BLOCKCHAIN POLICY SERIES

Opportunities and Challenges of Blockchain Technologies in Health Care

December 2020

Much hype surrounds the potential of blockchain technology in the health sector but few practical applications of the technology have been implemented in real-world health care settings. This policy brief supports health policy makers in their evaluation of blockchain solutions by explaining what is meant by blockchain technology, its advantages and limitations, emerging and potential uses in the health sector and policy considerations for its deployment.

Key Findings

- Blockchain is a relatively new technology for managing electronic data that has the potential to support transparency and accountability. A blockchain is a ledger of transactions where an identical copy of the ledger is visible to all the members of a computer network.

- Blockchain is best suited to transactions with a lightweight digital footprint where transparency and immutability are an advantage. In the health sector, blockchains may be particularly useful for identity verification; medical and pharmaceutical supply chain management; and managing dynamic patient consent and data sharing and access permissions.

- Blockchain-enabled tools are emerging to combat the COVID-19 pandemic, such as an identity management system in support of contact tracing in South Korea and a system to support sharing data and software code for research purposes. Blockchain has also been used or proposed for supply chain management for medications, medical supplies and for a future vaccine.

- Hype surrounds the potential of blockchain technology in the health sector and its usefulness can be overstated. Most published research on the use of blockchain in the health sector presents theoretical frameworks, architectures, or models with few technical details. There is seldom a prototype or pilot implementation to learn from. Deployment of blockchain technology in health at a national scale is rare.

- To meet information needs and policy goals, blockchain should be deployed where it is best suited and in combination with other technologies within a well-governed health information system.

- Importantly, Blockchain is ill-suited to storing high-volume data due to the computational and capacity constraints of replicating the blockchain across every network participant (node). Storing large records on the blockchain, such as full electronic medical records or genetic data records, would be inefficient and costly. It is also difficult to query data within a blockchain, limiting clinical, statistical and research uses of data.

- Further, storing personal health data ‘on chain’ and thus, by definition, visible to other network participants, is a data privacy infringement. Rights under the *EU General Data Protection Regulation*, particularly the right to erasure, are incompatible with the immutability of blocks in a chain.

- To leverage the strengths of blockchain and avoid pitfalls, potential blockchain applications should be assessed within the framework provided by the Recommendation of the OECD Council on Health Data Governance and focus on four key aspects: fitness of the technology for the use to which it will be applied; alignment with laws and regulations; incremental adoption to allow time for evaluation; and a training and communications plan.

Introduction

Blockchain is a technology designed to manage electronic data that has the potential to support transparency and accountability. A blockchain is a ledger of transactions where an identical copy is visible to all the members of a computer network. Network members validate the data entered into the ledger; and once entered, the data are immutable (OECD, 2020). Blockchain was originally developed for cryptocurrencies to eliminate the need for intermediaries, such as banks, while protecting against a high risk of fraud and theft.

In the health sector, there are transactions where transparent and immutable record keeping may also be important, such as purchasing and shipping transactions in supply chains for medical equipment and pharmaceuticals; and tracking permissions and access of personnel to facilities, medical records or other health data. Questions for policy makers include, to what degree is blockchain necessary to preserve the integrity of these transactions? Do its costs and benefits compare favourably against alternative technologies, such as a traditional, centrally-managed, database?

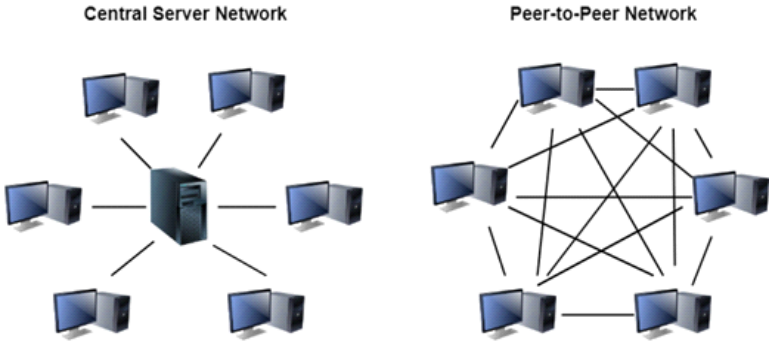
While well-established systems for assessing pharmaceutical innovations exist, there is no equivalent for other types of innovations, including digital solutions. Often there is asymmetry of information between software vendors and purchasers that can place health systems at a disadvantage. This is particularly problematic for blockchain-enabled solutions, because there are few practical applications of the technology in real-world health care settings to learn from.

