Design of Blockchain-based Precision Health-Care Using Soft Systems Methodology

By: Ravi Sharma, Charcy Zhang, Stephen C. Wingreen, Nir Kshetri, and Arnob Zahid

Sharma, Ravi; Zhang, Charcy; Wingreen, Steve; Kshetri, Nir; Zahid, Arnob (2020) "Design of Blockchain-based Precision Health-Care Using Soft Systems Methodology." *Industrial Management & Data Systems* Vol. 120 No. 3, pp. 608-632. https://doi.org/10.1108/IMDS-07-2019-0401.

Abstract:

Purpose: The purpose of this paper is to describe the application of soft systems methodology (SSM) to address the problematic situation of low opt-in rates for Precision Health-Care (PHC). **Design/methodology/approach:** The design logic is that when trust is enhanced and compliance is better assured, participants such as patients and their doctors would be more likely to share their medical data and diagnosis for the purpose of precision modeling. **Findings:** The authors present the findings of an empirical study that confronts the design challenge of increasing participant opt-in to a PHC repository of Electronic Medical Records and genetic sequencing. Guided by SSM, the authors formulate design rules for the establishment of a trust-less platform for PHC which incorporates key principles of transparency, traceability and immutability. **Research limitations/implications:** The SSM approach has been criticized for its lack of "rigour" and "replicability". This is a fallacy in understanding its purpose – theory exploration rather than theory confirmation. Moreover, it is unlikely that quantitative modeling yields any clearer an understanding of complex, socio-technical systems. **Practical implications:** The application of Blockchain, a platform for distributed ledgers, and associated technologies present a feasible approach for resolving the problematic situation of low opt-in rates. **Social implications:** A consequence of low participation is the weak recall and precision of descriptive, predictive and prescriptive analytic models. Factors such as cyber-crime, data violation and the potential for misuse of genetic and medical records have led to a lack of trust from key stakeholders – accessors, participants, miners and regulators – to varying degrees. **Originality/value:** The application of Blockchain as a trust-enabling platform in the domain of an emerging eco-system such as precision health is novel and pioneering.

Keywords: design science research | trust-less platform | digital healthcare

Article:

1. Challenges facing Precision Health-Care

An emerging trend in the practice of medicine known as Precision Health-Care (PHC) has been suggested as a promising service on digital health ecosystems or clouds. It is defined as the development of a quantitative model which links the individual EHRs to the population and derives the benefit of aggregating EHRs with consideration to social context (Colijn *et al.*, 2017). Although there are distinctions made between PHC and personalized medicine, a simplifying assumption is that the former is a system-level perspective whereas the latter is patient-centric. More specifically, PHC comprises health and medical records which are networked to various front-end clients. It is an instance of an evidence-based approach which provides personalized medicine, including clinical decisions, treatments and products to the individual patient (Lu *et al.*, 2014; Zimmerman, 2019). This approach is driven by data analytic models, which possess the ability of dealing with large amounts of genome information which combine genetic diagnoses with EHRs or EMRs (Mehta and Pandit, 2018).

With the support of robust data analytics and machine learning, PHC is capable of descriptive, predictive or prescriptive diagnostics by benchmarking individuals with the population in order to “discover” diseases, treatments or outcomes (Colijn *et al.*, 2017). Typically, patients of universal healthcare who opt-in, consent to share their medical data (including genetic sequence data) into such a data base. They are the actual cases used for the construction of regression or machine learning models, which formulate prescriptions and predictions linking to diagnosis, treatments and outcomes with anonymised patient profiles as moderators. When PHC is applied as a service, input will be the patient’s profile and diagnosis report(s); and the output will be the treatment (e.g. therapy, medication, behavioural changes and surgical procedure). In a best-case scenario, PHC learns from each health event of individuals who opt-in and provides more precise predictions along with prescriptions. However, the reluctance of individuals to opt-in and share genetic and medical data results in a weaker analytic model and machine learning environment and hence a tragedy-of-the-commons scenario for PHC.

With Digital Healthcare having “crossed the chasm”, a large volume, velocity, variety and veracity of health data is produced and shared among numerous players in the eco-system such as Patients (Consumers), (Health-Care) Providers, Payers, Vendors, Infomediaries and Regulators (Stephanie and Sharma, 2016). The twin issues of security and privacy are hence critical. Security refers to protection against the unauthorized access or modification of health data such as controls in place to limit who can access the information. Privacy is harder to define, in part because user-specific details (Personally Identifiable Information (PII)), preferences and contexts, but also because it refers to what many believe to be a “human right”. The idea of what constitutes PII is an important aspect of security and privacy in digital health and contribute significantly to user experience[1].

