# Trust-building in digital health: An exploration of the business case for Block Chain technologies

**David Lopez, David Plans, Alan Brown, Phil Godsiff**

*University of Exeter*
*{d.lopez2*;d.plans; alan.w.brown; p.j.godsiff}@exeter.ac.uk*

## Abstract

This paper aims to shed light on the phenomenon of citizen adoption of digital health mechanisms. The study draws upon theories from information systems and economics to propose and operationalize a model explaining users' uncertainty to adopt digital health and contribute with their own personal data.

We further conduct a design-based examination of block chains and their potential to enable trustworthy transactions of personal health data.

The results of our research support block chains as important technological artefacts in data-intensive digital health contexts: block chains nurture citizens' trust by providing five technology affordances: Decentralized management of information, End-to-End communication, Controlled Transparency, Irreversibility and Self-executing contracts.

***Keywords*** – digital health; trust; information privacy; design science; block chains

## 1 Introduction

Over the past decade, electronic health records have been widely adopted in hospitals and clinics worldwide. Significant clinical knowledge and a deeper understanding of patient disease patterns and pathways of care can be inferred from the aggregation and further processing of medical records (Hannauer et al. 2009, Hannauer el a. 2011, Linn et al. 2011, Kohli and Tan 2016). The combination of medical records with advanced analytical capabilities affords economic and operational improvements derived from evidence-based clinical practices, better processv traceability and decision support systems (Wang et al. 2018).

Artificial intelligence, defined as a set of computer techniques that enables systems to perform tasks normally requiring human intelligence is finding innovative applications in healthcare contexts. Widely applied, new advances are continually announced. Most recently, for instance, researchers have unveiled artificial intelligence models that scan retinal images to predict eye- and cardiovascular-disease risk, and that analyse mammograms to detect breast cancer with a precision level comparable to that of a clinician (Economist 2016, 2018a, Nature 2018).

Moreover, the combination of artificial intelligence with clinical and personal health data holds great potential to support precision medicine, an emerging approach for disease treatment and prevention that considers individual variability in environment, lifestyle and genomic information to match patients with the therapy that is best suited to them and their condition (Schork 2015, NIH 2018).

Precision medicine has been portrayed as a revolutionary breakthrough in health care empowering both patients and the general public to participate more in treatment decisions. One key consequence of this shift is a focus on preventive measures and thus support for the transformation of healthcare from reactive and hospital-centric to preventive, proactive and evidence-based with a focus on wellbeing rather than disease control (Hamburg and Collins 2010, Wactlar 2011, Árnason 2012, Chen 2012, Jameson 2015, Collins 2015).

Information privacy concerns are expected to play an important role in an individuals' willingness to be profiled (Milberg et al. 2000, Van Slyke et al. 2006), and their intentions to embrace digital health (Malhotra et al. 2004). Digital health viewed as the triad of artificial intelligence, clinical records and personal health data will only become a reality if individuals can be persuaded to change their attitudes and allow their medical information to be digitized and processed by third parties (Angst and Agarwal 2009, Kohli and Tan 2016).

Recent data breaches and data management malpractices bring to the fore the importance of adequate provisioning of information privacy in healthcare: in 2016, DeepMind, an AI company in London owned by Google's parent, Alphabet, became mired in controversy after press reports revealed that a branch of the UK National Health Service had given the company access to 1.6 million patient records without adequate consent. The information included names and sensitive information, such as whether a person had transmitted diseases (Maxmen 2018).

Inevitably, such concerns continue to grow with each new high-profile failure. The recent Cambridge-Analytica scandal is the most recent instance of a series of incidents highlighting the importance of information privacy and the scale of risks involved in the harvesting and further processing of personal data for commercial purposes (Economist 2018b). Moreover, it constitutes a case in point of the personalization-privacy paradox: the tension between how digital services requires users' data to offer them personalized experiences and users' growing concerns about the privacy of that information (Kavassalis et al. 2003, Lee and Benbasat 2003, Sutanto et al. 2013).

