The Digital Network of Networks: Regulatory Risk and Policy Challenges of Vaccine Passports

Abstract

The extensive disruption to and digital transformation of travel administration across borders largely due to Covid-19, means that digital vaccine passports are being developed to resume international travel and kick-start the Global economy. Currently a wide range of actors are using a variety of different approaches and technologies to develop such a system. This paper considers the techno-ethical issues raised by the digital nature of vaccine passports and the application of leading-edge technologies such as blockchain in developing and deploying them. We briefly analyse four of the most advanced systems: IBM's Digital Health Passport "Common Pass," IATA's Travel Pass, the Linux Foundation Public Health's COVID-19 Credentials Initiative and the Vaccination Credential Initiative (Microsoft and Oracle) and then consider the approach being taken for the EU Digital Covid Certificate. Each of these raise a range of issues, particularly relating to GDPR, and the need for standards and due diligence in the application of innovative technologies (e.g., blockchain) that will directly challenge policymakers when attempting to regulate within the network of networks.

I INTRODUCTION

In May 2021, the EU approved the adoption of the EU Digital Covid Certificate from 01 July 2021, which will facilitate the resumption of free movement throughout member states.[1] While offering a paper version, the certificate will be most effective as a digital instrument to ensure safe travel across borders. Renamed from the green passport, it will contain a limited data set, will be encrypted, and may be shown independently of the passport.

The speed of agreement and delivery of the Covid-19 vaccine passport suggests that there has not been sufficient time to fully consider the risks or to develop policy around their regulation. There are clear issues concerning restricting movement based on one's medical profile. While understanding of the immunology of Covid-19 is advancing, driven by for example, the Sinai Immunology Project,[2] it may not be seen as providing sufficient policy expertise to underpin vaccine passport regulation.

[1] EC (2021) Coronavirus: Commission proposes a Digital Green Certificate. Available at: https?//ec.europa.eu/commission/presscorner/detail/en/IP_21_1181

[2] Vabret, N. et al (2020) Immunology of COVID-19: Current state of the science. Immunity, 52(6), 910-941.

The prospect of limited vaccine production capacity and inequities in distribution, alongside issues of intellectual property creates some concern about Global access to the vaccine. In addition, the technological gaps experienced by those negatively impacted by the global digital divide will mean that the excluded both inside and outside the EU, may exceed those connected and included for some time to come.[3]

Issues concerning fairness, responsibility and the erosion of civil liberties have been well rehearsed.[4] The exclusion of people who are unable to have the vaccine for medical reasons, the discrimination against vaccine hesitant ethnic minorities and others, the differential rollout of vaccines in different countries and differential access to vaccines and medical care are some examples of the social and ethical issues associated with vaccine passports.[5] It can be argued, that not only will a vaccine passport be ineffective if vaccination has not extended to appropriate epidemiological levels, but that it will create new borders based on safe or unsafe bodies.[6]

However, less attention has been given to the ethical and regulatory issues associated with the digital platforms and networks appropriated to develop vaccine passports. These technologies involve substantial integrated networks, connecting a range of institutional actors and leading-edge technologies such as blockchain. The development of the passports and associated applications, involve technology companies and open-source communities in application programming, in an ecosystem in which regulation is weak and risks are significant.

Regulatory frameworks in these areas are in their infancy. For example, in the United Kingdom, the NHS risk assessment of digital health applications, implemented as the Digital Technology Assessment Criteria, was only introduced in early 2021.[7] Efforts to regulate the growing population of digital health applications is hampered by the lack of sources of evidence about their use, benefits, and harms.[8]

This contribution summarises the technological basis and processes for four health passes currently under development/being deployed, to expose the regulatory risks, and policy vacuums[9]

[3] Editorial (2021) The rocky road to universal COVID-19 vaccination Lancet Infectious Diseases May 14;21(6):743. doi: 10.1016/S1473-3099(21)00275-9

