan cryptocurrency.¹² These sanctions enforcement actions emanate primarily, albeit not solely, from the hegemonic country currently most *capable* of extending exclusions to and through activities enabled by blockchain technologies. Yet, the US is not necessarily the only country *willing* to extend exclusions through blockchain. As noted, European countries are exploring both the inclusive and exclusive possibilities of CBDCs. Sanctioned countries themselves, moreover, are harnessing cryptocurrency and blockchains in ways that are enabling new exclusions while extending existing ones.

The sum of these emerging trends does not entirely curtail possibilities for actualizing decolonial ambitions through financial technologies. The decolonial possibilities offered by blockchain technologies in Africa and across the Global South instead need to be understood in parallel with extensions of exclusionary practices at the heart of the existing finance/security infrastructure. As we contemplate in the conclusion section, blockchains are double edged swords whose integration into existing socio-technical relations does not follow a predetermined path. It remains possible that African blockchain-based experiments enact more inclusive socio-technical relations that can provide more genuine alternatives to the exclusionary existing finance/security infrastructure. Yet, without understanding how current blockchain-based activities help to enforce sanctions and extend exclusions, it remains difficult to conceive of alternative finance/security infrastructures that are *more* open and *less* based on exclusions.

Conclusions

This article has sought to nuance growing hype around blockchain as a (de)colonial technology. We argued that blockchain-based fintech are facilitating, rather than displacing, exclusionary practices of sanctioning underpinning the existing finance/security infrastructure. Experimentation with blockchain technologies across the African continent risks being enrolled socio-technical relations that, as we have shown, are persistently exclusionary. Instead of displacing or ‘disrupting’ sanctions (Smith 2019), blockchains are enabling both new and old sanctioners with exclusionary possibilities. For blockchain, or any ‘fintech’ for that matter, to contribute genuine decolonial possibilities to an alternative finance/security infrastructure, sanctioning and other exclusionary practices of digital technology must be confronted.

We situated evolving applications of this set of fintechs within the wider, geographically dispersed attempts to both enforce and evade sanctions. The very socio-technical relations enabling sanctions evasions, we argued, extend exclusions *themselves* and instigate relations between a blockchain intelligence industry and governments enforcing the exclusions central to an existing finance/security infrastructure. Although they may incorporate different actors and technologies, the novelty of these socio-technical relations does not preclude the exclusions that the existing finance/security infrastructure enables. Like all technologies, blockchains need to be understood within human practices and their *relations* with technical objects as double-edged swords that cut multiple ways. In the case of sanctions, both the evasion and enforcement of this set of exclusionary practices are being enabled in socio-technical relations that are not creating a new or alternative finance/security infrastructure. As a set of technologies that was originally designed to challenge existing finance/security infrastructures, blockchain is paradoxically reinforcing existing relations. Yet, blockchain applications do not entirely foreclose possibilities for decolonial relations. There remain efforts in and between BRICS countries,¹³ as well as the Russian and Chinese governments via the Shanghai Cooperation Organization,¹⁴ that warn against suggestions that ‘there is no alternative’ (Dörry *et al* 2018) to an exclusionary neo-colonial existing finance/security infrastructure.

Future cultural economy research should strive to further situate decolonial ambitions in wider international efforts to alter, change, or undermine finance/security infrastructures. Interdisciplinary research can help investigate these possibilities in considering how *open source* technologies those who code is available to anyone with a computer and internet connection — is *equally* used by enforcers of existing socio-technical relations and by those seeking to enable ‘alternative’ finance/security infrastructure. How earlier technologies not only enabled the development of the existing finance/security infrastructures (de Goede 2020), but also undermined and limited previous attempts to create alternative sets of socio-technical relations, should be explored. Future studies could, for example, draw out possible historical comparisons with the current trajectories of technological change and exclusionary nature of finance/security infrastructures. Studies could also trace on-going technology-enabled attempts in and across African countries, from the Central African Republic to Zimbabwe, to evade and emerge from sanctions, as well as the roles of foreign actors in attempts like those of the Swiss-based Bitcoin Association to promote its Blockchain for Government in Sudan (Bitcoin Association 2021). Our hope is that this contribution provides an impetus for further scholarly exploration of the decolonial possibilities of blockchain and other fintechs situated with infrastructural relations within and between the Global North and Global South.

Notes

1. South Africa in 2021 announced the second phase of Project Khoka, which allows the country’s four biggest banks to trial the use of digital currency, blockchain and tokenised money supervised by the country’s Inter-departmental Fintech Working group (IFWG).
2. See most prominently, Watchdog Uganda (2021) and Quarmby (2021).
3. Keohane (1984) for instance defines hegemony as ‘the relationships between politically independent societies through a combination of hierarchies of control and the operation of markets’. Yet the realities of both *pax*

Britannica and *pax Americana* very much involved coercive forms of domination over less-than-consenting 'politically independent societies' around the world (*ibid*).