New technological approaches to managing and securing sensitive data have been investigated for many years. More recently, Block Chain Technology (BCT), an instance of Distributed Ledger Technology (DLT), is rewriting conventional notions of business transacting, creating fresh opportunities for value creation and capture. DLT is one of the latest in a long list of digital technologies that appear to be offering increased confidence in secure data sharing. This was emphasized in a recent report by the UK government's Chief Scientific Officer, Sir Mark Walport, in which it is stated that "in distributed ledger technology we may be witnessing one of those explosions of creative potential that catalyse exceptional levels of innovation" that could have "the capacity to deliver a new kind of trust to a wide range of services".

From this perspective this paper, adopting a normative perspective, explores the design implications of uncertainty and trust in new digital health services. A core tenet of the paper is the role Block Chains (BCTs) will play in digital health, BCTs by providing (1) Decentralized management of information, (2) End-to-End communication, (3) Controlled Transparency, (4) Irreversibility and (5) Self-executing contracts facilitate: tracking and settling transaction attributes (e.g. data ownership) as well as the enforcement of contracts in digital health ecosystems (Iansiti and Lakhani 2017, Ito et al. 2017).

In this regard we are finding BCTs as potentially disruptive enablers of costless verification in next generation, data-intensive, digital health services.

# 2 Uncertainty and trust in digital health

To better understand the nature of trust and uncertainty and mitigate its detrimental impact in the adoption of digital health, we refer to the principal-agent theory (Rothschild and Stiglitz 1978, Akerlof 1978). The principal-agent perspective addresses the ubiquitous agency relationship whereby one entity (the principal) delegates work for another (the agent) who performs the work according to a mutually agreed contract. Agency relationships arise whenever one party depends on another party to undertake some action on its behalf (Eisenhard 1989).

The principal-agent perspective is particularly applicable to digital health as: (1) involved parties (e.g. citizens, AI-providers, insurers, public bodies) have different goals and interests, (2) there is a possibility for participants to act opportunistically (e.g. for-profits using personal data without consent) , (3) it is difficult to monitor agents and enforce their expected actions (e.g. an AI-provider misusing personal data for non-authorized purposes), (4) there are significant time lags in which an agent's actions can be manifested (e.g. an AI-provider retaining personal data for an indefinite time period). As a result, digital health faces two challenges: hidden information and hidden action.

Hidden information arises ex-ante to the data exchange transaction as data-buyers possess hidden information about the real value of the data (Stiglitz and Edlin, 1992; Stiglitz, 2002).

Hidden-information results in two sources of uncertainty in digital health: First, information asymmetry, which is due to the fact that data-owners perceive data-buyers to have a greater quantity of information that they have. Second, data-owners have fears that data-buyers may act opportunistically to serve their self-interest due to divergence of interests (Pavlou 2011).

Hidden action takes place ex-post to the data exchange as data-owners give their data to data-buyers who may not exert the promised effort or engage in hidden actions that profit them at the data-owners' expense.

Hidden-action causes additional uncertainty in digital health due to side effects of the data exchange in which the data-owner implicitly renders personal information in the transaction. This leads to two additional sources of uncertainty: information privacy concerns and information security concerns.

## 2.1. Information Asymmetry and Opportunism

A Principal-Agent perspective assumes that involved parties are motivated by self-interest and, whenever possible, will attempt to exploit the situation to maximize their profits. Opportunism is possible in agency relationships where there is goal incongruence and data-buyers may act opportunistically since the data-owner cannot fully monitor data-buyers' behaviour and enforce compliance (Eisenhardt 1989). Examples of data-buyer opportunism include contract default, fraudulent data reselling and unauthorized uses of data among others.

Information asymmetry has also been recognized as a common problem in buyer-seller transactions in which one side usually possess more information than the other. Under information asymmetry conditions it is difficult for both parties to distinguish among high- and low-value data exchanges. Even if data-buyers try to pre-contractually assess the value of the data a true inference can only be made after the transaction has been completed and fulfilled. Whenever there is physical or temporal separation between data-buyers and data-owners, information asymmetry dominates giving rise to hidden information. Higher levels of information asymmetry lead to higher uncertainty associated with any health data exchange.

If digital health is to thrive, participants thus need to be able to efficiently and effortlessly verify and audit transaction attributes, including the credentials and reputation of the parties involved, the ownership and characteristics of the data and services exchanged.

