SPECIAL ARTICLE

ANZJSurg.com

Part 2: Blockchain technology in health care

Lorwai Tan,* David Tivey,*† Helena Kopunic,* Wendy Babidge,*† Sally Langley‡ and Guy Maddern*†

*Research, Audit and Academic Surgery, Royal Australasian College of Surgeons, Adelaide, South Australia, Australia
†Discipline of Surgery, The Queen Elizabeth Hospital, The University of Adelaide, Adelaide, South Australia, Australia and
‡Plastic and Reconstructive Surgery Department, Christchurch Hospital, Christchurch, New Zealand

Key words
blockchain, computer security, electronic health records.

Correspondence
Dr Lorwai Tan, Research, Audit and Academic Surgery, Royal Australasian College of Surgeons, 199 Ward Street, North Adelaide, Adelaide, SA 5006, Australia. Email: lorwai.tan@surgeons.org

L. Tan BSc (Hons), PhD; **D. Tivey** BSc (Hons), PhD; **H. Kopunic** MRes, PhD; **W. Babidge** BApp Sci (Hons), PhD; **S. Langley** MBChB, FRACS; **G. Maddern** PhD, FRACS.

Accepted for publication 31 October 2020.

doi: 10.1111/ans.16455

Abstract

Blockchain technology is one of the many disruptive technologies of the Fourth Industrial Revolution that will irrevocably change the way we live and work. These technologies are well embedded in the areas of global finance, health care and defence, to name a few. This review focuses on the relevance of blockchain technology to health care. Blockchain technology will be the unifying platform for sharing patient data currently inaccessible due to the siloed architecture of legacy software systems, and as a result potentially be the basis for precision or individualized patient treatment. It will also strengthen digital security of sensitive patient data that is presently a lucrative target for cyber criminals. In the current COVID-19 environment, clinicians will rely more on telehealth to reduce person-to-person contact. This service can be delivered by the clinical team with confidence in the veracity of the patient data made accessible through the blockchain platform. Smart contracts written on the blockchain platform will reduce the possibility of international humanitarian aid to low- and middle-income countries being misspent. The pharmaceutical supply chain industry is adopting blockchain technology to ensure supply chain provenance. Similarly, the health insurance industry recognizes how the blockchain ecosystem can improve services to its members and expedite reimbursements to clinicians.

Blockchain technology

Background

Distributed ledger technology allows data to be recorded, shared and synchronized across an unlimited number of digital ledgers hosted on networks distributed around the globe.[1] The blockchain shares similar features with distributed ledger technology; however, its point of difference is that blockchain technology uses cryptographic and algorithmic methods to record, share and synchronize data across networks. As a decentralized network, the blockchain reduces the dependence on a single, central administrator that is vulnerable to becoming a point of failure.[1]

Although considered a nascent technology, the IBM Institute for Business Value analysis identified financial services, insurance and health care as industries actively considering or are already engaged with blockchains.[2] Examples of its applications in the fintech space extend into areas such as cross-border payments to reduce costs and improve transaction times[3] and settlement of shares by stock exchanges such as the Australian Stock Exchange that previously used the Clearing House Electronic Sub-register System.[4] In other arenas, the United States Department of Defence reported that sovereign nations in the super power league have also been investing heavily into programs that explore the utility of digital technology in weapons logistics, tactics and strategy.[5]

In 2008, Bitcoin, a cryptocurrency, was introduced as a peer-to-peer payment system built on the blockchain platform.[6] Specifically, a blockchain is a digital record or ledger of transactions where individual records, called blocks, are linked together in a single list, called a chain. Each transaction added to a blockchain is validated by multiple computers called miners which when interconnected through the internet are referred to as nodes. Nodes form a peer-to-peer network and are configured to monitor specific types of blockchain transactions. They work together to ensure each transaction is valid before it is added to the blockchain. Bitcoin's inventor who went by the pseudonym Satoshi Nakamoto devised the proof of work (PoW) validation mechanism that involves solving a challenging mathematical puzzle whereby the miner who is first to solve the puzzle is awarded a number of Bitcoins.[6] This highly lucrative PoW system encourages miners to invest in computer application-specific integrated circuits chips built solely to solve the puzzle. However, with the increased computational speed comes higher electricity consumption and excessive heat generation. Consequently, large mining facilities are located in countries such as Iceland where electricity costs and ambient temperatures are low.