4. Sanctions imposed by the UN implicate Global South countries, yet are typically though not always led by 'Global North' countries.
5. For example, the U.S. Treasury Department imposed a \$327 million fine on UK bank Standard Chartered in 2012 after \$24m transactions processed on behalf of Iranian parties and a total of \$109m to Burma, Sudan and Libya between 2001 and 2007 (Mallard et al. 2020, p. 131)
6. When possible, we confirmed reporting by more pro-industry sources such as *Coindesk* and *Cointelegraph* through further reference both (1) the original documentation cited by these outlets and (2) reporting by established business press like the *Financial Times* and *The Economist* that have tended to be far more skeptical of cryptocurrencies.
7. <https://www.nigerianembassy.ru/index.php/ru/free-crypto-currency-economic-zone-in-nigeria.html>
8. Which issued and began immediately enforcing a version of the Travel Rule for US-based exchanges in 2019.
9. Through the Digital Dollar Project led by the consultancy Accenture, which has been involved with CBDC research in Canada, Singapore, France, and Sweden (Young 2021a).
10. Initiated in 2020, the European Central Bank (EC) in 2021 completed its public consultation a digital euro (Partz 2021b).
11. Technology that is 'slow, expensive, opaque, and carries risks for banks ... a payment can cost up to 60 EUR and can take between three and five working days, with transparency in pricing, timing and tracking significantly lacking. A lack of standardization means payments are error-prone, often requiring costly and time-consuming manual intervention, while anti-money laundering (AML) and know your customer (KYC) regulatory compliance is also costly' (Dorry et al 2018, p. 9).
12. As well as leading to a formal accusation of US discrimination by Venezuela at the World Trade Organization (Alexandre 2019)
13. A 2018 memorandum of understanding agreement was signed between the central banks of BRICS countries to collaborate on blockchain research, who in 2019 contemplated developing a digital currency to reduce reliance on settling international trade in US dollars (Finextra 2018, Palmer 2019)
14. Blockchain was listed as one of the areas of cooperation in the 2019 Shanghai Cooperation Concept in Digitalisation and Information and Communications Technologies (The Shanghai Cooperation Organisation 2020).
15. <https://www.globenewswire.com/news-release/2020/02/04/1979427/0/en/BIGG-Digital-Assets-Inc-subsiary-Blockchain-Intelligence-Group-Signs-CAD-715-000-Contract-with-United-States-Federal-Government-Agency.html>

Acknowledgements

Research assistance by Claudia Mellier and Ines Rojas Fernandez is gratefully acknowledged, along with the feedback provided by the special issue editors and participants in the January 2021 'FinTech in the Global South' workshop, the November 2020 24-hour Conference on Organized Crime, as well as the November 2020 Global Network of Financial Geography (FinGeo) 'Evolving Geographies of FinTech' workshop.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Malcolm Campbell-Verduyn is assistant professor in International Political Economy at the Department of International Relations and International Organization, University of Groningen, as well as Senior Research Fellow at the Käte Hamburger Kolleg Centre for Global Cooperation Research University of Duisburg-Essen, Germany. His research is generally concerned with the roles of emergent technologies, non-state actors and expert knowledge in contemporary global governance. He studies the on-going and varying implications of big data and blockchain technologies at the intersections of global environmental, financial and security governance. He is the editor of *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance* (Routledge, 2018) and author of *Professional Authority After the Global Financial Crisis: Defending Mammon in Anglo-America* (Palgrave MacMillan, 2017).

Francesco Giumelli is associate professor of International Relations at the Department of International Relations and International Organization, University of Groningen. His research areas are international sanctions, illicit trade and international security. He is the author of *Coercing, Constraining and Signalling: Explaining and Understanding UN and EU Sanctions* with ECPR Press and *The Success of Sanctions. Lessons Learned from the EU Experience* with Ashgate/Routledge.