This leads us to suggest costless verification as a design principle (DP1) to be fulfilled in digital health services. *Costless verification of transactions* emerges a required capability that prevents participants in digital health to engage in opportunistic behaviour out of fear of facing the adverse consequences of being dishonest. Costless verification of transactions mitigates opportunism and information asymmetry as it provides structural assurances and calculative-based trust (Geffen et al. 2003). Structural assurances refer to an assessment of success in the transaction due to legal recourse, guarantees and regulation in the context of data exchanges (Shapiro 1987, McKnight et al. 1998). Calculative-based trust refers to the lack of rational incentives for any party to engage in opportunistic behaviour as the costs of being caught outweigh the benefits of cheating (Geffen et al. 2003).

## 2.2. Information Privacy concerns

Information privacy, defined in Clarke (1999), Belanger and Crossler (2011) as “the interest and individual has in controlling, or at least significantly influencing, the handling of data about themselves” emerges as yet another source of uncertainty in digital health. In digital health, buyers (e.g. insurance companies, public bodies, AI-providers) collect detailed personal information from data-buyers for the purposes of research, insurance, medical diagnosis or recommendations. While data-buyers profit from the availability of personal fined grained health data, data-owners often perceive this as an invasion of privacy.

When data-owners disclose their personal information, two types of information privacy concerns arise. One related to the improper use of information due to absence of sufficient controls, another related to a potential secondary use of personal information without the data-owner’s consent (Bélanger and Crossler 2011, Pavlou 2011, Smith et al. 2011). We contend that addressing information privacy concerns in digital health requires: control over data collection (DP2), control over data processing (DP3) and awareness of privacy practices (DP4).

*Control over data collection and data processing*: The collection of personal health data is an important source of privacy concerns in digital health. Consumers want to exercise process control and influence changes in organizational policies they find objectionable regarding their personal data, especially when a large potential exists for opportunistic behaviour and breach of the social contract in a relational exchange. Hence, giving data-owners control over personal information (e.g. approval, modification, opt-out) is an important instrument to address information privacy concerns.

*Awareness of privacy practices.* Control over data collection and data processing are active instruments to address information privacy concerns. Awareness, however, is a passive antecedent of information privacy as it refers to the degree to which a citizen is concerned about his/her awareness of organizational information privacy practices. In this regard we contend that citizens must explicitly be provided with notice on private policies and procedures and informed on the purposes for which personal information is collected, used, retained and disclosed.

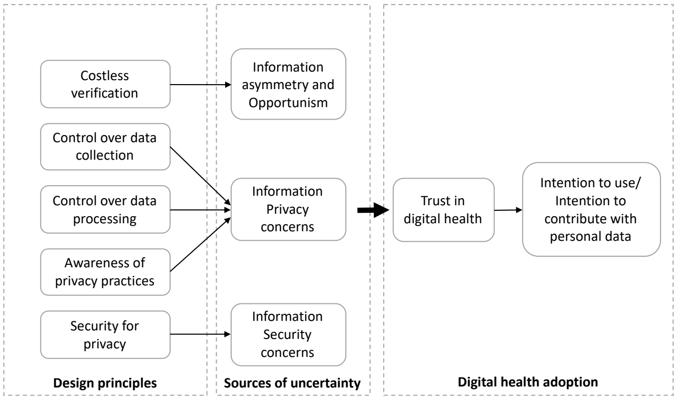
## 2.3. Information Security concerns

Information security concerns are formally defined in a digital health context as the data-owner’s beliefs about a data-buyer’s inability and unwillingness to safeguard their personal information from security breaches during transmission and storage (Lohr and Donaldson 1994).

Security for Privacy entails three critical components: (1) Pseudonymisation and encryption of personal data; (2) confidentiality, integrity, availability and resilience of processing systems and services; (3) availability and access of personal data, regular auditing and evaluation of the effectiveness of technical and organizational measures ensuring the security of data processing (EU 2016).

We believe that Security for Privacy, as an instrument to address information security concerns, needs to be incorporated as a core design principle (DP5) in new digital health services.