This decentralized network of computers ensures no one single computer can add invalid blocks to the chain. When a new block is added to a blockchain, it is linked to the previous block using a cryptographic hash generated from the contents of the previous block. This guarantees that the chain is never broken and that each block is immutable and permanently recorded. It is also intentionally difficult to alter past transactions in a blockchain as all the subsequent blocks must be altered first.[7] *Hashing* is defined as taking an arbitrary amount of input data (e.g. a single character, patient medical records, academic qualifications and a spreadsheet of your banking history) applying an algorithm (computer program) to it and generating unique and irreversible output data consisting of a fixed length alphanumeric code called the hash.

In addition to Bitcoin, Ethereum and XRP (Ripple) which operate on their own respective blockchains comprise the top three listed cryptocurrencies on Coinmarket Cap (https://coinmarketcap.com/). Together with Bitcoin, they represent a collective market capitalization of USD310 billion of the total USD400 billion market cap.

Blockchains such as Ethereum have adopted proof of stake as their validation mechanism as a means of reducing electricity costs required to operate the nodes. The Ethereum blockchain has become the preferred platform for developers to build and host decentralized applications (dApps) and for the execution of smart contracts. *Smart contracts* are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed and decentralized blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system or external enforcement mechanism. They render transactions traceable, transparent and irreversible.

The blockchain architecture exists primarily in three forms depending on access and whether permission is required; they are:

(1) *Public or open blockchain*: This type of blockchain is permissionless, that is, any member of the public with the appropriate computer hardware can download the complete copy of the ledger and participate by becoming a node in verifying transactions. In return, the individual receives a fraction of the cryptocurrency or token that powers all transactions on this blockchain.

(2) *Consortium/enterprise blockchain*: Commonly used by commercial entities, consortium/enterprise blockchains such as Hyperledger Fabric and Quorum are considered 'semi-private'. Permission to access the blockchain is granted to member companies with common business interests. Taking the approach of blockchain as a service, major financial institutions such as Goldman Sachs and software giants IBM and Microsoft are actively developing use cases with real-world applications such as frictionless cross-border remittances, foreign exchange transactions, global supply chain management and logistics, and offering cloud-based blockchain platforms for dApp developers to build new business-friendly products.[8–11]

(3) *Private blockchain*: A private blockchain is maintained exclusively by one organization. Although it is the most efficient, the immutability of this type of blockchain can be at risk of tampering by bad actors from within the organization as this is a centralized ecosystem.

Blockchain technology applications in health care

The healthcare sector has been quick to explore how blockchain technology can further increase efficiencies in areas such as the sharing of electronic medical records between hospitals, pharmaceutical supply chain tracing and logistics and health insurance claim processing.[12,13]

The Republic of Estonia can rightly claim to be an early adopter of blockchain technology when in 2016 the Estonian Government partnered with Guardtime, a commercial technology company to store the health records of its 1.3 million citizens on the blockchain.[14,15] The aim was to increase operational efficiencies between different health authorities and to reduce the costs of medical care. Storage of medical data on the blockchain would assist health insurers with data auditing and better coordinating insurance claim processes.

The COVID-19 pandemic has brought renewed interest in utilizing telehealth services to reduce community disease spread. Celesti *et al.*[16] discussed how medical devices connected through the Internet of things could be used to upload and store a patient's validated clinical and pathology test results on a permissioned blockchain platform. These diagnostic test results would then be accessed remotely by a virtual health team of clinicians who had complete confidence in the veracity of the data when making a diagnosis or formulating a patient management plan.

Interoperability

The utility of large data sets such as the American College of Surgeons National Surgical Quality Improvement Program Surgical Risk Calculator is dependent on the analysis of relevant and available data. At present, building large data sets are labour-intensive and costly as these require manual input from discrete individual databases. Under the present configurations, linkage of existing databases poses a significant challenge due to the silo architecture of database systems. By making electronic health records (EHR) and databases interoperable through blockchain technology, data such as diagnostic tests and imaging studies can be shared across clinicians, laboratories, hospitals, pharmacy and the patient, regardless of the application or application vendor, thus avoiding redundant tests and reducing administrative costs.[17] Privacy is maintained by operating a consortium-style blockchain platform where access is only granted to member organizations. MedRec, a collaboration between MIT Media Lab and Beth Israel Deaconess Medical Center, serves both the patient and the practitioner. It not only returns the power of choice to the patient who is given easy access to their medical records held across multiple sites and by different health services,[18] but also integrates with the practitioners' and researchers' current data storage systems. The success of the MedRec model is underpinned by rewarding participants with access to anonymized and aggregated data when they act as blockchain miners responsible for maintaining the stability of this PoW network.

Interoperability is the ability of different information technology systems and software applications to communicate, exchange data and use the information that has been exchanged.