ORCID

Francesco Giumelli  <http://orcid.org/0000-0002-5101-7254>

References

- Afro Foundation, 2021. *Afro Coin* [online]. Geneva, Afro Foundation. Available at: <https://afrofoundation.org/afro-coin/> [Accessed 10 July 2021].
- Alexandre, A., 2018. *US Lawmakers Introduce Bill to Impose Sanctions on Iranian National Cryptocurrency* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/us-lawmakers-introduce-bill-to-impose-sanctions-on-iranian-national-cryptocurrency> [Accessed 10 July 2021].
- Alexandre, A., 2019. *Venezuelan WTO Request Accuses US of 'Discriminatory Measures' Against Petro Coin* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/venezuelan-wto-request-accuses-us-of-discriminatory-measures-against-petro-coin> [Accessed 10 July 2021].
- AllAfrica InfoWire, 2021. *Is Cryptocurrency the Answer to Africa's Problems?* [online]. Washington, D.C., All Africa. Available at: <https://allafrica.com/stories/202104020557.html> [Accessed 10 July 2021].
- Allison, I., 2021. *Russia's Darknet Criminals Have Novel Crypto Cash-Out System: 'Buried Treasure'*. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/russias-darknet-criminals-have-a-novel-crypto-cash-out-system-buried-treasure> [Accessed 10 July 2021].
- Amicelle, A., 2011. Towards a 'new' political anatomy of financial surveillance. *Security Dialogue*, 42 (2), 161–178.
- Arzdigital, J., 2021. China creates its own digital currency, a first for major economy. *Wall Street Journal*, 5 April. Online reference available at: <https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118> [accessed 26 January 2022].
- Arzdigital, 2020. *The CEO of the Kish Free Zone Organization suggested: to provide the currency needed to import cars through digital currency* [online]. Tehran, Arzdigital. Available at: <https://arzdigital.com/iran-importing-cars-with-cryptocurrency/> [Accessed 10 July 2021].
- Avan-Nomayo, O., 2021. *Rolling up the sleeves: China's tech giants drive digital yuan adoption* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/rolling-up-the-sleeves-china-s-tech-giants-drive-digital-yuan-adoption> [Accessed 10 July 2021].
- Barone, R., and Masciandaro, D., 2019. Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics*, 47 (X), 233–254.
- Barret, T., Byrd, H., and Foran, C., 2020. *Senate approves final sanctions bill to punish China over Hong Kong* [online]. Atlanta, GA, CNN. Available at: <https://edition.cnn.com/2020/07/02/politics/china-sanctions-hong-kong/index.html> [Accessed 10 July 2021].
- Barrier, E., 2013. *Iranian shoemaker bypasses sanctions with Bitcoin* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/iranian-shoemaker-bypasses-sanctions-with-bitcoin> [Accessed 10 July 2021].
- Bartholomew, C., et al., 2019. "Report to Congress of the US-China Economic and Security Review Commission". *US Government Publishing Office*. Washington, DC. Available at: <https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf>.
- Baydakova, A., 2021a. *Inside Iran's Onslaught on Bitcoin Mining* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/inside-irans-onslaught-on-bitcoin-mining> [Accessed 10 July 2021].
- Baydakova, A., 2021b. *Bank of Russia Plans Prototype for Its Digital Ruble Design in December* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/bank-of-russia-prototype-digital-ruble-design> [Accessed 10 July 2021].
- Baydakova, A., 2021c. Thriving Under Pressure: Why Crypto Is Booming in Nigeria Despite the Banking Ban. *Coindesk*, 6 July. [Accessed 10 July 2021].
- Bernards, N., 2019. 'Fintech' and financial inclusion. In: T.M. Shaw, L.C. Mahrenbach, R. Modi, and X. Yi-Chong, eds. *The Palgrave Handbook of contemporary International Political economy*. London: Palgrave Macmillan, 317–329.
- Bernards, N., forthcoming. *A critical history of poverty finance: colonial roots and neoliberal failures*. London: Pluto.
- Bitcoin Association, 2021. *BSV's Blockchain for Government Initiative completes historic first official visit to the Republic of the Sudan* [online]. New York, NY, PR Newswire. Available at: <https://www.prnewswire.com/news-releases/bsvs-blockchain-for-government-initiative-completes-historic-first-official-visit-to-the-republic-of-the-sudan-301285597.html> [Accessed 10 July 2021].
- Blockchain Tech, 2018. Argentina, Venezuela, Egypt Register High Crypto Trading Volumes for October. *Market Exclusive*, 18 October. Available at: <https://marketexclusive.com/argentina-venezuela-egypt-high-crypto-trading-volumes-october/2018/10/>.
- Buck, J., 2017. *Facing Hyperinflation, Venezuela to Issue Oil-Backed Cryptocurrency* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/facing-hyperinflation-venezuela-to-issue-oil-backed-cryptocurrency> [Accessed 10 July 2021].