[4] Brown. R.C.H., Saveluscu. J., Williams. B., Wilkinson. D., (2020a) Passport to freedom? Immunity passports for COVID-19. BMJ Journal of Medical Ethics 46:10

[5] Royal Society (2021) Twelve criteria for the development and use of COVID-19 vaccine passports. https://royalsociety.org/-/media/policy/projects/set-c/set-c-vaccine-passports.pdf?la=en-GB&hash=A3319C914245F73795AB163AD15E9021

[6] Kofler,N and Baylis,F. (2020) Ten reasons why immunity passports are a bad idea. Nature 581, 379-381

[7] NHS Digital Technology Assessment Criteria. https://www.nhsx.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/

[8] Rodriguex-Villa, E. and Torous, J, (2019) Regulating digital health technologies with transparency: the case for dynamic and multi-stakeholder evaluation. BMC Medicine, 17,226. https://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-019-1447-x

[9] Moor, James H. "What is computer ethics?" Computer Ethics. Routledge, 2017. 31-40.

we suggest must be incorporated into any proposed regulatory framework. In doing so we explain that the potential risks associated with technical implementation, demands attention as much as the issues associated with the validity of vaccination passports as potential instruments of border mobility, and the broader epidemiological and medical issues.

Section II offers a brief analysis of four technical proposals, identifying some regulatory and policy issues, and concludes with a discussion of the EU Digital Covid Passport. Section III discusses the regulatory risks associated with three technology platforms involved in digital vaccine passports – blockchain, open source and data networks. Section IV concludes that the key regulatory issues lie in the positioning of the digital passport in an ocean of networks, connected data sources and interested parties, such that the application cannot be considered for regulatory purposes as a simply standalone artefact but is one node, located in a complex network, which may pose intractable regulatory problems.

II REGULATORY ISSUES IN FOUR TECHNICAL PROPOSALS

There are currently several vaccine passport technologies being developed, each of which has its own technical and ethical challenges. The rationale for examining the four below is because they were identified by the Ada Lovelace Centre expert examination of vaccine passports in society (ALI, 2021) as the leading technologies in this area.

1. Vaccination Credential Initiative (VCI)

VCI is an alliance of 12 technology and health service providers, including Microsoft, Oracle, The Mayo Clinic, and others,[10] which was expected to be available in May 2021.[11] The goal is to power open-licensed, secure, and decentralized solutions, through an Application Programming Interface (API) to ensure the solution is interoperable and broadly adopted across several platforms and stakeholders. The solution will facilitate sharing of verifiable clinical information such as COVID-19 laboratory results, immunization, and other relevant data in the form of a smart-health card or digital-health wallet. As such, it will require an interoperable ecosystem of applications, data and processes contributed to by a wide range of stakeholders. In an open environment where responsibilities and provenance for technical changes may be difficult to determine, any contributor could be liable for the regulatory consequences.

There will be three main actors: the issuer, the holder, and the verifier.[12] The verifier validates the records on the smartcard by checking whether it is valid and cryptographically signed. The digital-health wallet could be installed as a mobile app on smart devices, while the card could be issued as identity cards with QR-codes. The VCI alliance claims the solution satisfies the privacy issue because signed data resides only with the end-users, and they have the prerogative to only present the data for verification.[13] However, the commercial nature of this approach means that there may be greater complexities with verifying GDPR compliance, and regulators may feel forced to compromise

[10] Mahindra, A. *et al.* (2021) 'Paper card-based vs application-based vaccine credentials: a comparison', *arXiv preprint arXiv:2102.04512*.

[11] https://www.healthcareitnews.com/news/vci-member-orgs-plan-verifiable-covid-19-vaccine-credentials-next-month

[12] https://smarthealth.cards/

[13] Vaccination Credential 2021. *The VCI Charter*. [online] Available at: https://vaccinationcredential.org/about [Accessed 3 April 2021].

transparency for interoperability. Further, the number of involved organisations from different jurisdictions makes this option difficult to regulate.