A challenge faced by early adopters of the blockchain technology is how best to overcome scalability especially in the healthcare sector where significant volumes of medical data are generated throughout an individual patient's lifetime.[19] This is being addressed by the National Health Insurance Administration of Taiwan who is trialling a blockchain-enabled iWellChain Framework designed to integrate electronic health and medical records to create a national medical referral service.[20] The iWebChain Framework is built on the Go Ethereum v1.7.3 stable platform which is a permissioned consortium blockchain using proof of authority as the mechanism to validate transactions. The National Health Insurance Administration also developed a dApp (iWellChain DApp), functional on both iOS and Android mobile phone platforms from which patients can access their personal medical data.

Precision medicine

Deloitte identified in their report that precision medicine and patient care and outcomes research are areas that would benefit from adopting blockchain technology.[21] Here, all patient data including genomic data and health records can easily be shared between the patient and their surgeon, general practitioner and clinical management team. This translates to more personalized healthcare delivery via a multidisciplinary team.[22] Data ownership is now returned to patients who predetermine which parties have access to their information. As a corollary, patients can monetize their data securely stored on the blockchain by anonymously allowing controlled access to pharmaceutical companies. This incentivizes their participation in large-scale clinical studies that require commitment of time including travel time to clinical trial centres hosting these studies, responding to quality of life surveys and follow-up tests.

Supply chain and registry provenance

The maturity of blockchain applications in the biomedical domain has yet to peak, nevertheless tracking the provenance of pharmaceutical supply chains is one real-world use case. For example, the use of ambient temperature sensors embedded in pharmaceutical drugs shipping containers will ensure an immutable record of the temperature ranges experienced during transit from the manufacturer to the receiving facility and through the supply chain to the end user.[23] Similarly, blockchain technology can be utilized to create tamper-proof registries of an implanted medical device in addition to monitoring the provenance of medical devices supply chains.[24]

Cybersecurity

The use of encryption, hashing and maintaining multiple copies of the decentralized ledger across the blockchain will bolster security and reduce opportunistic cyberattacks. However, cybersecurity mechanisms to safeguard patient data have yet to be fully implemented in the healthcare industry.

Health authorities have transitioned to cloud-based EHR management systems as a means of reducing the costs otherwise incurred in needing to provide physical storage for hard copies of patient files. In addition, the technology has created wireless monitoring systems of health devices that have uninterrupted signal transmission of patient data from outside the clinical environment to a central server within a hospital. Laudable no less, but with this 21st century solution has come new risks that at the time of implementation were not identified as significant cyber threats. Consequently, no or very little security processes were embedded into its electronic infrastructure. This was not through a lack of foresight, but in part due to the technological naivety of the decision-makers overseeing such mammoth tasks. This is exacerbated by a prevailing culture of complacency and lax security behaviours in handling EHRs by frontline healthcare workers, and a reluctance to invest in upgrading software operating systems that is worsened by lack of expert cybersecurity staff within hospital IT units.[25]

Cybersecurity experts have warned that on the black market, healthcare data are of more value than financial data. Here, a credit card number is worth USD0.10 compared to an EHR which fetches up to USD100.[26] Encapsulated within EHRs are comprehensive sets of personal and demographic information such as previous addresses, names and ages of relatives, medical history details including the number of general practitioner and specialists' visits and diagnoses. These details are used by hackers to build bogus customer profiles for the purpose of committing health insurance fraud. Authorities have detected an increase in these activities in the wake of the COVID-19 pandemic.[27]

The ease with which the security of EHRs can be breached was demonstrated by Victoria's Auditor General, who easily hacked the IT systems of some of the state's biggest hospitals (Royal Children's Hospital, the Royal Victorian Eye and Ear Hospital, Barwon Health and sections of the Department of Health and Human Services).[28]

Hackers use ransomware to exploit vulnerabilities within hospital EHR systems that override operator commands that substitutes the hospital's encryption keys with those of the hackers. This locks out hospital administrators from their own IT systems with access only restored when ransom demands are met. The WannaCry ransomware attack on the UK National Health System computers in 2017 that targeted a vulnerability in Microsoft Windows caused a major disruption resulting in cancellations and delays of surgical cases.[29]

Using real-world data from 41 686 security incidents and 2013 data breaches provided by 73 private and public entities from 83 countries, a 2019 Verizon Data Breach Investigations Report found that the healthcare sector was mostly affected by personal data breaches. It identified privilege misuse, miscellaneous errors and web applications as accounting for 81% of incidents. The highest threats were internal (59%) with an astonishing 83% of these breaches being financially motivated.[30] The fact that most data breaches originate from within an organization should cause hospital administrators considerable alarm. These attacks involved healthcare workers and billing specialists who have legitimate reason to access these data but abused the privilege for financial gain, revenge or out of morbid curiosity. Figures obtained for Australia are similar, where between April and June 2018, there were 242 notifications of data breaches. This came at an average total cost of AUD2.51 million to the organization in 2017 dollar terms.[31] The overwhelming factor was human error (59%) followed by malicious cyberattacks (36%) and systems errors (5%).

