Review of International Studies (2023), **49:** 4, 615–636
doi:10.1017/S0260210522000493

RIS

RESEARCH ARTICLE

From flows towards updates: Security regimes and changing technologies for financial surveillance

Carola Westermeier*

Goethe University Frankufurt and Justus Liebig University Giessen, Germany
*Corresponding author. Email: westermeier@soz.uni-frankurt.de

(Received 2 September 2021; revised 31 August 2022; accepted 23 September 2022)

Abstract

'Follow the money' is currently the central principle of international financial security, although money itself is probably one of the most unlikely objects to make traceable. Two recent scandals around a security unit and the payment processor Wirecard show how existing systems of financial surveillance that seek to capture 'flows' of money for security purposes are either enabled or frustrated. While this current regime of financial surveillance adheres to demanding the free flow of money through financial infrastructures and various actors and intermediaries, new digital currencies build on a set type of ledger(s) in which money is stored as data. Hence, what we understand as money does not 'flow', but is rather updated. This change in the underlying infrastructure means that traceability does not need to be enacted; it is an intrinsic feature of digital currencies. With new central bank digital currencies (CBDC), the regime of financial security thus changes from the monitoring of financial flows and flagging of (potentially) illicit transactions towards the storage of financial data in (de)centralised ledgers. This form of transactional governance is engendered by shifting geopolitical agendas that increasingly rely on fractured instead of globalised financial infrastructures, thus making CBDCs themselves subject to security efforts.

Keywords: Security; Central Bank Digital Currencies; Geopolitics; Technology; Infrastructure; Cryptocurrencies

Introduction

Markus Braun from Hanau, Germany, is a passionate diver. When he booked his last diving trip to Indonesia he used his credit card, issued by his local bank, to pay for parts of the trip. Months later, he learned through the media that the transaction that he initiated with this credit card had a longer journey than he had anticipated. It was reported as a 'suspicious transaction' by a British bank to the German financial authorities, the financial intelligence unit (FIU), and landed in the files of the biggest financial scandal in German postwar history, the bankruptcy of Wirecard. Why did Markus Braun's payment for his diving trip end up in the prosecutor's hands? Because he shares his name – yet nothing more – with the former CEO of Wirecard, a German payment processor and financial services provider who abruptly filed for bankruptcy in 2020.[1] Wirecard's collapse led to a public scandal, and its leading figures are under investigation for fraud involving billions of euros. The diver Markus Braun's story offers a glimpse into global financial traceability systems that flag a fraction of the world's 1.5 billion daily transactions as suspicious – while the majority of those transactions run smoothly through the various channels of the global financial system.

[1]Josef Streule and Arne Meyer-Fünffinger, 'Herr Braun aus Hanau in den Wirren des Wirecard-Skandals', *Bayerischer Rundfunk*, available at: {https://www.br.de/nachrichten/amp/deutschland-welt/herr-braun-aus-hanau-in-den-wirren-des-wirecard-skandals,SSfYMOy} accessed 1 August 2021. All translations from German are my own.

This article shows how the current system of financial surveillance that seeks to capture 'flows' of money for security purposes is either enabled or frustrated. It foregrounds an infrastructural perspective on the established and emerging regime of financial security and puts the concept of traceability at its core in order to describe different modes of traceability and how they shape financial security practice. It argues that new digital currencies have the potential to shift the regime of financial surveillance from the monitoring of financial flows and flagging of (potentially) illicit transactions towards the storage of financial data in (de)centralised ledgers that update rather than capture financial flows.

As it did in the case of Markus Braun, the established regime detects suspicious transactions by relying on categorisations, such as names, and risk assessments, based, for example, on countries or nationalities. These practices are adjusted to the desired free movement of capital in which money 'flows like mercury' and is sent from one bank account or custodian to another, crossing countries, financial actors and intermediaries and infrastructures.[2] This seemingly frictionless, multichannel regime makes it hard to detect and capture illicit flows. The following provides insights into how traceability of money is enabled by a complex regime of financial surveillance that involves public and private actors and relies on the use of technology and specific risk assessments. While the two cases are based in Germany, they have much wider implications given that traceability has been promoted globally for decades across public and private spheres as the key to ensuring money's free circulation and thus capitalist expansion. While international cooperation and standardisation are central aims of authorities and supranational organisations, the enforcement of financial security lies with the national state. The interrogation into financial security thus happens at the national level, which makes this level the point of access for an analysis of traceability.

'Follow the money' is both the central dogma and the key challenge of current financial surveillance in the fight against financial crime. Traceability is a norm desired not only for security and possible criminal prosecution, but also for all kinds of businesses that want to ensure safe payments and money transmission. Traceability can also serve emancipatory purposes and to reveal where payments originate and where they end, thus allowing people to discern (hidden) power structures and to change or dismantle them.[3] This article concentrates on financial surveillance for security purposes, such as preventing money laundering and terrorism financing. These measures also include targeted sanctions, for example, those applied in reaction to Russia's war against Ukraine, which also rely on techniques of traceability and categorisation of transactions.[4] Will 'follow the money' hold up as the central principle of financial governance amid technological and geopolitical shifts?

While the current regime of financial surveillance seeks to maintain the free flow of money through financial infrastructures and various actors and intermediaries, digital currencies store money as data on a set type of ledger(s), namely a blockchain or other permissioned ledgers. Hence, what we understand as money does not 'flow' from one place to another, but is rather updated where it is stored. Digital currencies entail underlying data infrastructures that have traceability as an intrinsic feature. As several states look for different modes of securing financial transactions, the emergence of central bank digital currencies (CBDC) entail the possibility of a more fractured financial system and altered forms of transaction monitoring amid growing geopolitical tensions.[5] In order to sustain these claims, this article uses an infrastructural perspective to describe the implications of traceability within the current model and the shifts that digital currencies entail, thus bringing international politics to the fore.

[2]Gordon L. Clark, 'Money flows like mercury: The geography of global finance', *Geografiska Annaler: Series B, Human Geography*, 87:2 (2005), pp. 99–112.

[3]Sara E. Davies and Jacqui True, 'Follow the money: Assessing Women, Peace, and Security through financing for gender-inclusive peace', *Review of International Studies* (2022), pp. 1–21.

[4]Marieke de Goede, 'Blacklisting and the ban: Contesting targeted sanctions in Europe', *Security Dialogue*, 42:6 (2011), pp. 499–515.

[5]Marieke de Goede and Carola Westermeier, 'Infrastructural geopolitics', *International Studies Quarterly*, 66:3 (2022).

This contribution builds on research on the finance/security nexus that emphasises the use of money as a tool for security and the regimes of traceability that underlie the security management of financial flows.[6] It connects that research to more recent contributions that highlight the importance of political economy infrastructures with regard to geopolitical tensions.[7] It advances both strands of the literature and argues that a new regime of financial surveillance looms with the introduction of new financial technologies that could lead to the fragmentation of the international financial order. Two decades after the war on terror intensified the use of financial systems for security purposes, we observe a shift from the question of how security is practised based on risk assessments and categorisations to how financial infrastructures have themselves become (national) security projects amid growing geopolitical tensions

The following analysis uses the notion of 'traceability infrastructures' to capture the changes in the financial security regime.[8] Throughout, the three faces or ontologies of traceability, as defined by Michael Power, are highlighted: (1) ideational, i.e., traceability as an ideal shared across public and private sectors; (2) material, i.e., traceability as financial infrastructure; and (3) processual, i.e., traceability as organisational connectedness.[9]

The article discusses the three faces of traceability using two scandals that arose when the traceability of money was disabled. Scandals are highly valuable for the analysis of normative (re)definition and correction within democracies, and the two incidents at play show how the traceability of money as a normative consensus is restated and enforced politically.[10] Both incidents arose when this consensus was challenged and traceability was restricted. The first scandal emerged in the wake of the German FIU's inability to enact systems of traceability and the resulting lack of action against financial fraud. The second incident, known as the 'Wirecard scandal', was a case of fraud involving billions of euros that was hidden in plain sight for years due to a series of regulatory failures and accounting tricks. Wirecard, a payment processor and financial services provider, was listed in the DAX stock index, consisting of thirty major German companies including Adidas, Siemens, and Volkswagen. From that position it abruptly went into insolvency in June 2020.

The article uses these two scandals to describe moments in which the consensus surrounding traceability for financial surveillance becomes apparent and is also politically enforced. Thomas Crosbie and Jensen Sass describe how scandals enforce a form of consensus, as 'parties who ordinarily oppose one another agree about the basic facts concerning a normative violation. More specifically, they agree about the status of the values at stake, and about certain facts surrounding their breach.'[11] The Wirecard scandal thus led to a public inquiry into the case and received international attention in the media and documentaries.[12] While at the time of writing the prosecution of the Wirecard case is still ongoing, it has already led to two kinds of revelations: first, the criminal acts that took place within the company; and second, the failure of traceability

[6]See *Finance and Security*, Special Issue, 3:2 (2017); Nina Boy, John Morris, and Mariana Santos, 'Introduction: Taking stock of security and finance', *Finance and Society*, 3:2 (2017), pp. 102–05; Marieke de Goede, 'Financial security', in J. P. Burgess (eds), *The Routledge Handbook of New Security Studies* (London, UK [etc.]: Routledge, 2010), pp. 100–09.

[7]Nick Bernards and Malcolm Campbell-Verduyn, 'Understanding technological change in global finance through infrastructures', *Review of International Political Economy*, 25:3 (2019), pp. 1–17; Malcolm Campbell-Verduyn and Francesco Giumelli, 'Enrolling into exclusion: African blockchain and decolonial ambitions in an evolving finance/security infrastructure', *Journal of Cultural Economy*, 15:4 (2022), pp. 524–43.