Cyber-security in health-care is a major problem with “hundreds” of reported violations (Williams, 2019). In reality, most people are unwilling to share their health data, considering that such disclosure might negatively impact on their privacy (Patil and Seshadri, 2014). An intrusive aspect of PHC is the requirement for genetic sequencing information from patients. Research by Ponemon (2016) suggests that 38 per cent are not willing to participate in genetic testing because of deep-rooted distrust. In current PHC platforms, patients’ privilege and control over their medical data are limited by insufficient data transparency; patients often do not know or control who accesses their health records and for what reason (Colijn *et al.*, 2017). Neither are players in the PHC eco-system explicitly accountable for data breaches (Das *et al.*, 2016). The Trusted Third Party (TTP) – a service provider – neither has the moral right nor the technical ability to mediate. However, unlike conventional EHRs and EMRs, genetic information is not common in established clinical practice (Nguyen *et al.*, 2014). For better treatment outcomes, sharing of personal health information (e.g. historic medical records of profiles, symptoms, treatments and outcomes) with patients' consent is necessary. Nevertheless, the contribution of sensitive genetic information for the development of predictive or prescriptive data models is controversial (Lunshof *et al.*, 2008). For reasons discussed by Schatz *et al.* (2017), among others, patients' high concern with respect to privacy and security of their genetic information contributed to their low enthusiasm for opting-in to the "collective good" of PHC (Brothers and Rothstein, 2015).

PHC hence gives rise to a "tragedy of the commons" scenario. Large contributions of rich cases from patients' opting-in and sharing their EHRs and EMRs allows the building of robust models and gain sufficient samples for data mining (Van Poucke *et al.*, 2016). Through data analysis, errors or redundancies in high volume and variety data sets can be reduced, which ensures higher accuracy of future outcomes even in complex, multilevel demographics (e.g. age, gender and ethnicity). Such collection of data with wider variation enriches the variety of data sources and leads toward the development of robust predictive models accordingly (Sedgwick, 2015). The availability of gene sequences from patients provides greater analytics ability of PHC (Frey *et al.*, 2014). However, while prospective users of PHC may wish to benefit from its advantages, they may not wish to risk their own medical records to misuse or abuse. Another significant concern of opting-in to a genetic sequence based PHC is that law-enforcement authorities may choose to subpoena such records and link patients to any number of activities. There was a need to examine the efficacy of a data management technology that protects against such abuses.

The application of Blockchain to digital health has received increasing research attention (Brodersen *et al.*, 2016; Burniske *et al.*, 2016; Mackey *et al.*, 2019; Mettler, 2016; Yue *et al.*, 2016; Halamka *et al.*, 2017; Agbo *et al.*, 2019; Park *et al.*, 2019; Shuaib *et al.*, 2019; Siyal *et al.*, 2019). Rabah (2017) claims that the technology – particularly its automated verification and trust resolution capabilities – promises the safe and interoperable sharing of real-time data among stakeholders that is required in a trusted digital health platform. To address the problem of low opt-in rates due to a lack of trust in a PHC service, our research objective is to explore the design feasibility of a Blockchain-based solution for PHC. The specification of design principles and artefacts is derived empirically through the application of Soft Systems Methodology (SSM) – developed by Peter Checkland (1995, 2000) and his associates for the purpose of developing socio-technical solutions where the interactions of technologies and their human users determine implementation success. The remainder of this paper is organized as follows. The next section reviews the underlying functionalities of Blockchain and their application to PHC. Following this, the paper outlines the major steps of SSM and their adaptation to our field study. Section 4 describes the application of Blockchain to PHC using SSM in order to address issues of data security and privacy. Section 5 is a discussion of the derived design principles that provide a solution to the problem of low opt-in rates. The paper concludes with some insights for policy and a recap of theoretical, practical and methodological contributions.