2. COVID-19 Credentials Initiative

The COVID-19 Credentials Initiative (CCI) is 'an open global community looking to deploy and/or help deploy privacy-preserving verifiable credential projects to mitigate the spread of COVID-19'.[14] Supported by the Linux Foundation (a non-profit organisation), one of its main aims is to develop a set of privacy-preserving verifiable credentials (VCs) that will be used responsibly within other projects. This initiative advocates a data minimisation approach whereby a trusted credential issuer (e.g., government or health services) can provide a holder of the VC with proof that the VC has the specific characteristic required (e.g., vaccination status), without any need for there to be communication directly between the verifier and the issuer. As with the VCI initiative, this is much like holding a physical driver's licence or passport, but with privacy-preserving features such as data minimisation. The health data credential can reside with health providers like the NHS or trusted providers. Like the VCI initiative, the networked nature of the approach creates the potential for data protection issues that cannot be fully rectified by data minimisation.

3. IATA Travel Pass Initiative

Successfully trialled on Singapore Airlines in March 2021, the International Air Transport Association (IATA) Travel Pass is now set to be used by several airlines as a global solution to validate and authenticate law and policies regarding passenger travel requirements during COVID-19.[15] This technology is based on four independent open-sourced components that can interact with each other using blockchain technology, and can be combined for an end-to-end solution. These include 1) a registry of global health requirements that provides information on vaccine status, testing and travel requirements, 2) a registry of testing vaccination centres to identify labs and testing centres at departure location, 3) a lab app through which labs and test centres can send test results or vaccination certificates to passengers and 4) a digital passport module, which will enable passengers to create, verify and share their certificates.

However, as there is currently no global standardization in terms of the key elements of a digital certificate, this app and similar ones may have no capability to differentiate between fake certificates and even fake results. The travel pass communicates with different governments, airlines, test centres, vaccination providers and passengers. This means that it interacts with different data protection laws and regulations. This clearly creates concerns about compliance with GDPR and there is little to indicate that the registries will not be used for other purposes such as marketing.

4. IBM Digital Health Pass

IBM's response to COVID-19 is pitched around helping customers to get people back to work, back to physical spaces.[16] and looks to be adopted in Germany.[17] Underpinning the technology of the digital health pass is the IBM approach to blockchain.[18] IBMs digital pass includes three major

[14] COVID-19 Credentials Initiative (2021) *COVID-19 Credentials initiative: Home*. Available at: https://www.covidcreds.org/ (Accessed: 14 April 2021).

[15] https://www.iata.org/en/programs/passenger/travel-pass/

16 IBM (2021) IBM Digital Health Pass. Available at: https://www.ibm.com/products/digital-health-pass (Accessed 21 April 2021)

[17] https://www.ledgerinsights.com/ibm-consortium-wins-german-digital-health-passport-contract-ubirch/

18 IBM (2021) IBM blockchain. Available at: https://www.ibm.com/blockchain (Accessed 21 April 2021)

leading-edge technologies that are already combined in the online marketing material. Firstly, an application issuing credentials as used by approved issuers such as test centres or hospitals is included. A second application, the digital wallet, receives the validated credentials. This is embedded on the phone in a complex array of algorithms and encryption mechanisms. A third application, used by verifiers, processes and identifies challenges and responses, and significantly has access to keys and schemes from the blockchain distributed ledger.[19] IBM, as gatekeepers to the system and to their approach to blockchain means that there will be transparency and commercial interests to create regulatory barriers. IBM's offering confronts the regulatory challenges raised by both blockchain and open source.