[8]Michael Power, 'Infrastructures of traceability', in Martin Kornberger, Geoffrey C. Bowker, Julia Elyachar, Andrea Mennicken, Peter Miller, Joanne R. Nucho, and Neil Pollock (eds), *Research in the Sociology of Organizations*, *Thinking Infrastructures* (Bingley, UK: Emerald Publishing Limited, 2019), pp. 115–30.

[9]Ibid.; see also N. B. Thylstrup, Matthew Archer, and Louis Ravn, 'Traceability', *Internet Policy Review*, 11:1 (2022).

[10]Thomas Crosbie and Jensen Sass, 'Governance by scandal? Eradicating sexual assault in the US military', *Politics*, 37:2 (2017), pp. 117–33; Peer Schouten, 'Security as controversy: Reassembling security at Amsterdam Airport', *Security Dialogue*, 45:1 (2014), pp. 23–42.

[11]Crosbie and Sass, 'Governance by scandal?', p. 118.

[12]Report from Deutscher Bundestag, 'Beschlussempfehlung und Bericht des 3. Untersuchungsausschusses der 19. Wahlperiode gemäß Artikel 44 des Grundgesetzes', Drucksache 19/30900, 22 June 2021.

systems to detect this fraud. Especially the second category of revelations is remarkable, as the field of (financial) security is characterised as being 'by nature secretive and particularly difficult to access', with secret operational information, and wherein 'classification and obfuscation are the rule'.[13] The article relies on a number of sources, ranging from interviews with practitioners and participation at practitioners' conferences to newspaper articles and scoops, that is, revelations by the *Financial Times* and other media outlets. Lastly, detailed insights into the role of the FIU and the investigations into the Wirecard scandal are provided by the final report of the German Bundestag's committee of inquiry that has investigated the issue and provided detailed insights and testimonies.

The article proceeds as follows: the following section discusses the current ontologies of financial security and traceability as an ideal of knowing the origins of money when it moves through different bank accounts and financial intermediaries via 'traces' that are produced and collected. Within this ontology money itself is perceived to resemble social relations, and the traces that their activities leave are interpreted as their representations. Section 2 delves into the two scandals and provides nuanced insights into how traceability is disabled and frustrated. It shows how the current regime of financial surveillance relies on practices of categorisation and risk assessments that can be thwarted by infrastructural actors themselves. The last section discusses how digital currencies present the ideal traceability infrastructure as they inextricably link the value of money to the ledger that saves transactions. Digital currencies entail a potential shift in financial security regimes from securing 'money on the flow' towards the securitisation of financial infrastructures themselves. Amid by geopolitical tensions that are fought in and through financial infrastructures these qualities of digital currencies might be leveraged to engender changes in the international financial order.

1. Follow the money: Ontologies of financial traceability

This section discusses the current ontologies of financial security and provides the conceptual nuances that are needed to understand the changes in security regimes, which are described later in the article. As several studies into the field have shown, the notion of financial security is subject to constant change and renegotiation and implies different dimensions, such as the stability of the broader financial system or the financial dimension of sovereign safety.[14] The war on terrorism financing post-2001 deepened another already present nexus of finance and security and brought the domain of mundane financial transactions into the sphere of security.

While appeals for ever more encompassing financial surveillance have become louder, the call to 'follow the money' also reflects the necessity to adjust the security regime to the demands of expanding global financial capital movements, as Anthony Amicelle[15] explains, 'While it has seemed inconceivable to obstruct capital movements in the so-called age of financial market globalization, modalities of control have been shaped to respect it and even to be based on it.' Practices of tracing money have thus 'subsumed the traditional territorialization regarding capital control'[16] that preceded the age of financial globalisation. That prior model was primarily envisioned as a 'fence system' with a topology of a 'container' in which national borders would restrict monetary streams. Making money traceable thus balanced requirements of security and financial liberalism amid new topologies that are defined by the absence of territorial continuity. 'Hence,

[13]Esmé Bosma, Marieke de Goede, and Polly Pallister-Wilkins, 'Introduction: Navigating secrecy in security research', in Marieke de Goede, Esmé Bosma, and Polly Pallister-Wilkins (eds), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* (London, UK and New York, NY: Routledge Taylor & Francis Group, 2020), pp. 1–27 (p. 1).

[14]Nina Boy, 'Sovereign safety', *Security Dialogue*, 46:6 (2015), pp. 530–47; Carola Westermeier, 'Political security and finance: A post-crisis and post-disciplinary perspective', *Zeitschrift für Politikwissenschaft*, 29:1 (2019), pp. 105–22.

[15]Anthony Amicelle, 'Trace my money if you can: European security management of financial flows', in Karin S. Helgesson and Ulrika Mörth (eds), *Securitization, Accountability and Risk Management: Transforming the Public Security Domain* (Abingdon, UK and New York, NY: Routledge, 2012), pp. 110–31.

[16]Ibid., p. 116.

this management of flows would tend to monitor without a priori interfering with the principle of "free circulation", because what becomes fixed is not the surveillance and control but the mark on mobile objects which registers their trajectory.'[17]

These traces that money leaves when it moves through the financial system are thought of as a trail that could provide verifiable information about illicit activities and means to identify those responsible. However, critical inquiries show that traces are both object and product of interventions and deliberations. Based on a review of Francophone literature on digital traces, Tyler B. Reigeluth describes the traces as 'in-formation', meaning that they are being continually formed and reframed, instead of information that is given and only needs to be captured and represented.[18] Traceability infrastructures are thus 'promise and dream of an infrastructure or organized capability in which the origins of things and people can be traced and made visible'.[19] We can then think of traceability as an ideal of knowing the origins of money when it moves through different bank accounts and financial intermediaries, but the traces that are produced and collected remain *in-formation*.

Several contributions to Critical Security Studies have examined the practices and problems of the current regime of financial surveillance, analysing how suspicion is produced algorithmically through correlations of various kinds of data, such as financial transactions, travel data, and social media posts.[20] The significance of financial transactions has been insightfully described by Marieke de Goede, who discusses how suspicious transactions are handled along the chain of security that connects banks, security actors, and financial infrastructure providers such as SWIFT. She describes how financial transactions are inscribed with security meanings and how these are modified when they are sent from private to public actors. Along the chain, financial transactions 'acquire new meanings, new combinations with other data, and new capabilities'.[21] The rest of this section takes a step back in order to shift attention to the infrastructural dimension that enables any transaction to be rendered suspicious (1.1) and the assumptions of traceability that underlie these practices (1.2).

1.1. Financial infrastructure produces traces

As the diver Markus Braun's example illustrates, payments and other forms of transactions have become 'central to security practice because [they are] assumed to provide a complete picture of a person, an "electronic footprint" that makes it possible to identify a suspicious body in movement'.[22] Transactions have obtained this status because they connect the data that conveys a value (the amount of money transferred) with meta-data that provides information about that bit of financial data, including timestamps of transactions, account numbers, names of account holders, location data, and other categorisations. As such, meta-data 'enables most analytic processes, because it is associated with context information'.[23] Taken together data and meta-data form the traces that are 'in-formation'. Transactions thereby link money to the traces that are central to financial surveillance.

[17]Ibid.

[18]Tyler B. Reigeluth, 'Why data is not enough: Digital traces as control of self and self-control', *Surveillance & Society*, 12:2 (2014), pp. 243–54 (p. 253).

[19]Power, 'Infrastructures', p. 118.

[20]Anthony Amicelle, 'Towards a "new" political anatomy of financial surveillance', *Security Dialogue*, 42:2 (2011), pp. 161–78; Karin S. Helgesson and Ulrika Mörth (eds), *Securitization, Accountability and Risk Management*: *Transforming the Public Security Domain* (Abingdon, UK and New York, NY: Routledge, 2012); Louise Amoore, 'Cloud geographies', *Progress in Human Geography*, 42:1 (2018), pp. 4–24.

[21]Marieke de Goede, 'The chain of security', *Review of International Studies*, 44:1 (2018), pp. 24–42 (p. 30).

[22]Louise Amoore and Marieke de Goede, 'Transactions after 9/11: The banal face of the preemptive strike', *Transactions of the Institute of British Geographers*, 33:2 (2008), p. 173.

[23]Mareile Kaufmann and Julien Jeandesboz, 'Politics and "the digital"', *European Journal of Social Theory*, 20:3 (2017), pp. 309–28 (p. 318).

Yet, the traces left behind by money as it 'flows' are produced not by the money itself, but by infrastructures of circulation and storage, such as bank or credit card accounts and networks. If stored in digitalised data repositories – which is the case for most non-cash money – money shares the characteristics of other forms of digital information that 'cannot exist outside of given instantiations in material forms', and that we need to account for how information moves from one material condition to another.[24] It thus matters whether money circulates as cash, via credit cards or as digital money. Each of these material underpinnings conveys different sorts of information – or in the case of cash, no information – that is possibly shared with payment processors and other financial actors when a transaction is sent using their services.