2. Background review of health Blockchains

Blockchain is a decentralized, distributed, anonymous, time-stamped ledger of data records (Shuaib *et al.*, 2019) which seems to intuitively fit with current digital health environments. Blockchains have received scholarly attention for their unique security characteristics such as being tamper-proof and transparent (Naerland *et al.*, 2017). Note that whilst a decentralized and distributed platform does not provide any security nor privacy guarantees, the unique functional attributes of the technology do. For instance, it is possible to exchange data records on such a network without the need for a centralized TTP (Agbo *et al.*, 2019) nor a "new clearing house" or "safe deposit box", but an intelligent control of records with a time-stamped, programmable ledger (Halamka *et al.*, 2017). Data in blocks form a chain of events, for example, the enrolment of a patient with a healthcare provider and her subsequent health transactions. Additions to these blocks are allowed if and only if broadcast by authorized entities and any changes are traceable (Xia *et al.*, 2017). Moreover, they are also synchronised and immutable; when a change occurs, all nodes in the network are notified and typically the change is effected when there is >50 per cent consensus (Shuaib *et al.*, 2019). In terms of functionalities, Blockchains go beyond the common use-case as crypto-currencies (Underwood, 2016).

Closely associated with Blockchain is the notion of a "Smart Contract" (SC) which is an extension of contractual obligations in the digital era. It can be defined as a set of programmable codes and privileges which can automatically move digital assets (including information) depending on pre-specified rules (Buterin, 2014). Data blocks may be programmed to be accessible with various rights (read, write, edit, delete, etc.) by all (public and permission-less) or pre-approved (private and permissioned) participants. All such terms of the contract are encrypted with Blockchain technology. SC hence alters the traditional notion of trust with an open, transparent and non-retractable scheme where the encryption key is now more important than trust. The SC codes may be audited to guarantee fairness and compliance (O'Hara, 2017). In a "private, permissioned" context such as digital health records, "only pre-defined nodes can read, submit and validate transactions" (Naerland *et al.*, 2017). There can also be classes of data (or objects) which contain unique read–write–edit–delete (RWED) privileges for various entities (e.g. patients, physicians, specialists, hospitals, regulators and payers). Large data sets may also be partitioned into centrally stored and distributed-blocks components. Hence, SC is a useful mechanism to implement such pre-specified rules, though solutions referring to the practice of PHC are few.

A meta-analysis of research reviews was conducted in order to synthesize the functional attributes of Blockchain that provide "trustless" security and privacy. Specifically, an electronic search of research spanning 2016–2019 using Google Scholar and Research Gate was performed using the following keywords and expressions: Review AND Blockchain AND (precision OR personalized) AND (health OR medicine). Upon examining the titles and abstracts over a hundred hits, a representative set of 15 articles was selected on the basis of their relevance and applicability to our objective of investigating the functional attributes of Blockchain in precision health. The performance considerations of Blockchain are beyond the scope of this paper and research describing such topics excluded from further analysis.

Table I summarizes the scope and coverage of the representative set of recent research articles that were selected for our meta-review. On closer examination, three distinct categories of coverage could be discerned: i) Blockchain in health, ii) Blockchain implementation and iii) PHC. At a high level, the focus of such scholarly reviews was to comprehensively explore issues and challenges in the application of Blockchain to Healthcare (cf. Agbo *et al.*, 2019), address functional design of Blockchain implementations (cf. Xia *et al.*, 2017) and in category (iii) describe the merits or perils of PHC (cf. Love-Koh *et al.*, 2018). Some articles were more expansive, covering two categories (cf. Vazirani *et al.*, 2019). To probe further, full text (PDF) documents of the 15 references given in Table I were parsed using the Nvivo v12 Qualitative Analysis software. Whereas a thematic analysis is not within the scope of this section, detailed outputs from Nvivo and brief annotations may be found in the Online Appendix 1 accompanying this paper (Electronic or digital copies are available from the corresponding author).

Table I. Meta-review of background research (2016–2019)