- Bull, B., and Rosales, A., 2020. Into the shadows: sanctions, rentierism, and economic informalization in Venezuela. *European Review of Latin American and Caribbean Studies*, 109, 107–133.
- Campbell-Verduyn, M., 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, 69 (2), 283–305.
- Campbell-Verduyn, M., Rodima-Taylor, D., and Hütten, M., 2021. Technology, small states and the legitimacy of digital development: combatting de-risking through blockchain-based Re-Risking?. *Journal of International Relations & Development*, 24 (2), 455–482.
- Capozzalo, O., 2018. *Putin Adviser Says 'CryptoRuble' Will Circumvent Sanctions, Government Remains Divided* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/putin-adviser-says-cryptoruble-will-circumvent-sanctions-government-remains-divided> [Accessed 10 July 2021].
- Chainalysis, 2020. *The 2020 Geography of Cryptocurrency Report*. New York, NY, Chainalysis. Available at: <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Geography-of-Crypto.pdf> [Accessed Day Month Year].
- Chainalysis, 2021. Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over \$160 million from Ransomware Attackers, Scammers, and Darknet Markets. Available at: <https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021> [accessed 11 November].
- Cointelegraph, 2021a. *China News* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/tags/china> [Accessed Day Month Year].
- Cointelegraph, 2021b. *Russia News* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/tags/russia> [Accessed Day Month Year].
- Crandall, J., 2019. Blockchains and the “chains of empire”: contextualizing blockchain, cryptocurrency, and neoliberalism in Puerto Rico. *Design and Culture*, 11 (3), 279–300.
- Crawley, J., 2021. *Central Banks of China, UAE Join Blockchain-Based CBDC Payments Project* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/central-banks-of-china-uae-join-hong-kong-thailand-cbdc-payments-project> [Accessed 10 July 2021].
- Dallyn, S., 2017. Cryptocurrencies as market singularities: the strange case of bitcoin. *Journal of Cultural Economy*, 10 (5), 462–473.
- Dana, J., 2020. *West Africa has ditched its colonial currency. Now the future is crypto* [online]. Riyadh, Arab News. Available at: <https://www.arabnews.com/node/1607116> [Accessed 10 July 2021].
- Day, Amy. 2020. Are Rogue Countries Turning to Crypto for Sanctions Relief?. *Finance Magnates*, 2 June. Available at: <https://www.financemagnates.com/cryptocurrency/are-rogue-countries-turning-to-crypto-for-sanctions-relief/> [Accessed 3 April 2022].
- De Goede, M., 2012. *Speculative security: The politics of pursuing terrorist monies*. Minneapolis: University of Minnesota Press.
- De Goede, M., 2020. Finance/security infrastructures. *Review of International Political Economy*, 28 (2), 351–368.
- De Meijer, C. R. W., 2017. *SWIFT Blockchain POC: enhanced cross-border payments* [online]. Finextra.com. Available at: <https://www.finextra.com/blogposting/14321/swift-blockchain-poc-enhanced-cross-border-payments> [Accessed 10 July 2021].
- De, N., 2021. *US Government Sanctions Crypto Addresses Linked to Russian Election Fraud Scheme* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/us-government-sanctions-crypto-addresses-linked-to-russian-election-fraud-scheme>.
- Del Castillo, M., 2019. Crypto's Valachi Papers. *Forbes*, 4 December. Available at: <https://www.forbes.com/sites/michaeldelcastillo/2019/12/04/cryptos-valachi-papers/?sh=2e208d433117>.
- Dörry, S., Robinson, G., and Derudder, B., 2018. There is no alternative: SWIFT as infrastructure intermediary in global financial markets. Oxford, Global Network on Financial Geography (FinGeo), Financial Geography Working Paper Series – ISSN 2515-0111. Available at: http://www.fingeo.net/wordpress/wp-content/uploads/2019/02/FinGeoWP22_Doerry_Robinson_Derudder_SwiftGPN.pdf [Accessed 10 July 2021].
- The Economist, 2021. Cuba's communist regime is trying to control crypto. Available at: <https://www.economist.com/the-americas/2021/10/30/cubas-communist-regime-is-trying-to-control-crypto> [accessed 11 November 2021].
- Emirbayer, M., 1997. Manifesto for a relational sociology. *American Journal of Sociology*, 103 (2), 281–317.
- EY Global, 2019. *How data analytics is leading the fight against financial crime* [online]. London, EY. Available at: https://www.ey.com/en_gl/assurance/to-fight-fraud-should-you-trust-human-instinct-or-machine-logic-more [Accessed 10 July 2021].
- Fanusie, Y., 2018. Seeking Sanctions Resistance Through Blockchain Technology. *Forbes*, 11 October. Available at: <https://www.forbes.com/sites/yayafanusie/2018/10/11/seeking-sanctions-resistance-through-blockchain-technology/?sh=770ffc5a6392>.
- Fanusie, Y. J., and Zilberman, B., 2017. *Blockchain technology may give Russia its next Sputnik moment* [online]. Washington, D.C., The Hill. Available at: <https://thehill.com/blogs/pundits-blog/technology/346476-blockchain-technology-may-give-russia-its-next-sputnik-moment> [Accessed 10 July 2021].