Contemporary financial surveillance is closely connected to the financial infrastructures (including cables, wires, software, and other technologies) that enable international capital flows. As Amicelle explains, 'to the extent that they promote fast, real-time transactions almost all over the world, technological developments would also enhance surveillance by leaving "electronic traces" which enable "money trails" in and out of sovereign territories.'[25] The electronic traces that money leaves are produced by the infrastructures and institutions that allow money to be transferred around the globe. Money relies on infrastructure to store the attributes, such as ownership, that it does not contain itself.[26] As Ludovico Rella argues, '[m]oney's materiality is also always already infrastructural, entailing the system of records, accounts, addresses, and logistics, allowing money's circulation.'[27] We need to take money's infrastructures into account to explain how money is used in differing security regimes. Whereas some forms of transactions such as cash and informal structures leave no traces, more recent and increasingly digitised forms of money tend to carry ever more information about related transactions itself.[28]

1.2. Money as a social relation

The central assumption of financial surveillance that money trails actually reveal activities outside the financial realm is quite remarkable considering that money is actually one of the most unlikely objects to make traceable.[29] Nevertheless, such surveillance is promoted by political actors and security professionals alike and remains largely uncontested.[30] Money remains a potentiality: it holds (purchasing) power, but it does not provide meaning by itself. It is a unit, it merges with other units of money, but money itself is not able to tell anything about its history or possible future.

Financial 'events', such as payments, transactions, and withdrawals produce traces, meaning that concrete actions are captured as data such as payment timestamps or identifiers indicating a transaction's sender or receiver or the medium of payment (credit card or payment application). Financial surveillance is most effective when activities of targeted persons are nearly entirely captured within financial records, in the sense that the events that are outside the financial system are (presumably) captured by financial activities. A trip to Indonesia that is paid for on a credit card, combined with a hotel reservation, fees for diving lessons, and a dinner at a certain restaurant will provide a trail of

[24]Jean-François Blanchette, 'A material history of bits', *Journal of the American Society for Information Science and Technology*, 62:6 (2011), pp. 1042–57 (pp. 1042–4).

[25]Anthony Amicelle, 'Trace my money if you can: European security management of financial flows', in *PRIO New Security Studies*, vol. 10, in Helgesson and Mörth (eds), *Securitization, Accountability and Risk Management*, pp. 110–31 (p. 117), referring to Michael Levi and David S. Wall, 'Technologies, security, and privacy in the post-9/11 European Information Society', *Journal of Law and Society*, 31:2 (2004), pp. 194–220.

[26]Bill Maurer, 'Postscript: Is there money in credit?', *Consumption Markets & Culture*, 17:5 (2014), pp. 512–18.

[27]Ludovico Rella, 'Steps towards an ecology of money infrastructures: Materiality and cultures of ripple', *Journal of Cultural Economy*, 2:14 (2020), pp. 1–14 (p. 10).

[28]Carola Westermeier, 'Money is data: The platformization of financial transactions', *Information, Communication & Society*, 23:14 (2020), pp. 2047–63.

[29]Brett Christophers, 'Follow the thing: Money', *Environment and Planning D: Society and Space*, 29:6 (2011), pp. 1068–84 (p. 1070).

[30]Amoore and de Goede, 'Transactions after 9/11', pp. 173–85.

transactions, all captured in a credit card statement. In sum, these traces form a coherent picture of how the diver Markus Braun might have spent his holidays. Financial transaction data holds immense potential for deducing information about an individual's activities, purchases and geographical movements, but also someone's sexual orientation, health status, religious and political beliefs.[31]

Money has been a long-standing discussion topic within a wide array of social sciences. In particular, studies into the anthropology of money help to conceptualise the claim that money trails resemble and enact social relations. Money carries specific social or cultural meanings, as Viviana Zelizer describes for the use of 'special money': money that is earmarked, that is, intended for a specific use, like the money in the honey jar that is meant for sweets.[32] A basic assumption held by security professionals is that 'special money' can be identified because its earmarking is an objective fact. Thus, financial crime investigations follow money's ascribed social meaning. At the same time, some attributions of money are securitised; for example, sending money to particular organisations is considered to be terrorist financing in some countries, but not in others. Counter-financial crime professionals thus follow money's social, cultural, and political dimensions. Money that circulates between people is understood to manifest their social relations, and the traces that their activities leave are interpreted as representations of these relations – as 'maps' of social networks that seemingly allow the social to be observed from the computer screen upon which these networks become apparent.

In his piece on following money, Brett Christophers discusses what the 'following' the 'thing' that is money aims to 'interrogate the broader constellations of social and economic relations in which money's mobilisations and movements are embedded.'

Money is thus uniquely positioned to 'reveal and examine the social and economic relations both underpinning and occasioned by [its] creation and circulation'.[33] However, the traces that money leaves are not an unequivocal testament to the past but a means of generating and constituting the present. In her response to Christophers' article, Emily Gilbert underscores Reigeluth's suggestion that traces are 'in-formation': the nexus between trace and traceability is not unambiguous. Gilbert highlights the problematic implications of the categorisations and attributions associated with traces, such as social othering along regional differences: 'untraceable cash payments in the Middle East, for example, are used to entrench ideas about shadowy and dubious economies.'[34] Such assumptions are very prevalent in banks' risk assessments, which often tag specific regions as risk indicators.[35]

2. Money on the move

This section examines the processual and material ontologies or faces of traceability. The former 'requires the organisation of technologies – documentary and digital – in processes which create and maintain connectivity among persons and things'.[36] It positions these processes within the global governance of financial surveillance and shows how traceability is supposed to function and can be disrupted along 'chains of security'.[37] Current financial surveillance practices seek to classify transactions within a risk-based reporting regime. The resulting categorisations rely

[31]Valeria Ferrari, 'Crosshatching privacy: Financial intermediaries. Data practices between law enforcement and data economy', *European Data Protection Law Review*, 6:4 (2020), pp. 522–35.

[32]Viviana A. Zelizer, *The Social Meaning of Money: Pin Money, Paychecks, Poor Relief, and Other Currencies* (Princeton, NJ: Princeton University Press, 1997).

[33]Christophers, 'Follow the thing: Money', p. 1070.

[34]Emily Gilbert, 'Follow the thing: Credit. Response to "Follow the thing: Money"', *Environment and Planning D: Society and Space*, 29:6 (2011), pp. 1085–8 (p. 1087).

[35]Marieke de Goede, *Speculative Security: The Politics of Pursuing Terrorist Monies* (Minneapolis, MN: University of Minnesota Press, 2012).

[36]Power, 'Infrastructures', p. 123.

[37]De Goede, 'The chain of security'.

on the collection of traces of money and are thought to enable interventions in possible (but unwanted) futures. The information that is included within transactions is seen as a tool to reveal, for example, terrorists' structures using methods such as social network analysis. The shared belief that 'money trails don't lie' allows for interactions of differing practices and actors.[38] In terms of financial surveillance, explains Anthony Amicelle, 'the existence of traces (financial data), the mechanism to collect them (databases) and the structures to analyse them are needed to enable traceability (compliance officers, FIUs, security services) within an organized system of vigilance.'[39] Yet, traceability is not ensured just because all three components exist; it still has to be enacted, that is, actively put to use. To prove this point, the focus now turns to the efforts of a financial intelligence unit to make the financial traces that are collected by banks useable for prosecution.

The task of making money trails traceable to fight financial crime is highly institutionalised, which encompasses many actors and professions within both public and private realms.[40] It is also enacted as a global regime. Intergovernmental bodies, such as the Financial Action Task Force (FATF), set international standards and monitor their implementation in more than two hundred countries worldwide, aiming for a 'co-ordinated global response to prevent organised crime, corruption and terrorism'.[41] Traceability relies on the close cooperation of private actors such as banks with public sector security authorities: 'According to the logic of "government at a distance", each regulated actor is to be active, responsible, self-regulated and able to decide on what he or she regards as appropriate measures.'[42] Thus, surveillance of financial transactions is a task that is shared between the public and private spheres, as the circulation and distribution of money is largely in the hands of private actors – not only banks, but also payment companies, payment networks, payment technology providers, and messaging networks. Transactions may pass through a number of layers, intermediaries, and parties that are mostly invisible to the receivers and senders.[43] Enabling traceability is thus not only the work of infrastructures but also part of business models and risk calculations. In fact, transaction analysis uses commercial data that is 'collected, reported, shared, moved, and eventually deployed as a basis for intervention by police and prosecution'.[44]

2.1. Financial intelligence units

Around the world, financial intelligence units play a central role in a country's anti-money laundering (AML) and counterterrorism financing (CTF) operations. FIUs are a significant link between the global and national levels of financial governance, as they make individual suspicious transactions detectable by storing and/or possibly forwarding them to national and international security authorities. The tasks of FIUs are internationally agreed. The Council of Europe defines them so:

> The core function of an FIU is the receipt, analysis and transmitting of reports of suspicions identified and filed by the private sector. The FIUs therefore function as an intermediary between the private entities, subject to AML/CFT obligations, and law enforcement agencies.

[38]Tasniem Anwar, 'Time will tell: Defining violence in terrorism court cases', *Security Dialogue*, 53:2 (2022), pp. 130–47.

[39]Amicelle, 'Trace my money', p. 118.

[40]Eleni Tsingou, 'Fighting financial crime: Who designs global governance and who does the work?', *Fudan Journal of the Humanities and Social Sciences*, 13:2 (2020), pp. 169–79.

[41]FATF Homepage 2021, available at: {https://www.fatf-gafi.org/} accessed 1 June 2021.

[42]Amicelle, 'Towards a "new" political anatomy of financial surveillance', p. 173, referring to Nikolas Rose and Peter Miller, 'Political power beyond the state: Problematics of government', *British Journal of Sociology*, 61:1 (1992), pp. 271–303.

[43]Lana Swartz, *New Money*: *How Payment Became Social Media* (New Haven, CT: Yale University Press, 2020), pp. 76–107.

[44]de Goede, 'The chain of security', p. 2.