This policy brief aims to support health policy makers in evaluating blockchain solutions by explaining (1) what is meant by blockchain technology, and its advantages and limitations and (2) emerging and potential uses in the health sector and the policy considerations in deploying it.

Blockchain is a major change from traditional approaches to data management

In a traditional database, the data are held in a single, central server (or server network) with a centralised database administrator. In contrast, blockchain is an approach to managing data where they are appended on an electronic ledger that is distributed across a peer-to-peer network with no central administration of the data (Figure 1).

Figure 1. Centralised versus a distributed, peer-to-peer network



Source: Source: HIMSS Blockchain Networks Overview (HIMSS, 2019)

Box 1. Blockchain is a family of technologies with different features and costs

There is no single 'blockchain' just as there is no single database. Rather, there is a range of different ways to deploy the blockchain concept, with different features and operating costs.

Most blockchains have an 'append only' structure. This means that the blockchain allows new data to be entered but, once a block has been added, it cannot be edited or deleted by any of the participants. This 'append only' structure ensures the consistency and validity of each participant's copy of the blockchain, and allows participants to validate each new block appended to the chain.

Each time a user enters a block into the chain they must record information about the transaction into a cryptographic hashing algorithm that produces a code (a set of letters and numbers) that is distinct to that transaction (OECD, 2020). If any part of the data block were later changed, then the hashing algorithm would produce a different code that would be incompatible with the rest of the codes in that blockchain and would alert members of the network to a potential case of data tampering. The degree of difficulty in tampering with blocks rises with the number of participants in a blockchain network because a successful attack would require hacking into many copies of the distributed ledger to change them all simultaneously (Miles, 2017).

Public blockchains for cryptocurrencies, where anyone can join the network and participate in it anonymously, are known for high operating costs and energy consumption. For example, a single bitcoin transaction is estimated to use 718.53 kWh of energy, which is as much energy as an average US household uses in 24 days (Digiconomist, 2020). A reason for the high cost is that public blockchains use 'mining' to validate new blocks of data to be entered into the ledger. Miners are network nodes that compete to validate blocks and are rewarded financially for doing so. For a cryptocurrency, they are checking a new block against past blocks to ensure that a bitcoin sender isn't trying to spend the same funds twice. Results of the mining allow the network to reach a consensus to publish the block to the chain. The average bitcoin transaction involves several confirmations from miners that the block can be published and can take from 10 minutes to a day or more to complete (Tuwiner, 2020). This approach to reaching consensus to add blocks is also called 'Proof of Work'.

Private blockchains, where nodes entering blocks are authorised and known to one another, may not need to rely on 'Proof of Work' methods to validate the data. For example, a private network of authorised users of a health authority's blockchain could agree to use other consensus rules to validate the data and resolve any discrepancies or conflicts, such as 'Proof of Authority' which assigns validation responsibilities to certain network nodes or 'Byzantine Fault Tolerance' which is where a block is published after a sufficient number of nodes vote to do so, even if some fail to vote (EY, 2019).

In a blockchain, data such as a sales transaction record or a medical record are stored in blocks. When the data to complete a block have been entered, the block is added to the chain of previous blocks and a new block is created for the next data entry. Blockchains are decentralised and can have an unlimited number of participants in a network, such as a global network of vendors and purchasers of medical equipment. All participants in a blockchain have a full copy of the blockchain, which is continually updated and synchronised as new blocks are added. A node is a computer/device that stores or provides access to a copy of the blockchain. All the records in a blockchain are visible to all the participants in the blockchain network.

While all blockchains have these features, there are many ways to deploy them. Blockchains may be public and open to anyone to participate anonymously, such as a cryptocurrency blockchain, or the they may be private, where network members uploading blocks of data are authorised to do so and known to the members of the network (Box 1).

Blockchain fits situations where transparency and immutability of the data are needed

Blockchain is best suited to recording transactions with a lightweight digital footprint where transparency and immutability are an advantage. In other words, it is best suited to situations where there is less trust among participants in a network and where the size of data blocks is relatively small. Situations in health care where blockchain may be particularly useful include identity verification of patients, providers or suppliers; supply chain management; and management of dynamic patient consent to data uses.