The EU Digital Covid Certificate [20]

Agreed by the European Parliament on 21 May 2021, and due to be implemented on 01 July 2021, the renamed EU Digital Covid Certificate sets out to standardise and harmonise the vaccine passport approach across all EU member states (with a few exceptions) (9a, 25a). The aim is to re-enable the free movement of people during the period of the pandemic and intends to be rolled back after 12 months (42). From a techno-ethics perspective, the digital divide has a major impact on individual's access to services, and vaccine passports introduced without low-tech options could lead to further exclusion of already vulnerable groups.[21] By offering both paper and digital formats (14), the EU Digital Covid Certificate addresses this issue. There are strong GDPR, and personal data protections built into the regulation, and the document is further at pains to emphasise both the 12-month, time limit and the specifically Covid nature of the regulation (42). There is also a requirement that no central database will be maintained, which also prohibits the retention of personal data by Member States (40), a reassurance that may allay the fears of some regarding mission creep.

However, the framework will operate utilising a public key infrastructure (39), which as discussed below, creates regulatory concerns regarding GDPR and ownership/access/further processing of the data. The problems of regulation in a distributed system that utilises blockchain technology are in part because it is so complex, with many interlinked gateways and entry points. A key element of data protection for the individual is to be able to edit or add notes to records should they be incorrect. The use of the blockchain, by its trusted nature, cannot do this, and could result in people being refused entry at borders based on earlier records that they had been unable to delete or revise.

The EU Digital Covid Certificate approach includes a 'strong preference' for the use of open-source technology (15) which begs two questions, 1) who will be developing this technology, and 2) would a partial open-source disclosure be acceptable to have the systems up and running ahead of the 01 July 2021, deadline? The involvement of commercial interests, alongside a preference rather than a requirement for open-source technology could be potentially problematic for regulators in attributing liability should there be a data breach or other problems in the future.

III RISK-BEARING VACCINE PASSPORT TECHNOLOGIES

[19] IBM (2021) How IBM blockchain powers IBM Digital Health Pass. Available at: https://www.ibm.com/watson/health/resources/digital-health-pass-blockchain-explained/ (Accessed 21 April 2021)

[20]EU Digital COVID Certificate: European Parliament and Council reach agreement on Commission proposal (2021) Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2593 Accessed 27/05/21

[21] Osama T, Razai M S, Majeed A. Covid-19 vaccine passports: access, equity, and ethics BMJ 2021; 373: n861 doi:10.1136/bmj.n861

1. Blockchain

Several vaccine passports employ blockchain in their implementation. The technical foundation of the IBM Digital health pass is Hyperledger Fabric, an open source blockchain modular framework for building a distributed ledger. Fabric enables the building of a network of networks.[22] Data can remain private while sharing hashes as validation evidence. It uses a permissioned architecture which requires a centralised authority to define and operate the blockchain system, granting access according to the authorities' rules. While Hyperledger fabric has been developed by an open-source software community, IBM envisages its implementation as meeting the needs of the client owners, supported by IBM consultancy. IBM's digital health passport is already operating in the field with voluntary testing in New York State.[23] The use of blockchain as the engine of the European Digital Covid Certificate, the IBM Digital Health Pass and the IATA Travel Pass Initiative requires a focus on the ethics of blockchain as a transaction technology.[24]

Tensions arise, for example, between blockchain and the GDPR, depending on the use case and the type of blockchain. Opinion differs as to whether blockchain is an aid or a hindrance of the GDPR.[25] Blockchain is a distributed ledger technology which allows a network to validate a transaction and is based on a distrust of any centralised control.[26] It is trust-less by design, outside the control of centralised databases, platforms, or protocols.[27] The philosophy of the technology is essentially anti-regulatory. Blockchain has been compared to other technologies without central control such as M-PESA.[28] The effectiveness of M-PESA depended on it being kept out of the usual scope of financial regulation. A technology which promoted non-regulation poses significant problems when it is incorporated into health technologies which should be subjected to the rigor of regulation.

Blockchain technology is being used to support the implementation of self-sovereign identity in which the owner of the data chooses what data items to show, over which the owner has exclusive control, and which is stored locally. The concept, in its experimental phase,[29] may have consequences for laws of identity and hence the regulation of digital vaccine passports.