> The added value of the FIU is the analysis it undertakes of all the information received, as well as the broad range of other financial information it has at its disposal and which it can use to better assess the information on suspicions provided.[45]

In most countries, the procedure is envisioned along the chain of bank → FIU → police authorities/prosecution. This is also internationally agreed, and thus, as noted above, a security practice that is shared across private and public spheres.[46] If banks detect suspicious activities within their customers' transactions, such as potential cases of money laundering or terrorism financing, they are obliged to report them to the national FIU. In many countries, the FIUs receive suspicious transaction reports (STRs) from private actors and are then tasked with obtaining additional information and – if the initial suspicion is substantiated – forwarding them to police authorities, or storing them for further and future investigations.[47] STRs are collections of various traces that money on the move created in the systems of the particular banks. These STRs are stored, compiled, and assembled along certain risk profiles by banks until a collection of traces forms a certain narrative of suspicion. In order to add 'financial intelligence' (i.e., further traces) to an initial suspicion that is reported by a bank, FIUs rely heavily on access to databases, for example, on (ongoing) criminal investigations or specific registers.

FIUs seek to ensure comprehensive surveillance of financial flows. They connect single traces to networks of transactions, categorise them, and decide whether immediate action is necessary. They focus on concrete leads and on particular persons or social networks that they seek to identify through the analysis of financial transactions. As Alya Guseva and Akos Rona-Tes explain, '[t]his clinical approach requires the building of a narrative by documenting sequences of transactions and paying attention to precise amounts, times, places, and recipients of the money – all the information that is attached to electronic payments.'[48]

2.2. Enhancing processual traceability

The German FIU's tasks and challenges are similar to those of other FIUs.[49] Due to automated detection systems, but also due to regulatory obligations, the volume and details of STRs submitted by financial actors have grown steadily over recent years. In Germany, the number of STRs sent to the FIU increased considerably from 60,000 in 2017 to 144,000 in 2020 to 298,507 in 2021.[50] In light of these numbers, the FIU intensified its reliance on traceability systems, which have been defined by Jacob Muirhead and Tony Porter as 'a system that makes it possible, in real time and retroactively, to predict and record reliably the journey of an object from its origin to its destination.'[51]

While banks use software provided by private companies, the FIU relies on software that is provided by the United Nations, called goAML.[52] GoAML's website states that they are 'currently

[45]Council of Europe, available at: {https://www.coe.int/en/web/moneyval/implementation/fiu} accessed 1 August 2021.

[46]Anthony Amicelle and Gilles Favarel-Garrigues, 'FINANCIAL SURVEILLANCE', *Journal of Cultural Economy*, 5:1 (2012), pp. 105–24.

[47]Anthony Amicelle and Vanessa Iafolla, 'Suspicion-in-the-making: Surveillance and denunciation in financial policing', *The British Journal of Criminology*, 58:4 (2018), pp. 845–63.

[48]Alya Guseva and Akos Rona-Tas, 'Money talks, plastic money tattles: THE NEW SOCIABILITY of MONEY', in Nina Bandelj, Frederick F. Wherry, and Viviana A. Zelizer (eds), *Explaining How Money Really Works, Money Talks* (Princeton, NJ: Princeton University Press, 2017), pp. 201–14 (p. 208).

[49]Pieter Lagerwaard, 'Flattening the international: Producing financial intelligence through a platform', *Critical Studies on Security* (2020), pp. 1–15.

[50]Financial Intelligence Unit Germany, Annual Report 2021, available at: {https://www.zoll.de/SharedDocs/Downloads/DE/Pressemitteilungen/2022/z89_jahresbericht_fiu_2021.pdf?__blob=publicationFile&v=3} accessed 29 Sept 2022.

[51]Jacob Muirhead and Tony Porter, 'Traceability in global governance', *Global Networks*, 19:3 (2019), pp. 423–43.

[52]Carolin Liss and J. C. Sharman, 'Global corporate crime-fighters: Private transnational responses to piracy and money laundering', *Review of International Political Economy*, 22:4 (2015), pp. 693–718.

engaged with 111 FIUs among which 49 have already deployed goAML'. It further explains that the software 'acts as a central repository to establish a database of reports on suspicious financial transactions including those from financial institutions (banks, casinos, real estate brokers, and so forth) that are required to report such information.'[53] Generating a database of suspicious financial activities is a core aim of Germany's FIU, along with providing intelligence for police authorities. Even if reports are not forwarded to a police authority, they are stored within the database and may be used for future inquiries.[54]

Figure 1 visualises the sequence for operational analysis as it is envisioned by the FIU. Once a suspicious activity report is generated by a bank and reported to the FIU, it will never disappear. Following a risk-based approach, the reports are processed with more or less urgency and effort.[55] Hence, the FIU should make a judgement whether to forward a report to police authorities immediately, to forward it with a delay in order to have the time to add information, or to not process it at all. If they are assessed, the overwhelming majority of the reported transactions are not passed on to the German police authorities, but nevertheless remain within the databases. Mostly, this is because there is no further evidence to substantiate the initial suspicion. But even the cases like the diver Markus Braun's that do not qualify for further investigation are stored within a database of potential suspicions. These reports then add to an ever-growing digital collection of cases that do not require immediate action, but form a base that may be mobilised for future cases (Figure 1).

Insight into the software's features show how information that is extracted from transactions are sorted into categories and risk assessments. GoAML's core function is to extract and list the traces that are connected to transactions. Figure 2 shows the 'knots', that is, sets of traces organised according to an FIU's demands and categorisations, that enfold from one or more transactions. The underlying data, such as transaction location, description, date, and amount is provided by the reporting entity. It involves information about how the transaction was executed ('transmode_code') as well as possible goods and services that are attached to a payment ('goods_services') and the involved parties (Figure 2).

While goAML works on the basis of applications that may be customised, its default settings already require a lot of information from banks about the customer and the transaction or action that is reported. The set-up is designed to capture the traces that are assumed to manifest within suspicious transactions. Several options are designed to visualise transactional networks and flows. A set of mandatory drop-down menu choices forces banks to assign their customers' actions to specific categories. For instance, goAML requires the user to fill in the legal reason for the report, as the extract from the goAML handbook depicted in Table 1 shows.

Furthermore, banks need to provide customer-related particularities, which are divided into 22 categories, including 'Politically exposed person', 'Conceivable/incomprehensible economic background of the customer', and 'Client or beneficial owner from a country without equivalent standards in relation to money laundering prevention'.[56] These categories determine if and how the transactions rendered suspicious are processed within the traceability systems. These processes of categorisation that are enforced by the software's report templates are thus the result of technologically mediated and culturally situated security practices. They are a key part of processual traceability infrastructures within the current regime of financial security that seeks to capture money as it flows.

[53]United Nations 2021, 'About goAML', available at: {https://unite.un.org/goaml/content/reports} accessed 26 August 2022.

[54]On 30 April 2018 the goAML repository had a total storage of 149,285 natural and legal entities; see Antwort der Bundesregierung auf eine Kleine Anfrage auf BT-Drs. 19/2263.

[55]Amicelle, 'Towards a "new" political anatomy of financial surveillance'.

[56]Terms directly quoted from the English part of the goAML handbook.

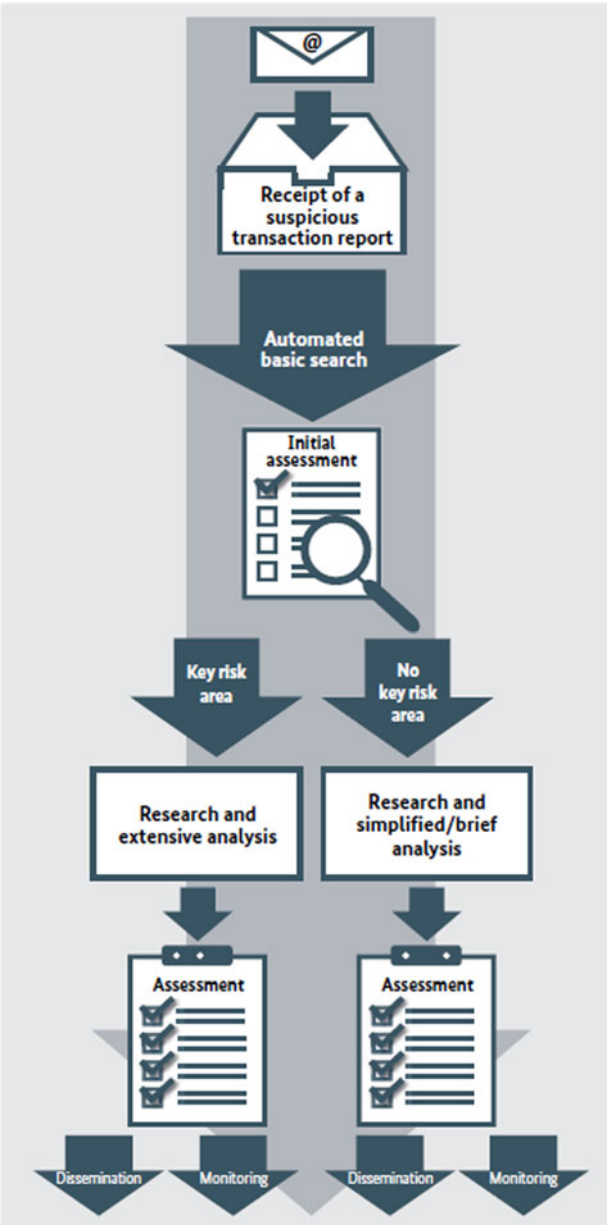

Figure 1. Process sequence for Operational Analysis as envisioned by the German FIU.
Source: Annual Report 2019, p. 14.