Blockchain is, however, ill-suited to storing high-volume data due to the computational and capacity constraints of replicating the blockchain across every network participant (node). Storing large records on the blockchain, such as full electronic medical records or genetic data records, would be inefficient and costly.

Personal health data are sensitive and subject to legislations protecting data privacy in OECD countries. Storing them 'on chain' and thus, by definition, visible to all other network participants would be a high risk to data privacy, even if records were de-identified.[1] Even storing metadata about personal health data (data about data) on chain, while technically feasible, raises data privacy concerns because of the potential for indirectly disclosing patient identities and because the data cannot be erased. (Panel for the Future of Science and Technology, 2019).

The visibility of the data in a blockchain risks contravening data privacy principles of data minimisation and use limitation (OECD, 2013). Compliance may be addressed if the blockchain is private and permissioned, which is where all the blockchain network nodes are known to one another and nodes must be authorised to view and add to the blockchain. Further, some network nodes may be approved access to only a portion of the ledger.

The distributed ledger makes it difficult for data subjects, such as patients or providers, to exercise rights that are related to the behaviour of the data controller because there is no single data controller, such as one organisation that is the custodian of the data, but rather network nodes that each hold a copy of the data. In the *EU Data Protection Regulation*, rights related to the behaviour of a data controller include the right to access your personal data, to correct them, to be informed about the processing of them, to object to processing of them and to have them erased. Further, the 'append only' aspect of blockchain that is the inability to change or erase data from the chain, is incompatible with the *EU Data Protection Regulation* right to erasure (Panel for the Future of Science and Technology, 2019) and has the potential to conflict with privacy legislations in other jurisdictions.

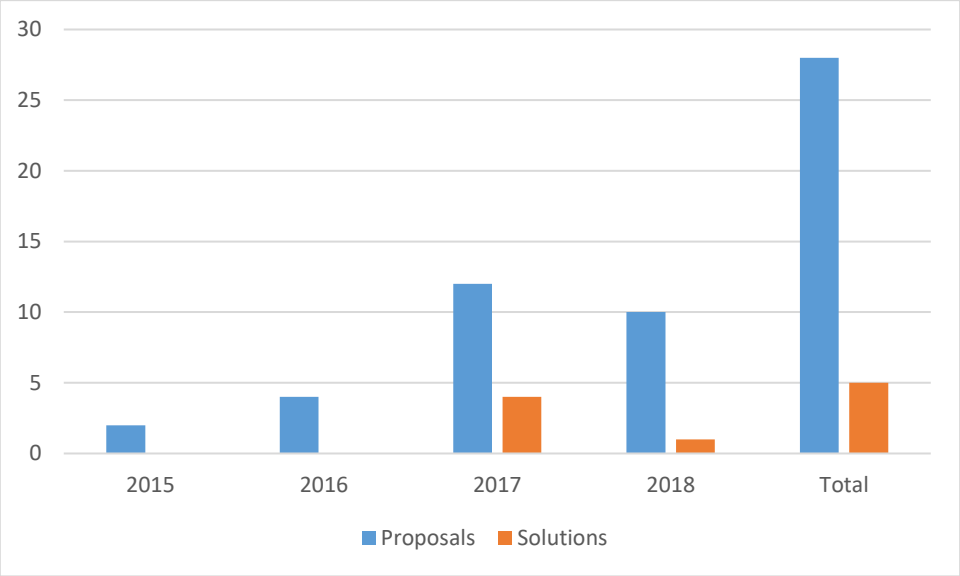
A related limitation is that, unlike conventional databases, distributed ledgers are difficult to search for specific terms or information. This limits their utility as information repositories for clinical as well as research purposes. User interfaces are still quite rudimentary and in the early phases of development (Vazirani, 2019) and this limits deploying blockchain-enabled ledgers at scale. Given that blockchain is a nascent technology, technological fixes may still emerge as the technology begins to be applied more regularly and across a range of sectors.

[1] As electronic health records can be very detailed, re-identification attacks can be successful.

Blockchain applications in the health sector are limited

Despite some growth in published research on the uses of blockchain in the health sector, the state of play is still immature. Most research presents novel blockchain frameworks, architectures or models but technical details about the blockchain elements used are rarely provided and there is seldom any prototype or pilot implementation to learn from (Figure 2). Deployment of blockchain technology in health at a national scale is rare. There are examples from some countries, such as Estonia and Malta, of how blockchain technologies offer useful features such as data security protection and management of patient consent. The most promising applications of blockchain in the health care sector are for identity management, dynamic patient consent, and management of supply chains for medical supplies and pharmaceuticals, as discussed below.