As summarized in the following figure 1, we suggest that digital health services can address uncertainty and nurture citizens’ trust by adopting costless verification, controls over data collection and processing, disclosure of privacy practices and security for privacy as design principles underpinning the development of technological artefacts and models of governance of digital health ecosystems.


Costless verification
Control over data collection
Control over data processing
Awareness of privacy practices
Security for privacy
Information asymmetry and Opportunism
Information Privacy concerns
Information Security concerns
Trust in digital health
Intention to use/ Intention to contribute with personal data
Design principles
Sources of uncertainty
Digital health adoption

# 3 Blockchain-based trust in digital health

Block chains (BCTs) as a digital evolution of ledgers, allow the recording and verification of transactions and terms of engagement. Like their former counterparts they record information about who owns what, who bought from whom or who has decision-making rights in a specific context (Felin and Lakhani 2018).

A unique feature of BCTs is their distributed and digital nature which allows business transactions to be instantly recorded and simultaneously updated across all involved parties' digital ledgers. Moreover, the record of each transaction is indelibly recorded using advanced cryptographic mechanisms.

More precisely BCT enable five technology affordances (Majchrzak and Markus 2013) required to facilitate the development, execution and verification of business transactions without the intervention of intermediaries:

**1. Decentralized management of information**. Each party involved in a business transaction has access to the entire history of transformations and involved attributes. There is no single point of control. Every party can verify the records of transaction partners directly.

**2. End-to-End communication**. Communication occurs directly between peers instead of through intermediaries

**3. Controlled Transparency**. Every transaction is visible to anyone with access to the system, participants can choose the level of attribute's privacy they desire.

**4. Irreversibility**. Once a transaction is entered in the database and ledgers are updated, records cannot be altered. Various computational algorithms and processes are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

**5. Self-executing contracts**. Transactions can be tied, and enforced, by means of computational logic thus allowing parties to set up algorithms and rules that automatically and irreversibly trigger transactions between nodes.

In our view these five technology affordances make BCTs suitable candidates to sustain design principles (DP1-DP6) as defined in section 2.

Costless verification (DP1) is facilitated as interested parties have transparent access to business transactions and derived data transformations, moreover irreversibility and self-executing contracts effectively enforces the fulfilment of contractual obligations.

Control over data collection (DP2) and data processing (DP3) is operationalized through the ability of citizens to choose the level of privacy they desire as well as the end-to-end communication principle.

BCTs underpin Security for Privacy (DP5) given their strong support for integrity, resilience and resistance to cyberattacks.

In this regard we find BCTs critical technological artefacts underpinning trust in next generation, data-intensive, digital health services.

# 4. Key findings

Observations from our work highlight the underlying concerns for individuals in the use of digital health solutions with respect to the trusted relations they require. Borrowing from Trust-TAM (Gefen and Straub 2003, Fang et al. 2014) and Information Privacy models (Bélanger and Crossler 2011) we find four antecedents of trust and uncertainty in digital health: information asymmetry, opportunism, information privacy and information security concerns.

The results of our research support block chains as relevant technological artefacts in data-intensive digital health contexts: block chains nurture citizens' trust by providing five technology affordances: Decentralized management of information, End-to-End communication, Controlled Transparency, Irreversibility and Self-executing contracts.

These five affordances facilitate granular and inexpensive tracking of transaction attributes, settling transactions and contracts enforcement thus allowing individuals, healthcare providers, insurers to: (1) validate in near real time relevant attributes of specific transactions and (2) engage in economic transactions over bits of information (e.g. one week's worth of heartrate data) that were previously uneconomical to trade.

# 5. Public policy implications

Based on our experience, existing block chain technologies (e.g. Ethereum, HyperLedger) have reached a level of maturity that allows rapid and stable prototyping and experimentation of use cases. The scaling up of block chain-based solutions in digital health, however, will require significant improvements in current performance of consensus mechanisms and replacement of current proof-of-work approaches for other, less computing intensive, alternatives (e.g. proof-of-stake).