- Fanusie, Y., and Logan, T., 2019. *Crypto Rogues. U.S. State Adversaries Seeking Blockchain Sanctions Resistance* [online]. Washington, D.C., Foundation for Defense of Democracies. Available at: <https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf> [Accessed 10 July 2021].
- Faria, I., 2019. Trust, reputation and ambiguous freedoms: financial institutions and subversive libertarians navigating blockchain, markets, and regulation. *Journal of Cultural Economy*, 12 (2), 119–132.
- Faria, I., 2021. The market, the regulator, and the government: making a blockchain ecosystem in the Netherlands. *Finance and Society*, 7 (1), 40–56.
- Faustino, S., 2019. How metaphors matter: an ethnography of blockchain-based re-descriptions of the world. *Journal of Cultural Economy*, 12 (6), 478–490.
- Feldman, M.S., 2000. Organizational routines as a source of continuous change. *Organization Science*, 11 (6), 611–629.
- Financial Tribune, 2019. *Iran Unveils Gold-Backed Cryptocurrency* [online]. Tehran, Financial Tribune. Available at: <https://financialtribune.com/articles/business-and-markets/96476/iran-unveils-gold-backed-cryptocurrency> [Accessed 10 July 2021].
- Financial Tribune, 2021. *Banks and Forex Shops Can Use Digital Assets to Pay for Imports* [online]. Tehran, Financial Tribune. Available at: <https://financialtribune.com/articles/business-and-markets/108313/banks-and-forex-shops-can-use-digital-assets-to-pay-for-imports> [Accessed 10 July 2021].
- FinCEN, 2021. *FinCEN Announces Acting Director and New Deputy Director* [online]. Vienna, VA, FinCEN. Available at: <https://www.fincen.gov/news/news-releases/fincen-announces-acting-director-and-new-deputy-director> [Accessed 10 July 2021].
- Finextra, 2018. *Brics bank consortium to collaborate on blockchain* [online]. London, Finextra. Available at: <https://www.finextra.com/pressarticle/74892/brics-bank-consortium-to-collaborate-on-blockchain> [Accessed 10 July 2021].
- Gilbert, E., 2017. Militaries, finance, and (in) security. *Finance and Society*, 3 (2), 180–87.
- Giumelli, F., 2011. *Coercing, constraining and signaling. explaining and understanding UN and EU sanctions*. Colchester, UK: ECPR Press.
- Giumelli, F., 2015. Understanding targeted sanctions of the United Nations: an empirical analysis. *International Affairs*, 91 (6), 1351–1368.
- Gkritsi, E., 2021. China's BSN to Launch Portals in Turkey, Uzbekistan. *Coindesk*, 12 October. Available at: <https://www.coindesk.com/business/2021/10/12/chinas-bsn-to-launch-portals-in-turkey-uzbekistan/> [Accessed 11 November 2021].
- Gravett, W., 2020. Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20 (1), 125–146.
- Green, J., and Gruin, J., 2021. RMB transnationalization and the infrastructural power of international financial centres. *Review of International Political Economy*, 28 (4), 1028–1054.
- Grossman, J.H., 2019. Passing cash from bank notes to bitcoin: standardizing money. *Journal of Cultural Economy*, 12 (4), 299–316.
- Gruin, J., 2021. The epistemic evolution of market authority: Big data, blockchain and China's neostatist challenge to neoliberalism. *Competition & Change* 25 (5), 580–604.
- Handagama, S., 2021a. *Crypto is Banned in Morocco, but Bitcoin Purchases Are Soaring* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/crypto-is-banned-in-morocco-but-bitcoin-purchases-are-soaring> [Accessed 10 July 2021].
- Handagama, S., 2021b. *Africa 'Is Leading Global Cryptocurrency Adoption': Paxful CEO* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/africa-is-leading-global-cryptocurrency-adoption-paxful-ceo> [Accessed 10 July 2021].
- Heasman, W., 2019. *Cuba becomes the latest country to use bitcoin to subvert US sanctions* [online]. New York, NY, Yahoo!finance. Available at: https://finance.yahoo.com/news/cuba-becomes-latest-country-bitcoin-164410414.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQA-AAFaYS1pi7w5ifh_RZNwUwv4-Bt3XtOadk5xn6E5pzknQKTMHAfoR7Dnat7dIUWDhgR6J6VknNqkK9m_O4ui2oNm6p7Dht60tYpYEmHuemvngISHrbghjuMS6zV0LJTWQVnmuHr871NaSu0iVTRo1oh-zac6WnAe-YI5ZLVJ6uam3Z [Accessed 10 July 2021].
- Hertig, A., 2020. *Nigerians Are Using Bitcoin to Bypass Trade Hurdles With China* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/nigeria-using-bitcoin-trade-with-china> [Accessed 10 July 2021].
- Herzfeld, M., 2002. The absent presence: discourses of crypto-colonialism. *South Atlantic Quarterly*, 101, 899–926.
- Howson, P., 2020. Climate crises and crypto-colonialism: conjuring value on the blockchain frontiers of the Global south. *Frontiers in Blockchain*, 3, Article 32.
- Iyatse, G., 2021. *Of e-naira and emerging digital currency imperialism* [online]. Lagos, Nigeria, The Guardian. Available at: <https://guardian.ng/business-services/of-e-naira-and-emerging-digital-currency-imperialism/> [Accessed 26 January 2022].
- Hufbauer, G. C., and Jung, E., 2020. What's new in economic sanctions? *European Economic Review*, 130, 1–12.