Reference	Category	Title	Extract – quotes
1. Agbo et al. (2019)	Blockchain in Health	Systematic Review of Blockchain Technology in Healthcare	While a number of studies have proposed different use cases for the application of blockchain in healthcare, there is a lack of adequate prototypes and studies to characterize the effectiveness of these
2. Bruynseels et al. (2018)	Precision Health	Digital Twins in Health Care: Ethical Implications of an Emerging Engineering Paradigm	A Digital Twin might not be an accessible technology for everyone, and given the fact that patterns identified across a population of Digital Twins can lead to segmentation and discrimination. This duality calls for governance as this emerging technology matures, including measures that ensure transparency of data usage and derived benefits, and data privacy
3. Hallwright and Carnaby (2019)	Blockchain Implementation	Complexities of Implementation: Oxfam Australia's Experience in Piloting Blockchain	Awareness and understanding of the technology, capacity constraints of in-house support services and issues related to engaging in non-traditional partnerships. Three types of precision medicine are expected to emerge in clinical practice: complex algorithms, digital health applications and "omics"-based tests
4. Jitesh and Scaria (2017)	Precision Health	From genomes to genomic medicine: enabling personalized and precision medicine in the Middle East	Reviews the genome projects and suggests how addressing the key areas including education, regulatory and ethical frameworks would accelerate Precision Medicine in the Middle East region
5. Love-Koh et al. (2018)	Precision Health	The Future of Precision Medicine: Potential Impacts for Health Technology Assessment	Innovation in precision medicine promises substantial benefits but will change the way in which some health services are delivered and evaluated
6. Mackey et al. (2019)	Blockchain in Health/ Implementation	Challenges and opportunities for applications of blockchain technology in the future of healthcare	Blockchain is a shared distributed digital ledger technology that can better facilitate data management, provenance and security, and has the potential to transform healthcare. However, it's conceptualization, development and deployment must consider actual healthcare needs from the diverse perspectives of consumers, patients, providers and regulators
7. Mehta and Pandit (2018)	Precision Health	Concurrence of big data analytics and healthcare: a systematic review	There is a paucity of evidence of real-world use of Big Data analytics in healthcare because usability studies have only considered qualitative approaches, and a majority of the studies were from developed countries which brings out the need for research on Healthcare Big Data analytics in developing countries
8. Rabah (2017)	Blockchain in Health	Review of Challenges and Opportunities for Blockchain Powered Healthcare Systems	Blockchain is immutable, time-stamped, tamper-proof ledger, accessible by all or preapproved participants and hence provides efficiency, security and privacy

Reference	Category	Title	Extract – quotes
9. Shuaib et al. (2019)	Blockchain in Health	Blockchains for Secure Digitized Medicine	Decentralized, distributed, without the need for a third trusted party (TTP), characteristics of blockchains are used to solve issues of cyberattacks could benefit healthcare systems and empower personalized medicine
10. Singh et al. (2020)	Blockchain Implementation	Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities	Theorem Proving and model checking are the most common formalization techniques used to verify security properties
11. Siyal et al. (2019)	Blockchain in Health	Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives	Blockchain provides personalized, authentic, up-to-date and secure healthcare by merging real-time clinical health records
12. Vazirani et al. (2019)	Blockchain in Health/ Implementation	Systematic Review of Implementing Blockchains for Efficient Health Care	Blockchain could create a mechanism to manage access to EHRs stored on the cloud and increase interoperability while maintaining privacy and security of data. It contains inherent integrity and conforms to strict legal regulations
13. Wynn et al. (2018)	Precision Health	The Patient in Precision Medicine: A Systematic Review Examining Evaluations of Patient-Facing Materials	Precision medicine (PM) has the potential to tailor healthcare to the individual patient by using their genetic information to guide treatment choices However, this process is complex and difficult to understand for patients and providers alike. it is evident that more work must be done to ensure that patients can engage in their care when faced with PM
14. Xia et al. (2017)	Blockchain in Health	Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments	Private, permissioned blockchain-based data sharing framework that addresses the access control challenges of sensitive cloud data using immutability and built-in autonomy properties
15. Yaeger et al. (2019)	Blockchain in Health	Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure	Potential applications of the blockchain in medicine include interoperable health data access, data storage and security, value-based payment mechanisms, medical supply chain efficiency, amongst others. While nascent, it is essential the healthcare community understand the fundamental concepts and potential impact on the future of healthcare

Figure 1 is a word cloud produced by Nvivo using PDF documents of the references listed in Table I. In terms of coverage, it is clear that the representative set of review articles have focused on topics central to our review. Using a synonymic, term-matching algorithm, Nvivo produced the following thematic links across the 15 articles reviewed: “health”, “blockchain”, “research”; “technology”, “system”, “process”; “data”, “information” and “process”. This is indicative of the scope and representative coverage of the review articles. Although there were differences in the clouds produced from the three categories of review articles, they were not salient. As our research focus is specifically about the security and privacy functionalities inherent in Blockchain, we examined the coverage of “security” and “privacy” in the 15 articles by generating word-trees (see Online Appendix 1, electronic or digital copies are available from the corresponding author). While not as central as the themes listed above, we may claim face and construct validity in that security and privacy were well-linked within the discussions of the 15 review articles. Primarily, of deepest and most direct interest for this meta-review, we were able to derive key Blockchain design attributes and their support in the review literature from the Nvivo-generated word trees of security and privacy (Table II). Each of the five attributes – transparent, traceable, tamper-proof, immutable and compliant – shall be utilized in the field research. Outside the scope of digital health, Zhang *et al.* (2018) have reported that transparency, traceability and immutability are among the fundamental considerations towards more secure

Blockchains. For brevity, the five attributes of Blockchain shall be collectively referred to as 3TIC.