The National Cyber Security Centre (UK) recommended that IT administrators implement risk management regimes within their organizations to combat cyberattacks.[32] The regime consists of instituting policies covering user education and awareness, malware prevention and controlling access to removable media. It also recommended that effective management processes and strict controls that limited the number of privileged user accounts were being established. These systems needed to be stress tested regularly to identify weakness points that the IT team could defend through the application of security patches. It was also expected that an incident management plan with a disaster recovery capability was at the ready for deployment in response to any attacks.

As the use of implantable medical devices (IMD) such as cardiac implants and insulin pumps become more commonplace, the threat of malicious actors being able to hack and intercept wireless signals controlling their function are a sobering reality. A similar risk management regime for IMDs should be incorporated but with some modifications. They are: (i) to have an auditing process where detailed logs of IMD activity are recorded to aid in diagnosing operational faults or to detect anomalous activity which may be a precursor to a cyberattack; (ii) swift reporting of software flaws to the manufacturer who can then supply patches to prevent exploitation of these security loopholes; (iii) installation of multi-factor authentication keys for user access to the IMD, and (iv) educating the patient and clinician about cybersecurity risks.[33]

Alleviating health insurance administrative burden

A blockchain healthcare startup, Solve.Care (https://solve.care), has partnered with the Arizona Care Network consisting of 5500 Arizona healthcare providers to improve transaction processes related to managing patients with complex and chronic illnesses. This cohort of patients is at risk of incurring higher care costs due to their disease states, which is expressed through higher administrative burdens associated with processing larger volumes of transactions per patient. The Solve.Care solution is delivered in the form of the Care.Wallet built on the Ethereum blockchain that documents all patient transactions, settles payments to service providers and serves as a ledger for patient clinical data. Solve.Care also introduced an innovative solution to improve patient attendance at predetermined appointments through their partnership with ridesharing company Uber, where patients book and pay for transportation using the Solve cryptocurrency through their Care.Wallet.

Efficient delivery of global health services

In the area of *global health*, blockchain technology and the use of cryptocurrencies or tokens have the potential to deliver global health services into low- and middle-income countries (LMICs).[34] Universal health coverage for LMICs depends on building infrastructure, growing a skilled health workforce and using inexpensive and incorruptible payment systems for local service providers. It is well accepted that investment in health care in LMICs requires significant amounts of capital flows into the country. However, it also presents opportunities for corruption. Inadequate monitoring of expenditure and no means of evaluating effectiveness of monies spent are factors that discourage investment from for profit institutions and not for profit organizations.

Blockchain and the use of cryptocurrency reduce costs of transmitting money across borders and remove intermediaries that add to the cost of transacting money. By using smart contracts built on the Ethereum blockchain as a means of reducing fraudulent activity, investor organizations are assured that grants/monies intended for the purchase of, for example, capital equipment are delivered to the predetermined location as stipulated in the smart contract.

Author Contributions

Lorwai Tan: Conceptualization; data curation; project administration; writing-original draft; writing-review and editing. **David Tivey:** Conceptualization; data curation; writing-original draft. **Helena Kopunic:** Conceptualization; data curation; writing-original draft. **Wendy Babidge:** Conceptualization; data curation; writing-original draft; writing-review and editing. **Sally Langley:** Conceptualization; writing-original draft. **Guy Maddern:** Conceptualization; writing-original draft; writing-review and editing.

Conflicts of interest

LT has pecuniary interests in Solve.Care.