From a public policy perspective, current approaches to digital health and wellbeing tend to follow provider-centric paradigms with models of governance strongly organized around a single stakeholder (e.g. Apple, Google,Microsoft, FitBit), in our view this leads to fragmentation and lack of interoperability thus severely limiting economies of scale and scope and more importantly (2) run counter to users' privacy concerns and rights (Lee et al. 2011, Pavlou 2011). In this regard we are finding block chains useful instruments to create commons-oriented ecosystems of value creation and exchange (Pazaitis et al. 2017).

These observations provide an important boost for the on-going regulation activities in digital government. Policy makers may consider supporting block chain-based paradigms by instituting standardization committees and supporting large scale deployments in collaboration with interested parties including citizens and the medical community.

## Acknowledgements

Authors acknowledge financial support from the Engineering and Physical Sciences Research Council (grant: EP/P03196X/1)

## References

Akerlof, G.A., 1978. The market for "lemons": Quality uncertainty and the market mechanism. *Uncertainty in Economics* (pp. 235-251).

Angst, C.M. and Agarwal, R., 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly*, 33(2), pp.339-370.

Árnason, V., 2012. The personal is political: ethics and personalized medicine. *Ethical Perspectives*, 19(1), pp.103-122.

Baird , A., Angst, C., Oborn, E., Health Information Technology. MIS Quarterly Research Curations, Ashley Bush and Arun Rai, Eds., http://misq.org/research-curations, June 20, 2018.

Bélanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly, 35(4), pp.1017-1042.

Chen, H., Chiang, R.H. and Storey, V.C., 2012. Business intelligence and analytics: from big data to big impact. MIS quarterly, pp.1165-1188.

Clarke, R., 1999. Internet privacy concerns confirm the case for intervention. Communications of the ACM, 42(2), pp.60-67.

Collins, F.S. and Varmus, H., 2015. A new initiative on precision medicine. New England Journal of Medicine, 372(9), pp.793-795.

Culnan, M.J. and Williams, C.C., 2009. How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS Quarterly, pp.673-687.

Economist, 2016. Artificial Intelligence in the real world. Economist Intelligence Unit.

Economist, 2018a. Artificial Intelligence will improve medical treatments. The Economist print edition.

Economist, 2018b. Britain moves to rein in data-analytics. The Economist print edition.

Eisenhardt, K.M., 1989. Agency theory: An assessment and review. Academy of management review, 14(1), pp.57-74.

EU, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Article 32.

Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E. and Lim, K.H., 2014. Trust, satisfaction, and online repurchase intention: The moderating role of perceived effectiveness of e-commerce institutional mechanisms. MIS Quarterly, 38(2).

Felin, T. and Lakhani, K., 2018. What problems will you solve with block chain?. MIT Sloan Management Review.

Gefen, D., Karahanna, E. and Straub, D.W., 2003. Trust and TAM in online shopping: An integrated model. MIS quarterly, 27(1), pp.51-90.

Gregor, S. and Hevner, A.R., 2013. Positioning and presenting design science research for maximum impact. MIS quarterly, 37(2).

Hamburg, M.A. and Collins, F.S., 2010. The path to personalized medicine. New England Journal of Medicine, 363(4), pp.301-304.

Hanauer, D. A. , Rhodes, D. R., and Chinnaiyan, A. M. 2009. Exploring Clinical Associations Using '-Omics' Based Enrichment Analyses. PLoS ONE (4:4): e5203.

Hanauer, D. A., Zheng, K., Ramakrishnan, N., and Keller, B. J. 2011. "Opportunities and Challenges in Association and Episode Discovery from Electronic Health Records," IEEE Intelligent Systems 26(5), pp. 83-87

Hevner, A.R., March, S.T., Park, J. and Ram, S., 2004. Design Science in information systems research. MIS Quarterly, 28(1), pp 75-105.

Iansiti, M. and Lakhani, K.R., 2017. The truth about block chain. Harvard Business Review, 95(1), pp.118-127.

Ito, J., Narula, N. and Ali, R., 2017. The block chain will do to the financial system what the Internet did to media. Harvard Business Review.

Jameson, J.L. and Longo, D.L., 2015. Precision medicine—personalized, problematic, and promising. Obstetrical & Gynecological Survey, 70(10), pp.612-614.