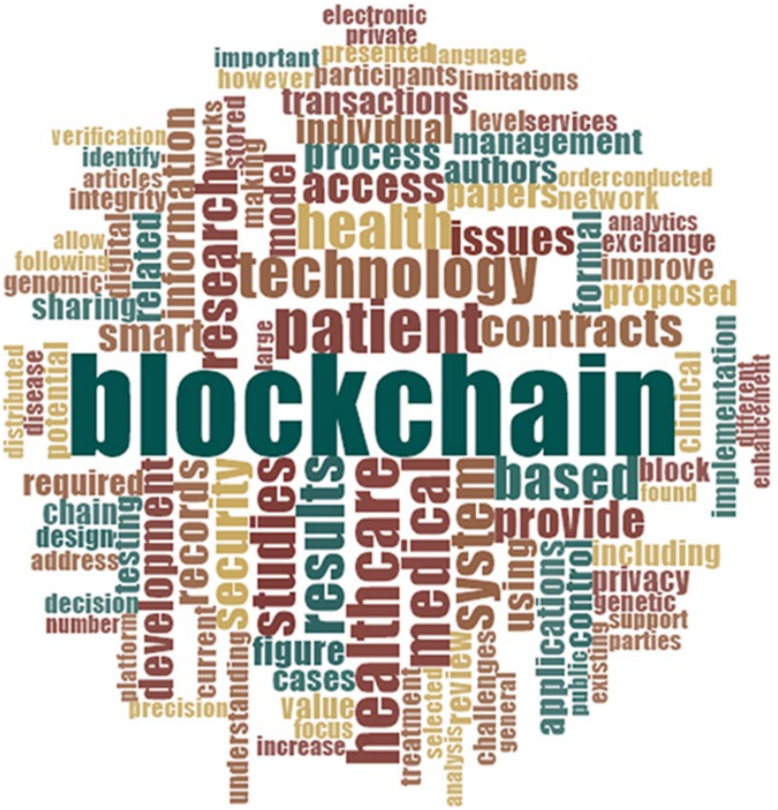

Figure 1. Word cloud of key terms used in blockchain research

Table II. Deprivation and support for blockchain 3TIC attributes

Design attribute	Brief description	Support [as listed in Table I]
Transparent	RWED accesses to data in blockchain are visible to all (public, permission-less) or authorized (private, permissioned) users	[1–15]
Traceable	Logs and audit trails of any RWED access to data in blockchain	[1, 3, 6, 8, 10, 11, 14]
Tamper-proof	Consensus algorithm prohibits any WED changes to data […] new data must be approved by consensus	[6, 8, 12, 14]
Immutable	The bockchain itself (data, links, etc.) is encrypted and cannot be edited nor deleted	[1, 6, 8–12, 14]
Compliant	SC will not execute any transaction that violates agreed data protection policies of the blockchain	[1, 6, 9, 12, 15]

To sum up, there is considerable agreement that Blockchain could bring a technically feasible improvement to the outcomes of PHC since it relies on an element of trust, satisfies the “big” needs of genomic data and significantly depends on higher opt-in rates of patients. Rabah (2017) suggests that the immutable, time-stamped, tamper-proof functionalities of Blockchain provides “efficiency, security and privacy” in patient care. However, such a claim has yet to be tested in large-scale implementations of PHC. The security and privacy attributes of Blockchain could provide considerable value to the health eco-system by providing a trusted environment, reducing unnecessary processing and decreasing its cost (Brakeville and Perepa, 2017). But again, the "how" question of such a design claim has yet to be addressed. More specifically, how can the distributed, decentralized and non-TTP nature of Blockchain address the security and privacy considerations of PHC? This remains a fundamental research gap. In Sections 35, the SSM approach to exploring such a solution is described.

3. Field research method

PHC ecosystems are complex and involve multiple "clients" (users), "actors" (stakeholders), "purposeful activities" (clinical protocols), "work-views" (health outcomes) and "environmental constraints" (ethics, policy, legislation, etc.). In such a context, the Soft System Methodology (SSM) appears appropriate for action research which helps to clarify ill-defined system requirements (Checkland, 1995, 2000; Checkland and Scholes, 1999; Staker, 1999). Over a 30-year period, it had been applied to hundreds of complex projects including diverse design challenges such as the Concorde Aircraft and the National Health Service in the UK. SSM originated from "systems thinking" and is an element of research which "concentrates on situations in which people are trying to take action" (Checkland, 2000, p. S41).