The use of blockchain raises puzzles concerning issues such as anonymity, erasure, and data control. As far as personal data are concerned however, hashing cannot be an anonymising technique, and therefore is not a solution to the data protection concerns (depending on the use case). Being an 'append only' system, the vaccine passport's immutability concept makes it difficult to exercise a data

[22] Hyperledger Fabric (2021) Hyperledger Fabric. Available at: https://www.ibm.com/downloads/cas/0XMOQJNP (Accessed 21 April 2021)

[23] IBM (2021g) New York and IBM begin COVID-19 Digital Health Pass Pilot. Available at: https://newsroom.ibm.com/New-York-State-and-IBM-Digital-Health-Pass-Pilot (Accessed 21 April 2021)

[24] Tang, Y., Xiong, J., Becerril-Arreola, R. and Iyer, L., 2019, June. Blockchain ethics research: a conceptual model. In Proceedings of the 2019 on Computers and People Research Conference (pp. 43-49).

[25] IBM (2018) blockchain and GDPR. Available at: https://iapp.org/media/pdf/resource_center/blockchain_and_gdpr.pdf (Accessed 21 April 2021)

[26] Gretch, A, Sood, I and Arino, L. (2021) Blockchain, Self-sovereign identity and digital credentials: Promise and praxis in education. Frontiers in Blockchain. https://www.frontiersin.org/articles/10.3389/fbloc.2021.616779/full

[27] Ibid.

[28] Ibid.

[29] Ferdous,S.M.K., Chowdhury, F. and Alassafi, M.O. (2019) In search of self-sovereign identity leveraging blockchain technology. IEEE Access https://ieeexplore.ieee.org/document/8776589

subject's right to rectification and erasure (GDPR articles 16 and 17). Even with the identification of a data controller or indeed joint data controllers. Being a decentralised system, it is impossible to delete or update records without tampering with the chain process. Even what constitutes erasure is not defined in the GDPR and has been opened to interpretation. It is important that data subjects' right to minimisation is enhanced by making sure that the protocol is designed in a way that each piece of data is accessed only by parties that need to and can be deleted or rectified upon request. Furthermore, as part of data subjects' right of access (GDPR article 15), individuals should be able to be informed when their data is being processed for automated decision making (GDPR article 22). One report recommended avoiding storing personal data on blockchain for this reason.[30]

The vaccine passport blockchain model is based on collective processing of personal data using a shared protocol, therefore identification of the data controller responsible for determining the purposes and means of processing under article 4(7) of the GDPR becomes difficult, particularly if blockchain transactions are written by the data subject.[31] Based on the interoperable nature of the vaccine passport model, one solution may be to adopt a joint controller approach where a consortium of entities is accountable for demonstrating compliance with GDPR.[32]

Privacy by design and by default raises another tension for vaccine passports. The development of technical, procedural, and organisational measures through the lifecycle of the processing is very important (GDPR article 35). One way to achieve this is by conducting a Data Protection Impact Assessment (DPIA).[33] This should be done as a default mechanism that aligns the process and outcomes of the blockchain technology to privacy and data protection. Currently, it is not clear what these measures are or how they will be achieved to comply with this requirement. Although a lawful basis for processing of vaccination details for the purposes of providing access to services or venues can be established under public interest (GDPR article 6(e)), being data concerning health, an individual's vaccination details fall under special category personal data (GDPR article 9), making it subject to special protection.[34,35]

2. Open source

Open-source software development has gained considerable traction in the software industry. Firms such as Microsoft and IBM which were previously resistant to open-source development have embraced the concept and deliver services using open-source software. IBM bases both its blockchain and quantum computing services on open-source. Specifically, the definition and programs for implementing a Hyperledger blockchain are readily available and non-proprietary, and open standards are applied in both the blockchain application and its security. The specifications for

[30] EU blockchain Observatory (2018) blockchain and the GDPR. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (Accessed 21 April 2021).