- Jia, K., and Zhang, F., 2018. Between liberalization and prohibition: prudent enthusiasm and the Governance of bitcoin/blockchain technology. In: M Campbell-Verduyn, ed. *Bitcoin and Beyond: cryptocurrencies, Blockchains and Global Governance*. London: Taylor & Francis, 88–108.
- Jutel, O., 2021. Blockchain imperialism in the pacific. *Big Data & Society*, 8 (1), 1–14.
- Kessler, O., 2011. Beyond sectors, before the world: finance, security and risk. *Security Dialogue*, 42 (2), 197–215.
- Kimani, M., 2021. *China Leads Africa's Digital Currency Race* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/china-leads-africas-digital-currency-race> [Accessed 10 July 2021].
- Kobo, K., 2021. Akon wants to run a Senegal city on cryptocurrency—could it work? *Quartz Africa*, 10 April. Available at: <https://qz.com/africa/1994122/akon-plans-to-run-a-senegal-city-on-akon-cryptocurrency/> [Accessed 11 November 2021].
- Levine, A. B., 2020. In Zimbabwe, Crypto Is a 'Liberation Tool': Bitcoin in Africa, Part 1 of a New Documentary Podcast Series [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/bitcoin-in-zimbabwe-part-1-of-a-new-documentary-podcast-series> [Accessed 10 July 2021].
- Lobo-Guerrero, L., 2016. *Insuring life: value, security and risk*. New York: Routledge.
- Mallard, G., 2019. Governing proliferation finance: multilateralism, transgovernmentalism, and hegemony in the case of sanctions against Iran. In: E. Brousseau, J. M. Glachant, and J. Sgard, eds. *Institutions of international economic governance and market regulation*, 1–21. Oxford: Oxford University Press.
- Mallard, G., and Hanson, A., 2021. Embedded extraterritoriality: US judicial litigation and the global banking surveillance of digital money flows. In: C. Beaucillon, ed. *Research Handbook on unilateral and extraterritorial sanctions*, 270–287. Edward Elgar Publishing.
- Mallard, G., Sabet, F., and Sun, J., 2020. The humanitarian Gap in the Global sanctions regime assessing causes, effects, and solutions. *Global Governance*, 26 (1), 121–153.
- Matera, P., 2020. Under hegemonic pressure: 2018 American sanctions against Iran and Turkey's response. *Digest of Middle East Studies*, 29 (2), 183–199.
- McDowell, D., 2020. Financial sanctions and political risk in the international currency system. *Review of International Political Economy*, 28 (3), 635–661.
- Meredith, S., 2021. U.S. sanctions will still have an impact despite the rise of crypto, Treasury's Adeyemo says. *CNBC*, 17 November. Available at: <https://www.cnn.com/2021/11/17/crypto-treasurys-adeyemo-says-dollar-to-remain-the-dominant-currency.html> [accessed 17 November].
- Michael, 2021. *The rising popularity of Bitcoin in Africa* [online]. Nashville, TN, Bitcoin Magazine. Available at: <https://bitcoinformagazine.com/culture/the-rising-popularity-of-bitcoin-in-south-africa> [Accessed 10 July 2021].
- Milano, A., 2018. *Russia's Central Bank Mulls Ethereum System for Pan-Eurasian Payments* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/russias-central-bank-mulls-ethereum-system-for-pan-eurasian-payments> [Accessed 10 July 2021].
- Mizrahi, A., 2017. *New Swedish Firm Offers Iranian Stock Investment for Bitcoin* [online]. Ramat Gan, Finance Magnates. Available at: <https://www.financemagnates.com/cryptocurrency/news/new-swedish-firm-offers-iranian-stock-investment-bitcoin/> [Accessed 10 July 2021].
- Murray, R., 2021. *How China Seized the Initiative on Blockchain and Digital Currency* [online]. Philadelphia, PA, Foreign Policy Research Institute. Available at: <https://www.fpri.org/article/2021/05/how-china-seized-the-initiative-on-blockchain-and-digital-currency/> [Accessed 10 July 2021].
- Nakamoto, S., 2008. *Bitcoin: a peer-to-peer electronic cash system* [online]. Bitcoin Project. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 10 July 2021].
- Naumoff, A., 2016. *Blockchain Revolution in Russia: Bank of Russia Tests Masterchain* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/blockchain-revolution-in-russia-bank-of-russia-tests-masterchain> [Accessed 10 July 2021].
- Nelms, T.C., 2016. Alt. economy: strategies, tensions, challenges. *Journal of Cultural Economy*, 9 (5), 507–512.
- Nelson, D., 2021. *Russia Floats Blockchain Based System as SWIFT Alternative* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/video/russia-floats-blockchain-based-system-as-swift-alternative> [Accessed 10 July 2021].
- New Money Review Staff, 2020. *Bitcoin mixers stump Europol*. London, New Money Review. Available at: <https://newmoneyreview.com/index.php/2020/06/05/law-enforcement-struggles-with-bitcoin-mixers/> [Accessed 10 July 2021].
- O'Dwyer, R., 2019. Cache society: transactional records, electronic money, and cultural resistance. *Journal of Cultural Economy*, 12 (2), 133–153.
- Office of Foreign Asset Control, 2021. Sanctions Compliance Guidance for the Virtual Currency Industry.
- Organization for Economic Co-Operation and Development, 2008. "Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security". Available at: <https://www.oecd.org/daf/inv/investment-policy/40700392.pdf>.
- Ozelli, S., 2018. *Pax Crypto: Russia Proposes First Multinational Cryptocurrency, Expert Blog* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/pax-crypto-russia-proposes-first-multinational-cryptocurrency-expert-blog> [Accessed 10 July 2021].