Figure 2. Most research papers on blockchain in health care describe proposals, not solutions



Source: Hölbl M et al., 2018

Blockchain for identity management in health care

Accurate and verifiable identification of individuals (e.g. patients and providers) as well as organisations (e.g., hospitals, pharmacies, academia and other research institutions) is fundamental to good outcomes in the health sector. A blockchain can add integrity and transparency and combat differential versioning of identities, thus enabling secure identification. This will become increasingly important as more data begin to flow from wearable medical devices and the Internet of Things (IoT) so that these data are, for example, matched accurately with individuals' electronic medical records.

Health care providers – both individual and organisational – must provide accurate and up-to-date information on their location and service availability to enable, for example, patients to locate them; accrediting agencies identify them; and payers to reimburse them accurately. A blockchain may improve the veracity and accuracy of the relevant information.

A blockchain can create an immutable log of each time a data record is accessed or amended. Estonia utilises an application of blockchain technology called KSI to protect government data, including electronic health records, from external cyber-attacks and from internal misuse. The KSI technology provides security without violating data privacy (e-Estonia, 2020). Any amendment to a record can be crosschecked with

separate electronic logs. Suspicious access can be verified quickly, and potentially malicious, systemic action prevented. Like CCTV in high crime-risk locations, the blockchain doesn't intervene when a transgression occurs. Rather, the visibility (transparency) and inability to interrupt or amend the signal of the recording (immutability) is a deterrent.

Notably, the transactional footprint of these instructions, which contains only a catalogue of health records and metadata, is tiny compared to the actual health information that are stored off-chain (Vazirani, 2019). This highlights how, as with most digital innovations, blockchain is most useful when it is applied in combination with other technologies within a health information system.

Box 2. Blockchain for identity verification in a contact tracing app

Jeju Island, a tourist destination in South Korea, announced they are deploying a blockchain-enabled solution to support contact tracing visitors to the island who test positive for SARS-CoV2. Visitors to the island will be required to download a smartphone app and use it to scan the QR codes of businesses and services they access while on the island. When users first download the app, their identity is confirmed via a public blockchain that issues a certificate. A digital fingerprint authentication and PIN code is then set up by the app user on their smart phone and a certificate for those credentials is recorded within a private blockchain. Both certificates are stored on the app user's phone. App user's personal identifying information is stored separately from the record of businesses and services they have used. The app user's data will remain private unless they are required for contact tracing a case of COVID-19.

Source: Blockchain News, 2020

Blockchain for management of patient consent and data access permissions

Blockchain can enable a transparent, auditable way for individuals, using their unique credentials and encryption key, to allow other parties to access their personal health data. This includes granting authority for health professionals, service providers and other relevant actors (e.g. researchers and social care providers) to access their medical records and other information for the purposes of direct health care delivery or to permit research, statistical or other secondary uses of their data.

Given that electronic data can be used and re-used ad infinitum, and new research questions and purposes for data use continually emerge, the incremental or 'dynamic' consent enabled by blockchain provides a highly useful alternative to 'blanket or one-time-only' consent models. If an individual decides to change their terms of permission or consent, the changes can be added as a new block that overrides the previous instructions on the chain.

The Malta biobank is using a blockchain technology called Dwarna to manage dynamic consent of individuals to the usage of their bio specimens in research studies (Mamo N, 2019). The Dwarna web portal stores individuals' consent in a blockchain to create a permanent/immutable record. It increases trust in donating samples to the biobank by allowing individuals to have control over which studies they will participate in and allowing them to withdraw consent and to request that bio specimens be destroyed.

MedRec is a blockchain-enabled system from the Massachusetts Institute of Technology's media lab that associates a medical record with viewing permissions and data retrieval instructions for external databases (MedRec, 2020). It uses blockchain 'smart contracts' to record patient-provider interactions. Once a

provider creates a record, it is verified, and the patient authorizes its viewing permissions. The party receiving new information receives an automated notification, and an encrypted pointer to the new medical record. Permissions are stored on the chain. This system allows patients to access and control their data. So far, it has been successful with medications, blood tests, vaccination histories, and other therapeutic interventions.