SSM is suited for investigating "purposeful action to change world views", namely, how Blockchain could enhance trust in a PHC eco-system and hence increase opt-in rates for the good of all. A key feature of SSM is the expression of significant requirements through the drawing of rich pictures, which follows the stages of the model's root definition and operating framework (Checkland and Scholes, 1999). The resulting artefact is then tested by applying the derived solution in a production environment. The model construction was accomplished by conducting interviews with key stakeholders to examine whether the proposed Blockchain-based ecosystem would address the "problematical situation" of low opt-in levels. Such an approach to field research which incorporates "case based reasoning" is well established in the field of health-care (cf. Andersen *et al.*, 2019; Laurenza *et al.*, 2018). It is also not inconsistent with the socio-technical approach (cf. Palvia *et al.*, 2001) which considers a system intervention such as technology, in the wider context of the tasks, organizations and stakeholders involved.

Figure 2 shows a "rich picture" of the SSM approach. Overall, SSM consists of four milestones (Checkland, 2000) across the seven steps originally identified by Checkland (1995). Descriptions of the procedures remain beyond the scope of this paper. In summary, Steps 1 and 2 fulfil the first milestone of finding out a "problematical situation" using techniques such as "rich pictures". Steps 3 and 4 fulfil the second milestone of formulating some relevant "purposeful activity" models. Step 5 fulfils the milestone of using the models for debate and discussion with the objective of achieving feasibility. Steps 6 and 7 fulfil the milestone of taking action to improve the situation. It should be noted that the milestones of SSM are consistent with Design Science Research (DSR) approach synthesised by Peffers *et al.* (2007): problem identification and motivation, definition of the objectives for a solution, design and development of artefacts, demonstrations of prototypes or proofs-of-concept, evaluation against key success criteria and communication of the design specifications to stakeholders. The seven steps of SSM may also be viewed from the lens of the classic relevance-rigour-design cycles of DSR earlier proposed by Hevner *et al.* (2004). In a retrospective journey, Checkland (2000) acknowledged the holistic consistencies between SSM and other offshoots of DSR such as Systems Theory and Design Thinking. While the later focus on the development of design artefacts such as UML diagrams, prototypes and source codes, SSM primarily addresses the specification of a feasible solution for the problem being considered.