- Palmer, D., 2019. *BRICS Nations Ponder Digital Currency to Ease Trade, Reduce USD Reliance* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/brics-nations-ponder-digital-currency-to-ease-trade-reduce-usd-reliance> [Accessed 10 July 2021].
- Pan, D., 2021a. *China's Central Bank Is Partnering With SWIFT on a New Joint Venture* [online]. New York, NY, Cointelegraph. Available at: <https://www.coindesk.com/chinas-central-bank-is-partnering-with-swift-on-a-new-joint-venture> [Accessed 10 July 2021].
- Pan, D., 2021b. *Card-Based Digital Yuan Wallet Manufacturer to Use Fingerprint ID Tech* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/card-based-digital-yuan-wallet-manufacturer-to-use-fingerprint-id-tech> [Accessed 10 July 2021].
- Partz, H., 2021a. *Digital ruble is 'highest form of money', Russian Bitcoin critic says* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/digital-ruble-is-highest-form-of-money-russian-bitcoin-critic-says> [Accessed 10 July 2021].
- Partz, H., 2021b. *European Central Bank releases results of digital euro consultation* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/european-central-bank-releases-results-of-digital-euro-consultation> [Accessed 10 July 2021].
- Phillips, J., 2018. Bridging the divide in Burkina Faso: How tech is changing lives. *Intelligent CIO*, 30 July. Available at: <https://www.intelligentcio.com/africa/2018/07/30/bridging-the-divide-in-burkina-faso-how-tech-is-changing-lives/#> [Accessed 10 July 2021].
- Phillips, T., 2021. *China unveils plan to build a global payment network based on central bank digital currencies* [online]. Vienna, VA, NFCW. Available at: <https://www.nfcw.com/2021/01/20/370197/china-unveils-plan-to-build-a-global-payment-network-based-on-central-bank-digital-currencies/> [Accessed 10 July 2021].
- Pinzur, D., 2021. Infrastructural power: discretion and the dynamics of infrastructure in action. *Journal of Cultural Economy*, 14 (6), 644–661.
- Plantin, J.C., et al., 2018. Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20 (1), 293–310.
- Quarmby, B., 2021. *Jack Dorsey notes lobbying efforts to get Ethiopian gov't to embrace Bitcoin*. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/jack-dorsey-notes-lobbying-efforts-to-get-ethiopian-gov-t-to-embrace-bitcoin> [Accessed 10 July 2021].
- Rao, P., 2018. *Africa could be the next frontier for cryptocurrency*. New York, NY, United Nations Africa Renewal. Available at: <https://www.un.org/africarenewal/magazine/april-2018-july-2018/africa-could-be-next-frontier-cryptocurrency> [Accessed 10 July 2021].
- Rella, L., 2020. Steps towards an ecology of money infrastructures: materiality and cultures of Ripple. *Journal of Cultural Economy*, 13 (2), 236–249.
- Reuters, 2021. \$9.5 billion spent using Chinese central bank's digital currency – official. 3 November.
- Robinson, T., 2021. *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil* [online]. London, Elliptic. Available at: <https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions> [Accessed 10 July 2021].
- Rodman, K.A., 1995. Sanctions at bay? Hegemonic decline, multinational corporations, and US economic sanctions since the pipeline case. *International Organization*, 49 (1), 105–137.
- Scott, B., 2016. How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? (No. 2016-1). UNRISD Working Paper.
- The Shanghai Cooperation Organisation, 2020. *SCO Secretary-General meets with Alibaba vice president* [online]. Beijing, The Shanghai Cooperation Organisation. Available at: http://eng.sectsc.org/for_media/20200523/649463.html [Accessed 10 July 2021].
- Sinclair, S., 2021. *Iran Central Bank to Allow Money Changers, Banks to Pay for Imports Using Mined Crypto* [online]. New York, NY, Coin Desk. Available at: <https://www.coindesk.com/iran-central-bank-money-changers-imports-mined-crypto> [Accessed 10 July 2021].
- Singer, A., 2021. *Rogue states dodge economic sanctions, but is crypto in the wrong?* [online]. New York, NY, Magazine by Cointelegraph. Available at: <https://cointelegraph.com/magazine/2021/06/08/rogue-states-dodge-economic-sanctions-but-is-crypto-in-the-wrong> [Accessed 10 July 2021].
- Smith, N.R., 2019. International order in the coming cryptocurrency age: the potential to disrupt American primacy and privilege? *Rising Powers Quarterly*, 3 (1), 77–97.
- Star, S.L., 1999. The ethnography of infrastructure. *American Behavioral Scientist*, 43 (3), 377–391.
- Suberg, W., 2019. *Venezuelan Gov't Reportedly Dodges US Sanctions With Crypto in Airports* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/venezuelan-govt-reportedly-dodges-us-sanctions-with-crypto-in-airports> [Accessed 10 July 2021].
- Sullivan, G., 2020. *The Law of the list: UN counterterrorism sanctions and the politics of global security law*. Cambridge: Cambridge University Press.
- Tassev, L., 2021. *Swiss, French Central Banks to Trial Wholesale CBDC Settlements With BIS and Private Sector* [online]. Saint Kitts, Bitcoin News. Available at: <https://news.bitcoin.com/swiss-french-central-banks-to-trial-wholesale-cbdc-settlements-with-bis-and-private-sector/> [Accessed 10 July 2021].