A trustworthy record of data ownership is the goal of RadBit, which allows patients to keep possession of their medical images along with an immutable chain of custody (Nichol, 2017). Temporary keys ("tokens") can be created by users of the blockchain and passed on to health care providers and insurance companies, providing them temporary access. The token is independent of the data, containing only authorization commands, and is verified and validated by adding them to the chain, triggering the dispatch of required reports. Potential ways to improve the integrity are to use blind signatures, which reinforce protection from tampering as well as confirming the sender's and viewer's identities, or to use signatures from multiple authorities.

Blockchain technologies for patient consent and permissions for data sharing and access are being deployed to improve recruitment and retention as well as patient and participant empowerment in biomedical research (Dubovitskaya A, 2019). Two notable blockchain-backed efforts in the pharmaceutical ecosystem are the Innovative Medicines Initiative (IMI) Blockchain Enabled Healthcare (IMI 2018) Project and the Pharmaceutical Users Software Exchange (PhUSE) Blockchain Project.

Blockchains could be used as a secure way to control the flow of personal data in the recruitment of participants to clinical trials (Angeletti F, 2017). A blockchain may protect the interests of both the individual, who can keep their data private until an agreement is reached, and the research team, which can trust that it is acquiring useful and authentic data.

A new blockchain application called Research Foundry has emerged to enable management of consent and permissions for the sharing of and access to health data, metadata, software code and other products connected with health research, including research related to the COVID-19 pandemic (Burstiq, 2020). It aims to facilitate cross-border collaboration in a way that ensures participants remain in compliance with applicable data privacy law. In this solution, network nodes control what data they wish to make visible to other participants. For example, metadata about a data repository may be shared with all participants while the health data repository remains private and not visible to the nodes on the blockchain. When there is an agreement to share all or part of a repository with other specific nodes then the sharing can be facilitated. The technology provider cannot access the private data repository without the explicit permission of the data owner.

Blockchain for managing medical and pharmaceutical supply chains

The most common use of blockchain across industries is for managing product supply chains. In the health sector, block chains are beginning to be used to manage supply chains for medications, clinical supplies, blood products, and medical devices.

Applications of blockchain in this sphere include the following (Clauson KA, 2018).

- Product identification: a unique product identifier may be validated more easily and quickly (e.g. in case of product failure).
- Tracing: manufacturers, distributors or dispensers can use a distributed ledger that automatically verifies relevant information.
- Product verification: verifies the authenticity of a product and enables public and private actors to detect products suspected as counterfeit, unapproved, or dangerous.
- Notification and response: enable a secure system to notify regulatory authorities of non-compliant products or transactions.

- Other relevant product and transaction information, such as licensing.

For example, health care systems are challenged to acquire medical equipment and supplies to combat COVID-19 due to high demand. Trust issues arise from the breakdown of supply chains with known vendors. Concerns about new vendors include compliance with standards, customs certification, timeliness of delivery of goods and fraud. These trust issues are further amplified by requirements of suppliers for up-front payment. Blockchain is a possible technology to assure the credibility of suppliers and to track shipments (Degnarain, 2020). In April 2020, IBM announced a blockchain enabled network - IBM Rapid Supplier Connect – to connect governments and health care organisations with non-traditional suppliers of equipment, devices and supplies to combat COVID-19 (IBM, 2020).

Trust issues exist in pharmaceutical supply chains. They include concerns about protection of intellectual property, quality control, counterfeiting and illicit drug sales (Mettler, 2016). With immutability of records, the blockchain may be an effective technology to verify the authenticity of suppliers and purchasers (MediLedger, 2020). For example, in the Hyperledger's Counterfeit Medicines Project, products are timestamped and entered on a blockchain for tracking and verification (Taylor, 2016). Ensuring adequate supply and avoiding shortages of drugs is another emerging problem area that can benefit from the transparency and immutability brought by blockchain technology. In China, hospitals have deployed blockchain to ensure accurate tracking and timely delivery of medications to Covid-19 patients' homes (Ting DSW, 2020).

Similar risks exist for medical device supply chains. These can range from safety and effectiveness issues, to high-risk devices with a history of security vulnerabilities (Goodin, 2017). Once agreed standards and protocols are in place, a blockchain could add security, transparency and authenticity to these efforts.

The need to manage the availability of staff, hospital beds, ICU beds and life-saving equipment across multiple hospitals and health authorities is high during the Covid-19 pandemic. Where there are trust issues or limited information sharing capabilities, blockchain may be a useful solution.