References

1. Natarajan H, Krause S, Gradstein H. *Distributed Ledger Technology (DLT) and Blockchain*. Washington, DC: World Bank Group, 2017.
2. Andrews C, Canepa S, Mangla U, Marchi L, van den Dam R. Enforcing accountability in media – how blockchain technology can work for media and entertainment. 2018.
3. Patel B, Chye B, Ortlieb P *et al*. *The Role of Blockchain in Banking: Future Prospects for Cross-Border Payments*. Crown Place London, UK: Official Monetary and Financial Institutions Forum and China Construction Bank University, 2020.
4. Chang J, Harano K. J. P. Morgan perspectives: blockchain, digital currency and cryptocurrency – moving into the mainstream? 2020.
5. Adams V, Alonso M, Henry W *et al*. Potential uses of blockchain by the U.S. Department of Defense. 2020.
6. Nakamoto S. Bitcoin: a peer-peer electronic cash system. 2008.
7. Dictionary TT. Blockchain definition. Techterms. 2019.
8. Allison I. IBM signs 6 banks to issue stablecoins and use Stellar's XLM cryptocurrency. Coindesk. 2019.
9. Gray M. Ethereum blockchain as a service now on Azure. 2015.

10. O'Bryne R. Blockchain technology is set to transform the supply chain. Logistics Bureau. 2019.
11. Writer DHS. IBM, Goldman Sachs and Morgan Stanley launch world's first global blockchain-based FX market enterprise. The Daily Hodl. 2018.
12. Fekih RB, Lahami M. Application of blockchain technology in healthcare: a comprehensive study. In: Jmaiel M, Mokhtari M, Abdulrazak B, Aloulou H, Kallel S (eds). *The Impact of Digital Technologies on Public Health in Developed and Developing Countries*. Tunisia: Digital Research Centre of Sfax, International Conference on Smart Homes and Health Telematics 2020. 2020; 268–76. https://doi.org/10.1007/978-3-030-51517-1_23.
13. Kuo TT, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* 2019; **26**: 462–78.
14. Heston TA. A case study in blockchain healthcare innovation. *Int. J. Curr. Res.* 2017; **9**: 60587–8.
15. Angraal S, Krumholz HM, Schulz WL. Blockchain technology – applications in health care. *Circ. Cardiovasc. Qual. Outcomes* 2017; **10**: 1–3.
16. Celesti A, Ruggeri A, Fazio M, Galletta A, Villari M, Romano A. Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors* 2020; **20**: 2590.
17. Schumacher A. Blockchain and Healthcare – 2017 Strategy Guide for the Pharmaceutical Industry, Insurers and Healthcare Providers. 2017. [Cited: 2 September 2020.] Available from URL: https://www.linkedin.com/pulse/blockchain-healthcare-2017-strategy-guide-released-axel-schumacher?articleId=6285436702550953984#comments-6285436702550953984&trk=public_profile_post
18. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data. Piscataway, NJ: IEEE Computer Society, 2016.
19. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. *Cryptography* 2019; **3**: 1–16.
20. Lo YS, Yang CY, Chien HF, Chang SS, Lu CY, Chen RJ. Blockchain-enabled iWellChain framework integration with the national medical referral system: development and usability study. *J. Med. Internet Res.* 2019; **21**: e13563.
21. Krawiec RJ, Housman D, White M *et al*. Blockchain: opportunities for healthcare. 2016; 1–16.
22. Peters AW, Till B, Meara JG, Afshar S. Blockchain technology in health care: a primer for surgeons. *Bull, Am. Coll. Surg* 2017; **102**: 27–36.
23. Drosatos G, Kaldoudi E. Blockchain applications in the biomedical domain: a scoping review. *Comput. Struct. Biotechnol. J.* 2019; **17**: 229–40.
24. Tang YM, Ho G, Wu J. Integrating blockchain for improving datasharing in implant surgery. Hamburg, Germany: Proceedings of ISER 147th International Conference. 2018; 27–31.
25. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas* 2018; **113**: 48–52.
26. Yao M. Your electronic medical records could be worth $1000 to hackers. Forbes. 2017.
27. Galloway A. Coronavirus cyber attackers going after hospitals. The Sydney Morning Herald. 2020.
28. Age T. Auditor General hacked into hospitals to expose online security flaws. 2019. [Cited: 2 September 2020.] Available from URL: https://www.theage.com.au/politics/victoria/auditor-general-hacked-into-hospitals-to-expose-online-security-flaws-20190529-p51sd9.html
29. AB Corporation. Ransomware cyberattack: UK's health system recovered from hacking, interior minister says. 2019.
30. Verizon. 2019 Data breach investigations report. 2019.
31. Poneman Institute. 2017 Cost of data breach study: Australia. 2017.
32. National Cyber Security Centre. 10 Steps to cyber security. 2018. [Cited: 2 September 2020.] Available from URL: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
33. Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. *Expert Rev. Med. Devices* 2018; **15**: 403–6.
34. Till BM, Peters AW, Afshar S, Meara J. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage? *BMJ Glob. Health* 2017; **2**: e000570.