2.3. Frustrating traceability processes

Traceability needs to be enacted via technologies and processes that connect concrete actors and objects, such as the traces or STRs, but traceability processes can also be frustrated or thwarted. GoAML was designed to report and transmit suspicious transactions and to 'enable processes without media disruption and integrated analysis'.[57] The software was introduced in Germany in June 2017 when the Financial Intelligence Unit was transferred from the Ministry of the Interior to the responsibility of the Finance Ministry within the 'Zoll' department, which is mostly responsible for

[57]Informationen zur Software goAML, available at: {https://www.zoll.de/DE/FIU/Software-goAML/software-goaml_node.html} accessed 26 August 2022.

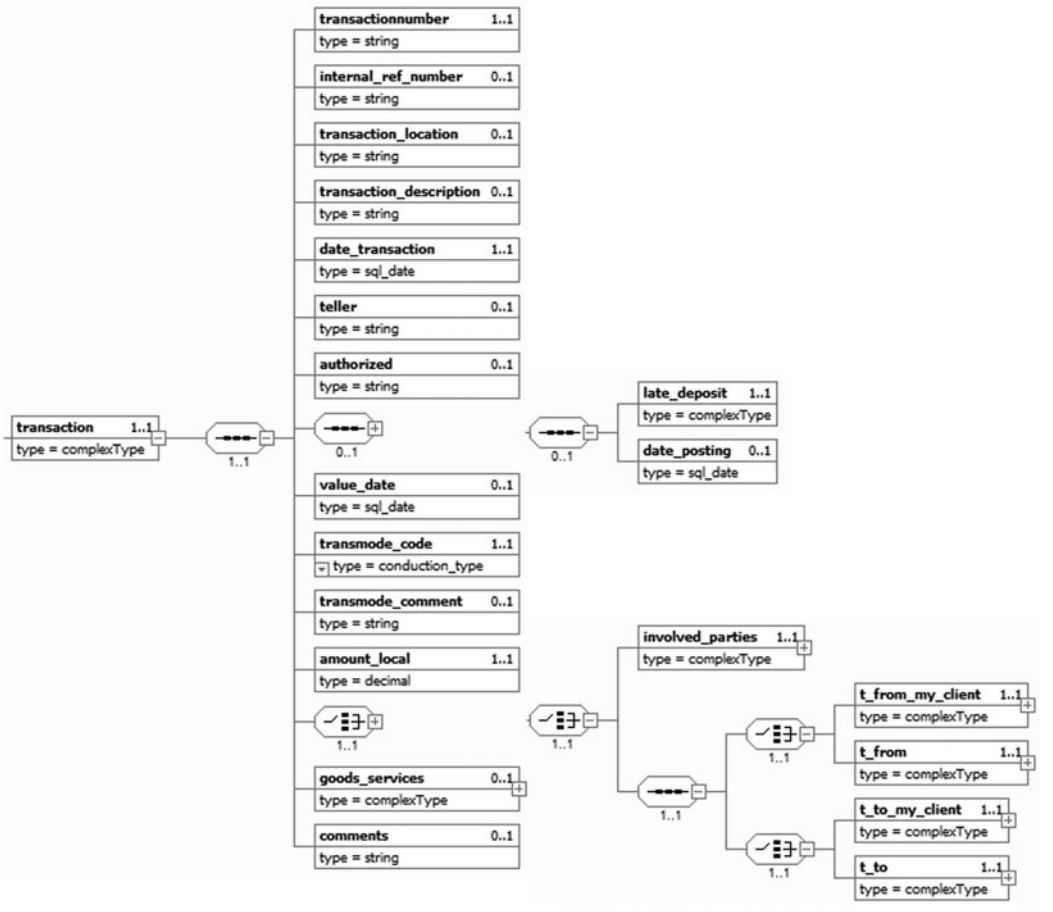

Figure 2. A 'knot' report of a transaction.
Source: AML attachment 2 to goAML Handbook 2018, FIU Germany, p. 9.

Table 1. Extract of a table of categorisation within goAML.

Legal reason acc. § 43 Abs. 1 GwG[58]	
A1000	**Money laundering**
A1001	Transaction i.c.w. money laundering (FIU approval required, §46 par 1)
A1002	Transaction i.c.w. money laundering (respite not possible, §46, par 2)
A1003	Transaction i.c.w. money laundering (subsequent finding, §46, par 2)
A1004	Business connection i.c.w. money laundering
A1005	Brokerage i.c.w. money laundering
A2000	**Terrorism financing**
A2001	Transaction i.c.w. terrorism financing (FIU approval required, §46, par 1)
A2002	Transaction i.c.w. terrorism financing (respite not possible, §46, par 2)
A2003	Transaction i.c.w. terrorism (subsequent determination)
A2004	Business model i.c.w. terrorism
A2005	Item of property i.c.w. terrorism

customs and border security. The aim of this move was to concentrate the STRs within one unit and to only forward 'relevant cases' to the investigating authorities. With the help of goAML, the FIU

[58]Table 1 is directly copied from the English part of the goAML handbook. GwG stands for Geldwäschegesetz, meaning Money Laundering Act.

was intended to act as a 'filter' between the financial institutions and police authorities and/or the prosecutors. However, before goAML could be fully implemented in Germany, it had to be approved by another government agency, which caused a delay of several weeks.

While banks were already using software that fed their data directly into the goAML template, the German FIU itself was simply not allowed to use it. Thus, until August 2017, the only possibility for banks and other authorities who were obliged to file their cases to the FIU was to use a fax machine.[59] This meant that banks' anti-money laundering officers had to print out the STRs which they had typed into the goAML template, and then send them to the FIU via fax. When the reports reached the FIU, the data had to be typed into the goAML system manually, mostly by student assistants. Given the high numbers of STRs submitted, these tasks took time and were prone to errors. Even once goAML was finally in use at the FIU, banks still had to report their cases using both goAML and the fax machine, at least until February 2018.[60] While this low-tech approach was initiated to circumvent the software solution, it created problems of its own. At one AML symposium, banks' employees reported that the FIU's fax machine had apparently run out of paper at some point. Hence, banks did not receive confirmation that their reports had been received. As some of these cases had a specified time limit, these banks resorted to sending their reports by (human) messengers to prove that they had fulfilled their responsibilities. The anecdote shows that the chain of traceability from banks to FIUs and police authorities may be stymied in many ways. Traceability is thus far from being a given within the current financial architecture in Germany or elsewhere.

The most striking evidence of how traceability has been frustrated is the high number of STRs filed by banks that have not been assessed at all. In 2019, the German FIU had accumulated over 40,000 such reports from financial institutions that had neither been passed to police authorities nor processed in their databases. These reports remained unprocessed for several months, and their number had steadily increased.[61] At a conference among financial security professionals, a high-ranking expert explained that he expected the majority of these reports to remain unassessed. He made a remarkable comparison to underline his statement amid the deluge of transaction data being generated but remaining unused: if all the unassessed reports that had been sent to the FIU by financial institutions were printed out and put into folders, these folders would cover the distance from the middle of Germany to Istanbul (more than 2,000 kilometres).

The FIU debacle provides insights into how traceability may be frustrated in its processual capacity, which requires connectivity among actors in the public and private sphere, technologies, and the traces that are generated. The challenges and efforts described here are part of traceability infrastructures as processes that aim to trace money and to collect those traces for further analysis. In an interview in 2019, FIU employees explained that most of their effort at the time went into achieving traceability, enabling the actual use of traces in the first place, and feeding the reports into the database.[62] Thus, traceability for financial security is not simply a product of money's circulation, but requires extensive efforts, cooperation, and thorough enquiry.

2.4. Infrastructurally untraceable: Wirecard

In addition to the ideational and processual faces of traceability, there is a third face that concerns the materiality of traceability infrastructures. For financial traceability, materiality encompasses the technology that processes transactions, including the providers of these technologies. The

[59]Jörg Diehl, 'Die unerträgliche Langsamkeit des Zolls', *Spiegel Online*, available at: {https://www.spiegel.de/panorama/justiz/geldwaesche-spezialeinheit-des-zolles-arbeitet-zu-schlecht-und-zu-langsam-a-1222203.html} accessed 26 August 2022.

[60]See FIU (Financial Intelligence Unit), available at: {https://www.anti-gw.de/29-06-2021/fiu-neu-zentralstelle-f%C3%BCr-finanztransaktionsuntersuchungen/} accessed; see also FATF 2022, 'Anti-Money Laundering and Counter-Terrorist Financing Measures in Germany', ch. 3, available at: {https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-germany-2022.html} accessed 26 August 2022.

[61]See Parliamentary Report, BT-Drs. 19/16464, Antw. BMF v. 02.10.2019 auf SANFR MdB Herbrand gibt es das Online?

[62]Interview FIU, October 2019.

Wirecard scandal exposed how money can be rendered untraceable *infrastructurally* by a financial technology company. The following analysis focuses on the business model that made Wirecard successful in the first place, rather than the question of how €1.9 billion could go 'missing'.[63]

The Wirecard affair has several layers: fraud, high-level lobbying and close relations between financial and security personnel, as well as regulatory failure. A parliamentary inquiry questioned why authorities failed to detect the accounting fraud, suspecting that the company was politically supported and protected because of the lure of establishing a national technology leader. The criminal case against Wirecard's executives has focused on accounting malpractices that the company conducted for years, reaching a peak in June 2019 when the *Financial Times* published a series of investigations.[64] The scandal and the revelations that followed Wirecard's collapse allow a reconstruction of how their business model built on the camouflaging of transactions, exploiting their infrastructural position in order to generate more revenue.