[31] Ibid.

[32] Van Geelkerken, F.W.J. and Konings, K., 2017, December. Using Blockchain to strengthen the rights granted through the GDPR. In INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 23–25 NOVEMBER 2017, LVIV, UKRAINE, (pp. 458-461).

[33] Bieker, F., Friedewald, M., Hansen, M., Obersteller, H. and Rost, M., 2016, September. A process for data protection impact assessment under the European general data protection regulation. In Annual Privacy Forum (pp. 21-37). Springer, Cham.

[34] Yuan, B. and Li, J., 2019. The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the European union: an empirical investigation. International journal of environmental research and public health, 16(6), p.1070.

[35] Marovic, B. and Curcin, V., 2020. Impact of the European General Data Protection Regulation (GDPR) on Health Data Management in a European Union Candidate Country: A Case Study of Serbia. JMIR medical informatics, 8(4), p.e 14604.

the IBM Digital Health Pass use cases are available on GitHub, as is some information on the EU Digital Covid Certificate. Further, the VCI consortium also offers access to the Smart Health Cards Protocol which takes an open-source approach.

IBM, in marketing the digital health pass, emphasise trust and transparency, citing the open-source nature of the technologies used. However, the argument that open-source is transparent is one that needs evaluation. Transparency is a complex concept. That the open-source nature of the blockchain development environment renders the specific blockchain implementation transparent, is a debateable point. Indeed, the complexity of blockchain renders it somewhat opaque. Furthermore, one needs to ask what any vaccine passport provider means by transparent, and whether the governance and execution of open-source development is any more open than a proprietary development by software houses, who may not be subject to regulatory frameworks.

Several of the proposed implementations depend on open-source development by third parties. While the EU has addressed open-source,[36] the focus has been primarily on intellectual property rights. The EU Source strategy[37] does not address responsibilities nor regulatory issues when the resulting software has significant legal, human rights and security implications. Accountability cannot be allocated. Although in many cases, while the platforms and requirements definitions are open source, the delivery of the service may be a commercial proposition through a company such as Red Hat (owned by IBM). It may be legally difficult to allocate blame. The problem lies with the inherent philosophy of open-source.

Open-source developed as an offshoot of the Free Software Foundation which promoted the sharing of software and changes to software. Open-source software is developed by decentralised and collaborative communities relying on peer review. This decentralised model has parallels in the development of the Internet and hence presents similar problems of regulation and control. Such projects are hosted on the GitHub software configuration database and cannot be managed or controlled by governments or companies. Hence companies enter the open-source ecosystem by contributing to existing communities to the benefit of the companies. Since the consequences of the GDPR for open-source and the conditions imposed on open-source are a matter of discussion and are yet to be tested,[38] it is likely the founding of vaccine passports on open-source will pose future regulatory headaches.

3. Data Networks

Vaccination passports will draw on a range of centralised and decentralised data sources to create a unique profile for everyone to represent their COVID-19 health status. As such that digital description may not be simply constrained to whether the individual has had a vaccination but may eventually relate to the whole health status of the individual, and which may come to bear on their calculated risk to themselves and others.

A vaccination passport system is not an isolated app on someone's mobile phone. Rather, it is a mass of connected systems, data and technologies. The marketing for the IBM Digital Health Pass references artificial intelligence (AI), the Internet of Things (IoT) and blockchain. The German implementation specifically partners IBM with a company whose focus is on IoT. Further integration as a border pass will involve connection with biometrics and technologies such as facial recognition

[36] EU (2020) Open Source software in the European Union. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Open_Source_software/2020_OSS_Full_EN.pdf

[37] EU (2020) Open Source Software Strategy 2020-2023

[38] https://www.termsfeed.com/blog/gdpr-open-source/

and data analytics which depend on AI algorithms. Digital health passports may well be integrated with IoT through Bluetooth beacons and wearable devices. The technology environment of vaccination passports is fluid and connected, which precludes the isolation of individual programmes or technologies for ethical consideration, resulting in further policy vacuums and regulatory gaps. A more systems-based approach, however, treats the vaccination passport as an IT ecosystem, and that the connections demanded by blockchain, alongside the connections required to validate the data on which the pass is based, constitute a network of networks.