- Teichmann, F.M.J., and Falkner, M., 2021. Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Control*, 24 (4), 775–788.
- Tetkin, M., 2018. *Iran, Russia May Start Using Cryptocurrencies To Bypass Sanctions* [online]. Moscow, RBC. Available at: <https://www.rbc.ru/crypto/news/5afd4fb69a794757df44fa3a> [Accessed 10 July 2021].
- Thomson, G., 2021. *Iran intelligence officers target illegal cryptocurrency miners* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/iranian-intelligence-officers-target-illegal-cryptocurrency-miners> [Accessed 10 July 2021].
- Tran, H., 2020. *Can China's digital yuan really challenge the dollar?* [online]. Washington, D.C., Atlantic Council. Available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/can-chinas-digital-yuan-really-challenge-the-dollar/> [Accessed 10 July 2021].
- U.S. Department of Treasury, 2018. Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses [online]. Washington, U.S. Department of Treasury. Available at: <https://home.treasury.gov/news/press-releases/sm556> [Accessed 10 July 2021].
- U.S. Department of Treasury, 2021. OFAC Enters Into \$507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions. Washington, D.C.: Enforcement Release. Available at: https://home.treasury.gov/system/files/126/20210218_bp.pdf [Accessed 10 July 2021].
- Watchdog Uganda, 2021. *Chinese crypto-currency money billionaire meets Museveni in Entebbe* [online]. Kampala, Watchdog News. Available at: <https://www.watchdoguganda.com/news/20180425/38552/chinese-crypto-currency-money-billionaire-meets-museveni-in-entebbe.html> [Accessed 10 July 2021].
- Wheatley, J., and Klasa, A., 2021. Cryptocurrencies: developing countries provide fertile ground. *Financial Times*, [accessed 6 September 2021].
- Wright, T., 2020a. *Iranian General Calls for use of Crypto to Evade Sanctions* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/iranian-general-calls-for-use-of-crypto-to-evade-sanctions> [Accessed 10 July 2021].
- Wright, T., 2020b. *'Secret' bridge turns ERC-20 tokens into privacy coins* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/secret-bridge-turns-erc-20-tokens-into-privacy-coins> [Accessed 10 July 2021].
- Wright, T., 2021. Jelurida will launch 30-day blockchain education campaign across East Africa. *Cointelegraph*. Available at: <https://cointelegraph.com/news/jelurida-will-launch-30-day-blockchain-education-campaign-across-east-africa> [accessed 11 November 2021].
- Young, M., 2021a. *Accenture and Digital Dollar Foundation to trial United States CBDC this year* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/accenture-and-digital-dollar-foundation-to-trial-united-states-cbdc-this-year> [Accessed 10 July 2021].
- Young, M., 2021b. *US sanctions agency OFAC to rely more heavily on Chainalysis* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/us-sanctions-agency-ofac-to-rely-more-heavily-on-chainalysis> [Accessed 10 July 2021].
- Zagaris, B., and Bannister, M., 2020. Money laundering, terrorism financing and asset forfeiture. *International Enforcement Law Reporter*, 36, 338–342.
- Zmudzinski, A., 2019. *SWIFT, HSBC, Deutsche Bank to Conduct Blockchain-Based E-Voting PoC* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/swift-hsbc-deutsche-bank-to-conduct-blockchain-based-e-voting-poc> [Accessed 10 July 2021].
- Zuckerman, M.J., 2018. *Venezuela's Cryptocurrency Petro Finds Foreign Investors, ICO To Take Place in March* [online]. New York, NY, Cointelegraph. Available at: <https://cointelegraph.com/news/venezuelas-cryptocurrency-petro-finds-foreign-investors-ico-to-take-place-in-march> [Accessed 10 July 2021].