To understand Wirecard's (initial success) story, one needs to take into account the growing importance of payments as a fast-growing sector in finance, profiting from the rise of e-commerce and cashless payments. Wirecard focused on what are called high-risk transactions, meaning transactions that many other payment companies would avoid, such as those related to gambling and pornography. High-risk transactions are often associated with the risk of fraud, merchant closure, or chargebacks. For these reasons, high-risk transactions come with higher costs for the merchant who is categorised as a risky business.[65] Wirecard claimed that their superior algorithms would allow them to process these high-risk transactions for a comparatively low price. While this might have been the cause of Wirecard's initial success, the recent revelations show that obscuring the nature of transactions was also part of Wirecard's business practices. They used their position as a payment technology provider to mislead traceability systems. Since transactions that carry payments are sorted into hundreds of categories, ranging from bakeries to gambling, Wirecard simply placed high-risk payments into low-risk categories. As a report by Bloomberg describes, 'some Wirecard programmers have spoken openly about masking merchants' identities, which can facilitate money laundering and circumvent laws banning online gambling. From that dross, … Wirecard [expanded] into a global payment player.'[66]

To disable the traces that render suspicious and risky transactions detectable by automated systems and other financial actors, Wirecard hid them in unsuspicious categories. As processing electronic payments often involves a number of players, such as merchants, (credit card) issuers and acquirers, Wirecard also defrauded card networks like VISA and Mastercard, which act as intermediaries between issuers and acquirers. These networks also need to comply with international AML and CTF regulations, and they set their own terms and conditions. As Wirecard infrastructures were closely entangled with payment networks, Wirecard 'relabelled' risky transactions in order to evade detection by the card networks' traceability systems. The large card networks demand that every processed transaction receives a country transaction code as well as a merchant category code. The latter is a four-digit number that describes the type of business receiving the payment, such as 7995 for gambling establishments, 5667 for pornography, 5698 for wig and toupee stores, 7273 for dating and escort services, and 9223 for bail and bond payments.[67] These codes permit other banks and the networks to decline transactions based on

[63]'Wirecard: Scandal-hit firm files for insolvency', *BBC News* (25 June 2020).

[64]'House of Wirecard', *Financial Times*, available at: {https://www.ft.com/content/47f13654-1ebc-4c4c-903a-55cafa453eb8} accessed 1 June 2021.

[65]Swartz, *New Money*, pp. 76ff.

[66]Eyk Henning and Benedikt Kammel, 'The Man Who Could Explain the $2 Billion Wirecard Mystery Is Missing', Bloomberg, available at: {https://www.bloomberg.com/news/articles/2020-11-10/jan-marsalek-the-man-who-could-explain-wirecard-s-2-billion-fraud-is-missing} accessed 1 June 2021.

[67]'Was hat dieser Mann mit Wirecard zu tun?', *ZEIT Magazin*, 41 (2020), pp. 15–17; Visa Core Rules and Visa Product and Service Rules 2021, available at: {https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf.} accessed 1 June 2021.

specific country or merchant codes that reflect high-risk transactions or high-risk locations. Hence, payment processors determine whether they place holds on merchant funds to protect themselves. If the code of the transaction is changed, say from gambling to florists, the transaction runs unflagged and thus smoothly through the systems. As illustrated in the Zatarra Report, Wirecard used a 'mirror company' with low risk categorisation to enabled the relabelling of transactions (Figure 3).[68]

When the details of the Wirecard scandal became public, the involvement of the beleaguered German FIU was also scrutinised. The case's political relevance and media attention enabled a detailed reconstruction of how STRs are handled, how traceability is turned into suspicion, and how this mechanism can fail. During the parliamentary inquiry it became apparent that it was well within the realm of possibility that a number of STRs issued by other banks concerning Wirecard were part of a total amount of 40,073 reports that were faxed to the FIU and handled manually, and that largely remained uncategorised and unprocessed.[69]

Wirecard was in a position to foil money's traceability on the infrastructural level for their purposes and thus largely avoided coming under suspicion themselves. The camouflaged transactions appeared in their and in other payment providers' databases and were transferred along financial infrastructures. However, due to the use of false categories, they were not detected. A provider of payment infrastructures was thus able to cover up the tracks of suspicious money flows. Additionally, as the scandal broke, it was discovered that other security authorities had asked for Wirecard's help in certain investigations. At the same time as Wirecard was camouflaging some transactions for their own fraudulent purposes, the company also cooperated with police authorities to facilitate the traceability of other money flows for security purposes. For instance, it opened several accounts and issued credit cards that were used to monitor money flows of suspects as part of criminal investigations. The data provided by Wirecard was used by the police to determine the location of known and unknown suspects. The financial data was shared so intensively with security forces that they could follow the suspects in close to real time. Wirecard also issued credit cards for the federal police that could be used by undercover agents.[70]

The Wirecard affair thus reveals how traceability can be thwarted by the materiality that sought to enhance it. Traceability relies on the infrastructure of transactions, their digital storage, and technologies of circulation. By manipulating and covering up the traces of data that money leaves when it circulates through their channels, Wirecard obscured the trail. Even so, the materiality of financial transactions is not yet perceived as a potential challenge to traceability. As the categorisations used by the FIU show, current regimes of security are not attuned to fraud at the level of transactional infrastructures, but focus on fraud within the social relations that the transactions are assumed to reflect. Consequently, no category of suspicion within goAML applies to the infrastructure of the transaction itself. Suspicion is only attuned to a change in the underlying materiality, such as large sums of cash, the use of anonymous payment services, or the usage of 'unusual means of payment outside the established banking sector'.[71] As current systems of financial surveillance adhere to the claim of 'follow the money', they are unable to scrutinise the infrastructure that makes money traceable. The infrastructural provision of payment channels is considered not as particularly risky, but as a presumably neutral technology.[72] However, as recent geopolitical battles have been fought in and via financial infrastructures, the presumable neutrality of financial technologies is increasingly contested, and financial infrastructures themselves are subjects of securitisation.

[68]Viceroy Research, 'Zatarra Research & Investigations – Wirecard Reports' (2020), available at: {https://viceroyresearch.org/wp-content/uploads/2020/07/final-main-report-zatarra-edited-3.pdf} accessed 1 June 2021.

[69]Report from Deutscher Bundestag, p. 1812.

[70]Report from Deutscher Bundestag, pp. 1466, 1473.

[71]See goAML Handbook.

[72]Jeff Salway, 'Wirecard's collapse exposes gap in payments regulation', *Financial Times* (30 September 2020).

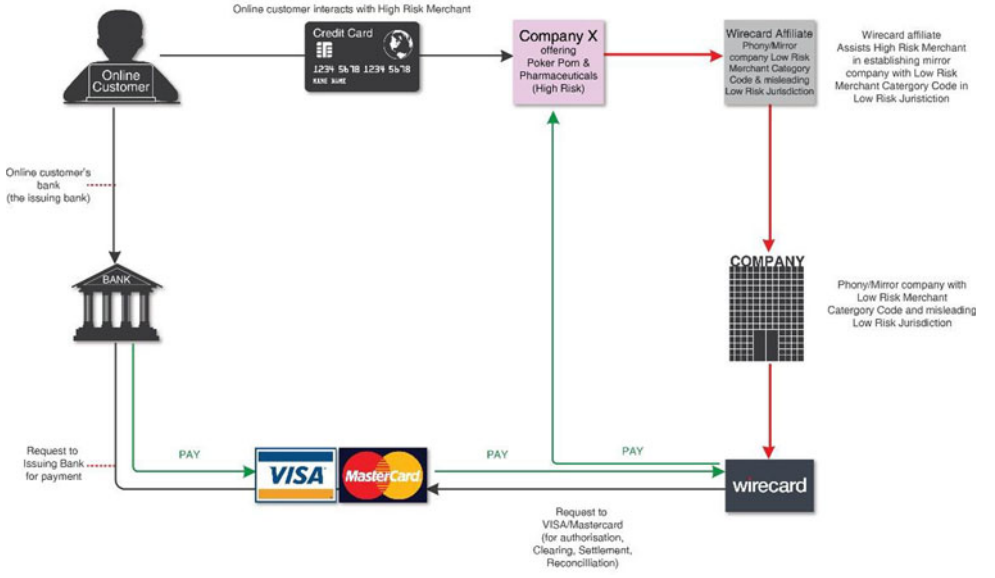

Figure 3. Wirecard's model to obscure transactions and evade detection by traceability systems.
Source: Taken from Zatarra Report, p. 3.

3. Traceability by design: Digital currencies

This last section discusses a shift in financial security regimes from securing 'money on the move' towards the securitisation of financial infrastructures themselves. This shift is engendered by geopolitical battles that are fought in and through financial infrastructures.[73] Digital currencies that rely on new financial infrastructures entail the possibility of enabling a regime of financial surveillance that does not primarily adhere to demands to keep financial globalisation moving. Instead, digital currencies that are currently being promoted by central banks around the world provide the infrastructural means to enhance a more fractured financial order in which money does not move across intermediaries and layers, but is instead stored in databases and updated. With fully digital money, the value of money is inextricability linked to the database that saves the transactions. As described above, with conventional bank accounts banks hold the digital records of their costumers' transactions. Making money traceable herein means to track money through (several) bank's records. In contrast, digital currencies rely on (de)centralised ledger(s) in which all transactions are stored, transactions are readily decipherable. Digital currencies thus decrease the need to 'follow the money' and instead put financial infrastructures themselves at the core of security efforts. The following first explains how digital currencies further the promise of traceability infrastructures by referring to the technology used by the digital currency bitcoin. It then turns to how the technological implications of digital currencies heighten new security demands amid growing geopolitical tensions.