IV CONCLUSION

Digital passports comprise a complex brew of technologies whose regulation is problematic. The technologies of blockchain and open-source systems and software are developed outside of traditional regulatory domains, which is antithetical to their founding philosophies. Further, artificial intelligence, used in the management of digital passports, and the potential for machine learning applications, introduces a domain where ethics and regulation are matters of debate and global concern. The regulatory epistemology[39] of digital vaccine passports poses a novel set of problems because of the variety of technology platforms and processes. Sources of expertise will be difficult to draw on and surface understanding of blockchain implementations, artificial intelligence algorithms and open-source specifications will not suffice. In an environment of authorities and actors, ranging from the EU, national governments and technology companies to individual programmers contributing to an open-source implementation documented on GitHub, there is a complex network and hierarchy of authorities and opinions. Furthermore, the malleability of purpose of vaccine passports, and the future potential for extending purposes across, between and within states may threaten the regulatory process and trigger a regulatory crisis.

Our discussion of the implementation of blockchain identifies the multiple data sources, authorities and actors involved in the digital vaccine process. The passport with its limited and defined dataset cannot operate without a distributed and extensive network of sources to support it. The authority is not encoded on the passport but rather with a population of institutions which maintain the blockchain and issues certificates. These authorities include the private companies running the tests, developing the blockchain applications, supporting the data sources through cloud offerings and interacting with one another. Thus, the passport floats in an ocean of data and connectivity which, when integrated, is open to hacking by individuals and states and can be corralled for a particular purpose by organisations occupying hubs within the network.

Blockchain is effectively a network of networks, supporting constant dynamic flows of information, vulnerable to intrusion at any point. Regulation of vaccine passports will be inadequate in managing the technological complexity and reach of the digital vaccine passport network of networks. The technical aspects are of equal if not greater significance than the health and border control issues being raised. As such, regulation of the network of networks will require a new regulatory and policy approach, which addresses the systemic and entangled nature of digital vaccine passport technology. We would suggest that approaches from complexity sciences which address the boundaries, networks, and hierarchies of the political, social, and technological

[39] Morvillo, M. (2020) Glyphosate effect: Has the glyphosate controversy affected the EU's regulatory epistemology? European Journal of Risk Regulation, 11(3) 422-435.

systems[40] be explored, to provide new approaches and models for the regulation of complex technological environments.[41]

The response to COVID-19 becomes a solution to any imagined scenario and a permanent strand of risk-reduction. The new normal irreversibly includes the monitoring of an individual's health, whether mediated through a vaccination passport, embedded in the work and travel environment, or embodied surgically. This irreversibility within the network of networks in the terms of Latour,[42] becomes a black box whereby vaccination passports and their development as a complex means of health monitoring, become taken-for-granted, and further proliferates the surveillance society. Within this environment, regulators and policymakers should consider the much wider context in which the setting and upholding of standards and oversight is made much more difficult, due to the leaky vessels that are sailing in the immense ocean that is the network of networks.

[40] McBride, N. (2015) The Application of an Extended Hierarchy Theory in Understanding Complex Organisational Situations. Systems Research and Behavioural Sciences, 33(3) 413-436.

[41] Minto, A. and Trincanato, E. (2021) The policy and regulatory engagement with corruption: Insights from complexity theory. European Journal of Risk Regulation First View, 1-24.
DOI: https://doi.org/10.1017/err.2021.18

[42] Latour, B. (1987) Science in Action. Open University Milton Keynes