Box 3. Blockchain may be the right technology to manage COVID-19 vaccine distribution

An equitable distribution of a COVID-19 vaccine would require a global consensus on its distribution and a supply management system that is transparent, verifiable and timely. Blockchain may be a suitable technology for such a difficult task, allowing all countries and participating organisations to be nodes in a network that can view the records that would be immutable and updated in real time (Shukla P, 2020). The system could track key factors such as production, distribution and stock of vaccine and related supplies (needles, glass vials, refrigeration units) within and across countries; and track the quality of the vaccine, such as batch number, producer, expiry date and temperature control. Further, the system should support measuring loss and waste, so that they can be minimised.

Source: Shukla P, 2020

Policy considerations for deploying blockchain

Theoretical and practical use cases suggest that blockchain may add value to the digital transformation of health systems, particularly in the areas of identity verification, patient consent and data sharing and access permissions, and medical and pharmaceutical supply chain management. However, to achieve

policy goals it should be deployed in combination with other technologies and a robust health information system and data infrastructure which, working together, provide the optimal solution to meet health information needs.

Hype surrounds the potential of blockchain technology in the health sector and its usefulness can be overstated. Blockchain doesn't remove the most challenging obstacles to the digital transformation of the health sector, such as a lack of data interoperability, and it doesn't replace the need for health data governance.

While blockchains do not need a central authority to hold data, they do not remove the need for any authority at all. Given the nature of the health sector and that its data are often personal and sensitive, blockchain applications will rely on regulation and oversight as well as standards and protocols. The consensus system for governing any blockchain is not based on technology but requires an agreement among participants.

With multiple actors and participants, a trusted body to make the rules (or, more accurately, the 'rules that set the rules') will always be needed. This can be the government, or an established agency or institution. For example, Standards Australia led the development of a road map of priorities to help establish common terminology for blockchain-enabled technologies (Standards Australia, 2017).

The cost of development and implementation of technologies is a key consideration for policy makers. Evidence from Estonia, where blockchain technology has been deployed in the national health system, suggests that the direct costs in terms of technical development and implementation are modest. Once the core architecture is developed, additional applications may be added at a lower cost. As with any technological transition, most costs are incurred to change processes, workflows and behaviours to ensure that the technology will be used as envisaged. Of course, operational costs will depend on the efficiency of the blockchain design and minimisation of the volume of data stored 'on chain'.

Blockchain represents a significant departure from the traditional notion of data management and storage and stakeholder communication is very important for the successful deployment of the technology. Training and education of the health workforce would be needed to ensure its effective and efficient use. When the technology is deployed to enable patients to have greater control over and access to their data, successful implementation will rely on public consultation and information to educate patients on how to access the technology and their rights and responsibilities.

The immutability of blockchains can be a doubled-edged sword. As it stands, the metadata stored on a blockchain that pertains to an individual's health record cannot be erased. While information stored off-chain can be deleted, the record that the information previously existed cannot be removed from the chain. This information can be potentially sensitive and a legal question arises whether the metadata counts as personal health data (Panel for the Future of Science and Technology, 2019). The field is rapidly evolving and technological solutions to address this problem may be found, such as masking blocks associated with a specified signature.

While blockchain-based ledgers are inherently secure and tamper-proof in terms of the data they contain, this does not ensure that the data entered are correct or of sufficient quality. In addition to user error, there is also potential for malicious actors to influence individuals' decision-making regarding consent and permissions to use their data. This risk is particularly important within ageing populations with growing numbers of people who are physically and cognitively vulnerable. Blockchain cannot manage this risk; only governance, regulation and enforcement can.

Given its central role in helping to manage health data (including sensitive, personal health data), an assessment of the use of blockchain in the sector is best approached within the framework provided by the Recommendation of the OECD Council on Health Data Governance (OECD, 2019). This concerns not only the mechanisms concerning privacy, security and consent but also those dealing with communication, engagement, education and the fostering of trust among stakeholders.

Four principles should assist policy makers with implementing blockchain technology in health.

1. Fit-for-purpose. Blockchain is an enabling, general-purpose digital technology. It should be evaluated on its merits and applied where it is the best application for the problem at hand, after comparing it to alternative solutions.
2. Governance and regulatory alignment. Blockchain-based solutions have particular features that must be evaluated in terms of the compliance of the solution with laws, regulations and data governance frameworks.
3. Incremental integration. Blockchain-enabled solutions should be considered in relation to existing systems and technologies. Blockchain should complement and leverage existing systems and be tested incrementally in a controlled environment before large-scale implementation.
4. Education, awareness and user-based design. Blockchain requires a new way of thinking about data and information. Users of this technology, including patients and the public, must be educated regarding the features of this technology and the implications of its use for data ownership, access and privacy.