Kavassalis, P., Spyropoulou, N., Drossos, D., Mitrokostas, E., Gikas, G. and Hatzistamatiou, A., 2003. Mobile permission marketing: Framing the market inquiry. International Journal of Electronic Commerce, 8(1), pp.55-79.

Kohli, R. and Tan, S.S.L., 2016. Electronic health records: how can IS researchers contribute to transforming healthcare?. MIS Quarterly, 40(3), pp.553-573

Lee, Y.E. and Benbasat, I., 2003. Interface design for mobile commerce. Communications of the ACM, 46(12), pp.48-52

Lee, D.J., Ahn, J.H. and Bang, Y., 2011. Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection. MIS Quarterly, pp.423-444.

Lin, Y., Brown, R. A., Yang, H. J., Li, S., Lu, H., and Chen, H. 2011. "Data Mining Large-Scale Electronic Health Records for Clinical Support," IEEE Intelligent Systems 26(5).

Lohr, K.N. and Donaldson, M.S. eds., 1994. Health data in the information age: use, disclosure, and privacy. National Academies Press.

Majchrzak, A. and Markus, M.L., 2013. Technology affordances and constraints theory (of MIS). Kessler E, ed. Encyclopedia of Management Theory.

Malhotra, N.K., Kim, S.S. and Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), pp.336-355.

Markus, M.L., Majchrzak, A. and Gasser, L., 2002. A design theory for systems that support emergent knowledge processes. MIS Quarterly, pp.179-212.

Maxmen, A., 2018. AI researchers embrace Bitcoin technology to share medical data. Nature, 555, pp.293-294.

McKnight, D.H., Cummings, L.L. and Chervany, N.L., 1998. Initial trust formation in new organizational relationships. Academy of Management review, 23(3), pp.473-490.

Milberg, S.J., Smith, H.J. and Burke, S.J., 2000. Information privacy: Corporate management and national regulation. Organization science, 11(1), pp.35-57.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Nature, 2018. AI Diagnosis needs attention. Nature, 555, pp. 285

NIH, 2018: https://allofus.nih.gov/

Pavlou, P.A., 2011. State of the information privacy literature: Where are we now and where should we go?. MIS Quarterly, pp.977-988.

Pazaitis, A., De Filippi, P. and Kostakis, V., 2017. Block chain and value systems in the sharing economy: The illustrative case of Backfeed. Technological Forecasting and Social Change, 125, pp.105-115.

Popovic, A., Smith, H.J., Thong, J.Y.L., and Wattal, S. “Information Privacy,” in MIS Quarterly Research Curations, Ashley Bush and Arun Rai, Eds., http://misq.org/research-curations, April 30, 2017.

Rothschild, M. and Stiglitz, J., 1978. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. Uncertainty in economics (pp. 257-280).

Schork, N.J., 2015. Personalized medicine: time for one-person trials. Nature, 520(7549), pp.609-611.

Shapiro, S.P., 1987. The social control of impersonal trust. American journal of Sociology, 93(3), pp.623-658.

Smith, H.J., Dinev, T. and Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), pp.989-1016.

Stiglitz, J.E. and Edlin, A.S., 1992. Discouraging rivals: Managerial rent-seeking and economic inefficiencies (No. w4145). National Bureau of Economic Research.

Stiglitz, J.E., 2002. Information and the Change in the Paradigm in Economics. American Economic Review, 92(3), pp.460-501.

Sutanto, J., Palme, E., Tan, C.H. and Phang, C.W., 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quarterly, 37(4).

Söllner, M., Benbasat, I., Gefen, D., Leimeister, J. M., Pavlou, P. A. “Trust,” in MIS Quarterly Research Curations, Ashley Bush and Arun Rai, Eds., http://misq.org/research-curations, October 31, 2016.

Van Slyke, C., Shim, J.T., Johnson, R. and Jiang, J.J., 2006. Concern for information privacy and online consumer purchasing. Journal of the Association for Information Systems, 7(1), p.16.

Wang, Y., Kung, L. and Byrd, T.A., 2018. Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting and Social Change, 126, pp.3-13.

Wactlar, H., Pavel, M., and Barkis, W. 2011. "Can Computer Science Save Healthcare?" IEEE Intelligent Systems 26(5), pp. 79-83.

Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, pp.1-32.