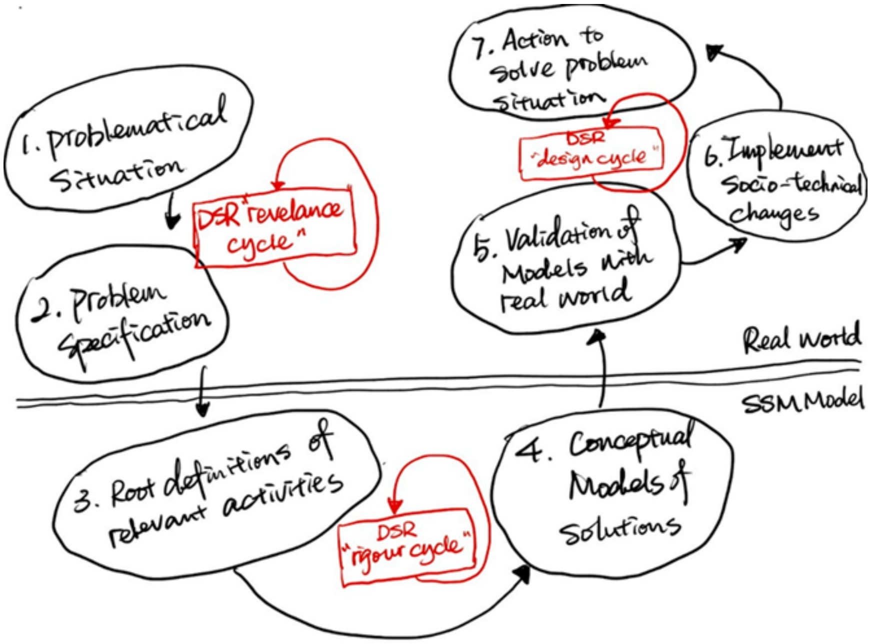

Figure 2. Using the soft systems methodology for PHC

The problematical situation here is the low "opt-in" of patients to a PHC offering. The design challenge is whether a Blockchain-enabled SC would alleviate the hesitancy of stakeholders (mainly patients) to share their EHRs including genetic sequencing. Using an SSM approach therefore requires addressing some key questions to major stakeholders such as patients, doctors, health administrators and policy-makers. A key element of SSM is the design discussion, which Checkland (1995) suggests is an effective means of modelling purposeful activities so as to discover desirable and feasible changes in system features and requirements (also see Libakova, 2015). Compared to large sample methods, the input from such interviews is more reliable and valuable as these are obtained from informed and engaged industry professionals (Dorussen *et al.*, 2005). It is also effective for comparing a proposed solution (ie Blockchain-enabled PHC) with the current problematic situation with low opt-in rates in order to extract valuable insights for improvement (Littig and Pöchhacker, 2014).

In accordance with the research ethics approval obtained for this study, a detailed "call for participation" was sent over e-mail to possible clients and actors who were informed and willing to contribute their time and inputs. The e-mail included background information on PHC, Blockchain and the design interview template (see Online Appendix 2, electronic or digital copies are available from the corresponding author). It is critical to establish that validation of an SSM study very much depends on identifying "lead" users and actors who could articulate issues, challenges and latent needs in a credible manner (Checkland and Poulter, 2010). Seven carefully vetted interviewees across different roles within the healthcare industry (two patients, two providers, one District Health Board (DHB) administrator, one PHC vendor and one health policy analyst) consented to giving their comments and inputs to the design of the Blockchain-enabled PHC. In accordance with the systems thinking school of thought, design interviews, workshops and focus groups are intense, creative activities which are deliberately kept to a certain length of time; quality takes precedence over quantity (Hanafizadeh and Mehrabioun, 2018). Our design interviews, each lasting up to 2 h, were conducted in a set sequence whereby each patient and then each practitioner was interviewed to give a generalist, high level input as “clients or customers” of a Blockchain-enabled PHC. As interviews proceeded to involve the “actors” – administrator, vendor and analyst, they took an increasingly more PHC-specific focus. The use of SSM visual techniques were augmented by UML tools (specifically, activity and use-case diagrams, cf. UML, 2017) for the purpose of exploring, communicating and clarifying design ideas, thoughts and enhancements.

The rich pictures and activity diagrams that were developed as design artefacts were based on a use case of New Zealand’s universal-access healthcare ecosystem (Gauld, 2016). Along with a brief overview of the scope and objectives of the research and an introduction to Blockchain technology, rich pictures served as the starting point to a discussion with interviewees about Digital Healthcare, PHC and Blockchain. Each interviewee was then “walked through” the contextual background of Blockchain-enabled PHC at the onset of each interview. Four typical health scenarios were selected by the research team in consultation with a domain expert as key business processes for PHC: registering a smart contract (enrolment); seeking clinical services (consultation); model building and validation (diagnostics); and performance monitoring of health outcomes (evaluation).

It is salient that Vaishnavi and Kuechler (2015) referred to DSR as an improvement method. The essence of approaches such as SSM, DSR or agile is the improvement of a solution’s design. The SSM steps taken to develop such design artefacts are discussed in the following sections. More specifically, Section 4 delves deeper into our understanding of the problematic situation which includes “rich pictures” of key scenarios, and explores a “root definition” of a Blockchain solution. Section 5 describes the iterative refinement of design artefacts when put through design interviews with stakeholders and the exploration of a feasible solution.

4. Problem specification of Blockchain-based PHC

4.1 Problematic consideration

The current challenge is that low opt-in rates and a lack of trust around genetic data sharing by patients leads to weak models and diagnostics. “Trustworthy” systems could reduce such concerns and increase patients’ willingness to participate in data sharing (Brodersen *et al.*, 2016). It is also known that there are significant ethical, legal and social implications of incorporating personalized medicine into healthcare. Brothers and Rothstein (2015) have analyzed the consequences of the significant increase in health information that will be brought about by personalized medicine and raise concerns about the potential of personalized medicine to exacerbate existing disparities in healthcare until and unless they are universal in scope and coverage. Therefore, our principal design postulate is that attributes of Blockchain such as transparency, traceability, tamper-proofing, immutability and compliance may mitigate against the current lack of trust in PHC services, especially with respect to the protection of genetic data, and bring about better cost and treatment outcomes.