Traceability is a central feature of digital currencies. Cryptocurrencies such as Bitcoin and most central bank digital currencies (CBDCs) either rely on distributed ledger technology (such as Blockchain) or a centralised ledger. Either way, they both store transaction data in files (called blocks) and use specific mechanisms to verify transactions. A transaction thus leads to an update in the database of records of monetary holdings when users transfer holdings of digital money to each other. This way, the underlying ledger of digital currencies, a blockchain or centralised ledger, does away with the frictions of intermediaries (i.e., tracing transactions

[73]de Goede and Westermeier, 'Infrastructural geopolitics'.

through the records of differing banks). As Power explains, 'blockchain is therefore the dream of, the metaphor for, a perfect, uniquely referential and precise traceability infrastructure. It is the audit trail in its purest form.'[74] Bill Maurer explains what this means for the digital currency Bitcoin:

> With Bitcoin, the token and the decentralised database are of a piece and inseparable. One cannot take a bitcoin out of the digital ledger and have it remain a bitcoin. … Bitcoins only exist within the network. The network is, in a sense, its own digital world.[75]

Bitcoins do not have any physical shape. They are not stored on a hard drive or on a spreadsheet, but exist as records of transactions within the blockchain.[76] 'Blockchains are infrastructures that enable the movement of data as representation and value', and they are used as the underlying infrastructure for a number of cryptocurrencies.[77] The (potential) value that is moved within these data infrastructures is thus '*data money*', which is merely a 'right to transfer data'.[78] Thus, crypto money is not just money that leaves traces, but it exists as data. Money thus does not 'flow' anymore, but is updated within the ledger.

Unlike digitised, 'regular' money that can still be carried as cash, Bitcoin only exists as value embedded within the blockchain. The traceability of every transaction is essential to cryptocurrencies. Obscuring the transmission of value from one (digital) wallet to another would run contrary to the efforts built into a cryptocurrency's design to establish trust in it.[79] However, traceability should not be confused with lack of anonymity. What is fully traceable is the value that is moved from one node to another within the network. What is not necessarily connected to these transactions are traces of ownership or other indicators of social interaction besides the transaction itself. A transaction can be *anonymous* if the sender and receiver are anonymised, that is, there is no identifiable information connected to their wallet, for example via a token-based access.[80] However, the traceability of the transaction cannot be disabled or hidden within digital ledgers. As the chain of transactions *is* the value, the cryptocurrency itself would fail if traceability were obscured.

Bitcoin's traceability by default might sound surprising given that the cryptocurrency is often perceived as part of the 'underworld' of the global economy. Once the address of a particular wallet is known, every transaction to and from that wallet can be traced while the wallet's owner might still be unidentified. To make their payments anonymous, users of the currency can anonymise the use of their wallets or use a new wallet for every transaction. Increasingly, though, AML compliance that follows requirements by global standard-setters like the FATF has led to the mainstreaming of blockchain usage.[81] XPR, a cryptocurrency offered by Ripple, even

[74]Power, 'Infrastructures', p. 120.

[75]Bill Maurer, 'The politics of token economics, then and now', in Antonino Crisà and Clare Rowan (eds), *Special Publication / Royal Numismatic Society, Tokens: Culture, Connections, Communities* (London, UK: Royal Numismatic Society, 2019), pp. 215–30 (p. 220).

[76]'How Do Bitcoin Transactions Work?', available at: {https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/} accessed 1 June 2021.

[77]Koray Caliskan, 'Data money: The socio-technical infrastructure of cryptocurrency blockchains', *Economy and Society*, 49:4 (2020), pp. 540–61 (p. 543).

[78]Ibid., p. 546.

[79]Taylor C. Nelms, Bill Maurer, Lana Swartz, and Scott Mainwaring, 'Social payments: Innovation, trust, Bitcoin, and the sharing economy', *Theory, Culture & Society*, 35:3 (2018), pp. 13–33.

[80]Token-based access is based on cryptographic knowledge, not necessarily identification.

[81]Malcolm Campbell-Verduyn and Marcel Goguen, 'The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime', in Malcolm Campbell-Verduyn (ed.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (London, UK: Taylor and Francis, 2017), pp. 69–87, pp. 78ff.

highlights their ability to make funds more visible than those in the established financial system, promising 'complete end-to-end transaction traceability'.[82]

Central banks around the world have pursued the question of whether they should issue a digital currency and, if so, what form this should take.[83] While the concrete architecture of most CBDCs still has to be decided, the broader implications of this traceability infrastructure are already becoming evident. CBDCs and cryptocurrencies such as Bitcoin both rely on a ledger that records all transactions of the digital currency. The crucial difference between cryptocurrencies and CBDCs is the form of the ledger. While Bitcoin relies on a decentralised system, which records all transactions on a ledger that is distributed across a network, a number of CBDCs will most likely rely on permissioned blockchain or centralised[84] ledgers that are not publicly accessible.[85] The concrete design choices that are currently discussed within central banks around the globe will decide if the central bank will keep a central ledger of all transaction or rather maintain a wholesale ledger while private intermediaries execute payments.[86] Regardless of their concrete choices, CBDCs would dramatically increase the control over financial transactions. As Horacio Ortiz describes based on an analysis of various CBDC projects,

> All transactions would be totally traceable by central banks and could only be made anonymous by design. Central banks, like other banks, would indeed have to guarantee total traceability in order to comply with regulations designed to prevent tax evasion, money laundering, and criminal transactions like the financing of terrorism.[87]

Control over a (centralised) ledger of a digital currency would provide central banks with unknown powers. A report published by the influential Bank for International Settlements explains that the shift from money as a 'social convention' to 'money as memory' comes with the 'idea of a complete digital ledger' and a monetary system that is built around it.[88] The inextricable link of money with its infrastructure has wide-ranging implications for the governance of money 'when it is used in exchange as the record-keeping device of society'.[89] The question whether a central bank digital currency (CBDC) can have cash-like features in the sense that there may still be transactions that leave no traces is answered straightforwardly: as a (fully) digital form of payment, CBDCs are 'generally traceable as they leave digital footprints that enable a transaction to be followed'.[90] The question how privacy can be ensured despite full traceability is an ongoing concern among central bankers.[91] Even though the concrete architecture of the

[82]Ludovico Rella, 'Blockchain technologies and remittances: From financial inclusion to correspondent banking', *Frontiers in Blockchain*, 2 (2019).

[83]Raphael Auer and Rainer Böhme, 'The technology of retail central bank digital currency', *BIS Quarterly Review* (March 2020).

[84]Gabriel Soderberg et al., 'Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons'. IMF FinTech Notes No 2022/004.

[85]The choice between a Distributed Ledger Technology and Centralised Technology is debated in a series of papers, see Raphael Auer, Giulio Cornelli, and Jon Frost, 'Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies', BIS Working Papers, No. 880 (2020).

[86]Design choices include distinct CBDC architectures, such as direct, hybrid, or intermediated CBDCs as well as account-based or token-based CBDCs. See Auer, Cornelli, and Frost, 'Rise of the Central Bank Digital Currencies'.

[87]Horacio Ortiz, '"CBDCs mean evolution, not revolution": Central bank digital currencies in the time of COVID', in Didier Fassin and Marion Fourcade (eds), *Pandemic Exposures: Economy and Society in the Time of Coronavirus* (Chicago, IL: HAU Books, 2021), pp. 369–83 (p. 373f).

[88]Raphael Auer, Cyril Monnet, and Hyun Song Shin, 'Permissioned Distributed Ledgers and the Governance of Money', BIS Working Papers, No. 924 (2021).

[89]Ibid., p. 40.

[90]Ibid., p. 11.

[91]European Central Bank, 'Report on a Digital Euro' (October 2020), p. 27, available at: {https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html} accessed 4 April 2022; European Central Bank and the Bank of Japan, 'Balancing

future central bank-issued digital money still has to be decided, none of the potential options make a cash-like degree of anonymity possible.[92] Digital currencies and more specifically the infrastructures (i.e., the ledger) that enable their usage and storage can thus be seen in a way as the culmination of current financial surveillance efforts: they provide an index of all financial relations executed with this currency. Unless some form of anonymity is explicitly enabled, financial, and the connected social traces are fully traceable within a database which inextricably links money to its transactional history.[93]

Central bank digital currencies connect money to the infrastructure that records transactions and thus enhance all three faces of traceability characterising the current financial surveillance regime, which subscribes to the dogma of 'follow the money'. With CBDCs, the main obstacles hindering traceability processes will be redundant as money will not travel through differing financial actors or intermediaries and their databases. Instead, banks and other financial actors could be linked to the (de)centralised ledger and have permission to update the record of transactions.

Infrastructural change, however, is not readily induced by technological innovation. The technology of digital currencies has already been in use for more than a decade as Bitcoin was set up in 2009. High-level financial policymakers entertained the idea of issuing a digital currency already in 2016, but central banks and governments have only started to push for their implementation in recent years.[94] One main driver for the introduction of CBDC has been the shift of security efforts to securing financial infrastructures amid geopolitical tensions. Infrastructural change, however, is not solely driven by altering (security) politics, but infrastructures also engender geopolitical change.