References

Angeletti F, C. I. (2017). The Role of Blockchain and IoT in Recruiting Participants for Digital Clinical Trials 2017 , Split, 2017, pp. 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-5.

Burstiq. (2020, 04 06). Introducing Research Foundry. Retrieved from Burstiq: https://www.burstiq.com/

Clauson KA, B. E. (2018, 03 23). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare. Blockchain in Healthcare Today, 1. Retrieved from https://doi.org/10.30953/bhty.v1.20

Degnarain, N. (2020, 03 22). Five Ways Blockchain Can Unblock The Coronavirus Medical Supply Chain. Forbes. Retrieved from https://www.forbes.com/sites/nishandegnarain/2020/03/22/5-ways-blockchain-can-unblock-the-coronavirus-medical-supply-chain/#25d72dd11380

Digiconomist. (2020, 04 06). Bitcoin Energy Consumption Index. Retrieved from https://digiconomist.net/bitcoin-energy-consumption

Dubovitskaya A, N. P. (2019). Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review. Oncology. Retrieved from https://www.karger.com/Article/Pdf/504325

Goodin, D. (2017, 08 30). 465k Patients Told to Visit Doctor to Patch Critical Pacemaker Vulnerability. Arstechnica. Retrieved from https://arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks/

HIMSS. (2019, 01 28). Blockchain Networks Overview. Retrieved from https://www.himss.org/library/blockchain-networks

Hölbl M, K. M. (2018). A Systematic Review of the Use of Blockchain in Healthcare. Symmetry. 10. 470. . Symmetry, 10(10), 470. doi:10.3390/sym10100470

Mamo N, M. G. (2019). Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Human Genetics. Retrieved from https://doi.org/10.1038/s41431-019-0560-9

MediLedger. (2020, 04 06). The MediLedger Network. Retrieved from https://www.mediledger.com/

MedRec. (2020, 04 06). What is MedRec? Retrieved from MedRec: https://medrec.media.mit.edu/

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3. Retrieved from https://doi.org/10.1109/HealthCom.2016.7749510

Nichol, P. (2017, 01 27). Top 3 Practical Innovations from Medical Hackathon. CIO. Retrieved from https://www.cio.com/article/3161886/top-3-practical-innovations-from-yale-healthcare-hackathon.html

OECD. (2019). Recommendation of the Council on Health Data Governance. OECD/LEGAL/0433, Paris. Retrieved from https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

Panel for the Future of Science and Technology. (2019). Blockchain and the General Data Protection Regulation. PE 634.445. Brussels: European Parliament Research Service. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Standards Australia. (2017). Roadmap for Blockchain Standards. Retrieved from https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

Taylor, P. (2016, 04 27). Applying Blockchain Technology to Medical Traceability. Securing Industry. Retrieved from Taylor (2016) https://www.securingindustry.com/pharmaceuticals/applying-blockchain-technology-to-medicine-traceability/s40/a2766/#.V5mxL_mLTIV

Ting DSW, C. L. (2020). Digital technology and COVID-19. Nature Medicine. Retrieved from https://doi.org/10.1038/s41591-020-0824-5

Vazirani AA, O. O. (2019, 02 12). Implementing Blockchains for Efficient Health Care: Systematic Review. Journal of Medical Internet Research, 21(2). Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/30747714

Acknowledgements

This report was prepared by Jillian Oderkirk and Luke Slawomirski of the OECD Health Division as part of the 2019-20 Programme of Work of the OECD Health Committee which supports countries in strengthening health data and their governance. For more information see www.oecd.org/health/health-systems/health-data-governance.

Members of the OECD Health Committee provided input and guidance. Stefano Scarpetta, Mark Pearson and Francesca Colombo provided advice and feedback. Pamela Duffin provided editorial and communications support.

This report contributes to the work of the OECD Blockchain Policy Centre which provides a global reference point for helping policy makers to address the challenges raised by blockchain and DLT and to seize the opportunities it offers for achieving policy objectives. For more information see www.oecd.org/daf/blockchain. http://www.oecd.org/daf/blockchain/. It also contributes to the OECD Going Digital Project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information see www.oecd.org/going-digital.