3.1. Securing financial transactions infrastructurally: Central bank digital currencies

As financial security practices and infrastructures enhanced by the demand to follow the money enabled the post-9/11 security regime to be broadened and deepened, central bank digital currencies similarly entail the possibility to enhance security demands that are currently evolving. CBDCs combine the role of 'money as data' and the use of transactional data for security and possibly economic purposes with the increasing relevance of financial infrastructures in geopolitical struggles.[95] With regard to the role of money as memory, that is, to store all transactional data in one non-public ledger, the digital yuan (or digital RMB) is perceived as a way for the Chinese government to get a more detailed picture of its population through big data, thus 'adding financial data to digital authoritarianism'.[96] Such centralised monitoring and control of a digital currency would make the efforts described in this article to collect and combine financial

Confidentiality and Auditability in a Distributed Ledger Environment', available at: {https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200212.de.html} accessed 4 April 2022.

[92]Currently, models that enable different levels of anonymity are discussed, i.e., stronger identification requirements associated with higher transaction limits. See also Hanna Armelius, Carl A. Claussen, and Isaiah Hull, 'On the Possibility of a Cash-Like CBDC', Sveriges Riksbank Staff memo, available at: {https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf} accessed 4 April 2022.

[93]See, for a discussion on CBDC and privacy, Jonas Gross et al., 'Designing a Central Bank Digital Currency with Support for Cash-Like Privacy', available at: {http://dx.doi.org/10.2139/ssrn.3891121} accessed 4 April 2022.

[94]See, for example, Yves Mersch, 'Distributed Ledger Technology: Panacea or Flash in the Pan?', Speech Frankfurt am Main, 25 April 2016.

[95]Westermeier, 'Money is data'; Marieke de Goede, 'Finance/security infrastructures', *Review of International Political Economy*, 28:2 (2021), pp. 351–68.

[96]Yaya J. Fanusie and Emily Jin, 'China's Digital Currency. Adding Financial Data to Digital Authoritarianism', Center for a New American Security, available at: {https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Chinas-Digital-Currency-Jan-2021-final.pdf?mtime=20210125173901&focal=none} accessed 23 August 2021; Barclay Bram, 'China's digital yuan is a warning to the world', *WIRED*, available at: {https://www.wired.co.uk/article/digital-yuan-china-bitcoin-libra} accessed 23 August 2021.

data for (financial) surveillance redundant and instead allow unknown forms of financial surveillance and intervention.

Other far-reaching implications of CBDCs have been highlighted with regard to the geopolitics of sanctions. Sanctions crucially rely on the ability of some state – primarily the United States – to weaponise financial infrastructures for their security agendas. Already before the recent use of unprecedented sanctions in reaction to Russia's war against Ukraine international payment infrastructures had been a field of geopolitical battles. The post-9/11 regime of financial surveillance has extended the reach of US security practices to financial infrastructure providers such as SWIFT, but also VISA and Mastercard, and thus amplify their political demand to 'follow the money' or to halt financial flows altogether.

However, the ability to use financial infrastructures for geopolitical means relies on (partly colonial) power relations that are sedimented into financial infrastructures.[97] Emerging financial technologies allow to challenge this power infrastructurally. Central bank digital currencies provide means to circumvent and recreate the established financial order and to organise national and international transactions in new ways. The digital RMB is thus promoted as a way to reduce exposure to US-controlled financial networks.[98] The fact that currently a number of central banks develop digital currencies against the background of increasing geopolitical tensions makes infrastructural changes more likely. However, it needs to be established that while emerging financial infrastructures allow new financial security regimes to take shape, these developments are not inevitable. What could diminish tendencies of financial fragmentation is the international community of central bankers as their epistemic community relies on close cooperation and shares a set of normative beliefs that include that promotion of global financial activities.[99]

In the context of geostrategic conflict, however, international governance and cooperation – as explained in section 2.1 – tend to get sidelined. Instead, control over domestic payment infrastructure gains importance so as to lower exposure to international sanctions. Here CBDCs provide an alternative to the established financial system in which intermediaries, such as SWIFT, and US-based financial networks, such as VISA and Mastercard, have the capacity to halt international transactions. With CBDCs, cross-border payments will need to take new forms to enable interoperability. Cross-border payment infrastructures may be provided by international actors such as SWIFT, but other options are multi-CBDC platforms, which are currently explored.[100] These arrangements would more likely resemble the 'container model' of financial security that preceded the current model of international flows. Within this digital container model, control over ledgers would determine control over monetary streams and financial surveillance.

While CBDCs present a culmination of the current security regime that seeks to enhance money's traceability, they also have the potential to alter the international architecture of financial surveillance and the concomitant geopolitical security practices. It is thus unsurprising that security experts have discussed the implications of CBDCs for the security interests of the United States and have urged US policymakers to consider them.[101] The European Central Bank develops the Digital Euro in response to the dominance of non-European actors in the European payments systems 'with the goal of safeguarding our strategic autonomy as established by the

[97]de Goede and Westermeier, 'Infrastructural geopolitics'.

[98]Ying Huang and Maximilian Mayer, 'Digital currencies, monetary sovereignty, and U.S.–China power competition', *Policy & Internet*, 14:2 (2022), pp. 324–47.

[99]Carola Westermeier, 'The Bank of International Settlements as a think tank for financial policy-making', *Policy and Society*, 37:2 (2018), pp. 170–87.

[100]Raphael Auer, Codruta Boar, Giulio Cornelli, Jon Frost, Henry Holden, and Andreas Wehrli, 'CBDCs beyond Borders: Results from a Survey of Central Nanks', BIS Papers, No. 116 (2021); see also projects 'mCBDC Bridge' and 'Project Dunbar' at the Bank for International Settlements.

[101]Sara Sewall and Ming Lou, 'Geopolitics of Digital Currency', Belfer Center for Science and International Affairs (January 2022).

European Council'.[102] Leading central banks thus see CBDCs as a crucial means to respond to perceived threats to the established international financial order, making the infrastructure itself subject to security efforts.

Conclusion

The introductory anecdote about Markus Braun, the diver, provided an example of how financial surveillance currently works: his name was flagged as suspicious and his transactions were reported to the German Financial Intelligence Unit by a bank that handled his international payments. The reason his transactions were declared 'suspicious' in the first place is the scandal around Wirecard in which an infrastructural actor, led by a person with the same name, camouflaged risky transactions by mis-categorising them. Analysing this scandal and the FIU's efforts to collect traces and their slow uptake of tracing software along the ideational, processual, and material faces of traceability infrastructures provided insights into how money's traceability can be enabled or frustrated. Financial security practices are currently adjusted to the desired free movement of capital in which money 'flows' and is sent from one bank account or custodian to another, crossing countries, financial actors, and intermediaries and infrastructures.

The two incidents, however, have not led to profound changes in the current security regime and its infrastructural setting. Rather, they have reiterated what has been found in the case of other financial scandals in which problems were turned into issues of individual failing. As such, the Wirecard scandal currently manifests in the prosecution of Wirecard's CEO and the search for its fugitive COO, not in a significant reform of today's financial security architecture.

While the practices of 'follow the money' have not been questioned in the light of these scandals, increasing geopolitical tensions give rise to new security demands. With digital currencies financial surveillance shifts from the monitoring of financial flows and flagging of suspicious or illicit transactions towards the storage of financial data in (de)centralised ledgers that inextricably link money to its infrastructure. Hence, in these ledgers, what we understand as money does not 'flow', but rather is updated, making the financial infrastructures themselves security projects. This new form of transactional surveillance corresponds to shifting geopolitical agendas that increasingly promote fractured instead of globalised financial infrastructures.

The 'follow the money' regime allowed states to link globalisation and the free flow of money to the security narrative of the 'war against terror'. While this regime will not be replaced but continue in the fight against financial crime, new central bank digital currencies have the potential to create 'digital currency containers' providing domestic control over financial transactions. This renewed use of finance for (security) politics also requires new attention by (critical) security studies and international political economists. While the war on terror has led scholars to question security practices and risk assessments at the intersections of finance and security, geopolitical security politics increasingly target financial infrastructures as an archive of national and international (financial) interactions and as a means to advance geopolitical security agendas. Further research needs to be attentive to this entanglement of (financial) security and (geo)political tensions, in particular to the development and implementation of CBDCs.

Acknowledgements. I would like to thank Martin Coward for his editorial work and four anonymous reviewers for their constructive comments. Many thanks to the participants to the workshop 'Production Chains and Security Apparatuses' at the University of Bayreuth for their generous comments. The section on CBDCs benefited from conversations during my fellowship at the Weizenbaum Institute, Berlin. The FOLLOW research team at the University of Amsterdam and Marijn Hoijtink provided feedback on an earlier version of this article.

Funding. This project has received funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme (Research Project 'FOLLOW: Following the Money from Transaction to Trial', Grant No. ERC-2015-CoG 682317).

[102]Fabio Panetta, 'The Present and Future of Money in the Digital Age', Speech, Rome, 10 December 2021; Fabio Panetta, 'The Digital Euro and the Evolution of the Financial System', Speech Brussels, 15 June 2022.

Carola Westermeier is Visiting Professor of International Relations and International Political Economy at Goethe University Frankfurt and co-leader of a research project on Financial Infrastructures and Geoeconomic Security at the Justus Liebig University Giessen. Before, she was postdoctoral researcher at the FOLLOW project, supported by a Consolidator Grant of the European Research Council (ERC). Her research is based at the intersections of (critical) security studies, international political economy, and political sociology. Her empirical focus lies on financial security and the politics of (data) infrastructures. Author's Twitter: @C__West and website: www.carolawestermeier.org

Cite this article: Westermeier, C. 2023. From flows towards updates: Security regimes and changing technologies for financial surveillance. *Review of International Studies* **49,** 615–636. https://doi.org/10.1017/S0260210522000493