4.2 Issues expression (rich pictures)

As described, SSM calls for hand-drawn illustrations as an aid to specify system requirements. In the case of the current context of PHC in New Zealand, Figure 3 shows such a “rich picture”. It was Checkland’s suggestion (cf. Checkland and Scholes, 1999) that such rich pictures provide a summary overview of the problematic solution as well as the iteratively enhanced solution. Typically, the SSM practitioner engages with system stakeholders to derive their “world views” of an existing system or eco-system and determine consensus on what the problematic situation is.

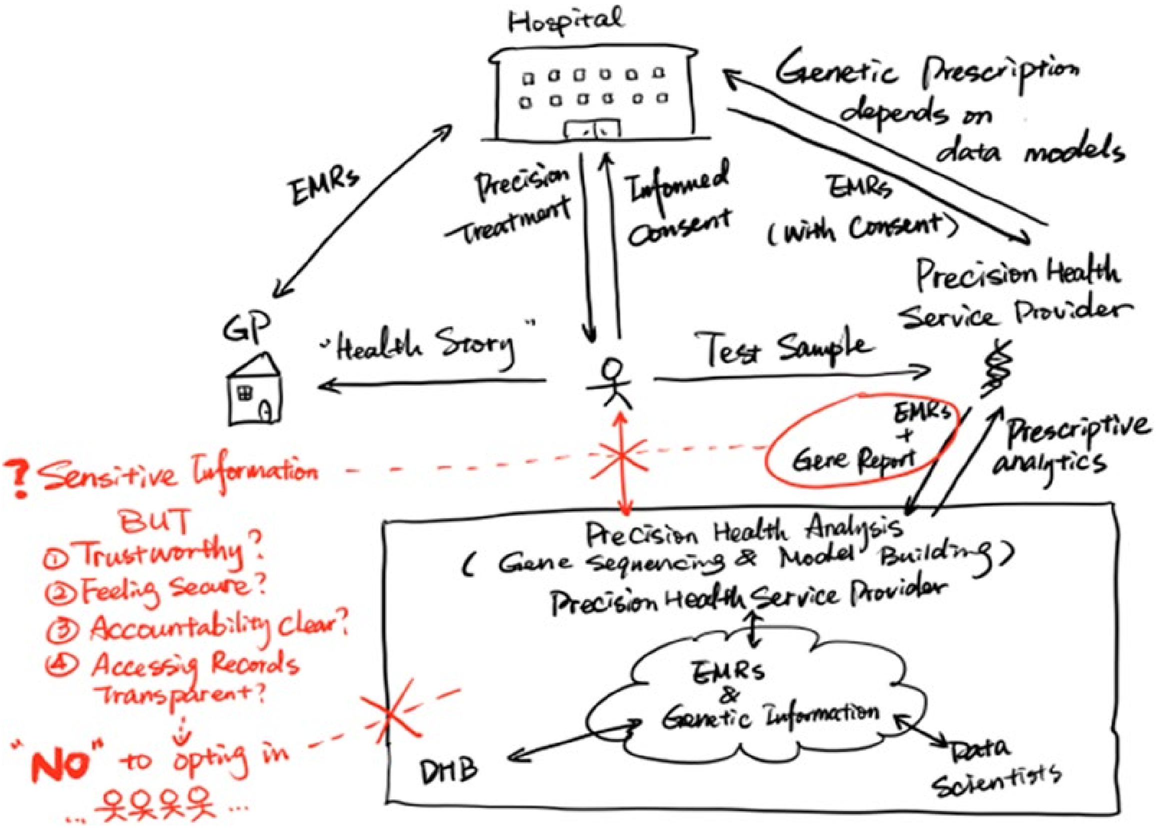

Figure 3. Problem expression and world-views of stakeholders

As previously mentioned, the healthcare eco-system of New Zealand was chosen for reasons of convenience as well as suitability. Currently in pilot stage, NZ’s PHC is based on a standard EHR architecture where every patient who opts-in is identifiable with his or her unique National Health Indicator (NHI). The benefits of an integrated, interoperable PHC-based EHR repository has yet to be introduced country-wide and each DHB operates its own “fire-walled” databases and models (Huang and Dobbie, 2017) using different standards, protocols and systems. Thus, data transactions are time-consuming and various security measures need to improve in order to deal with the redundancy of maintaining separate EHRs across DHBs. Moreover, the patients’ control over their own information is very limited (cf. Privacy-Commissioner, 2011). Research suggests that the rights of patients in granting data access privileges is a major contributor to their willingness to share their EHRs or EMRs (Patil and Seshadri, 2014; Kshetri, 2018). From a system level perspective, opting into PHCs could reduce time and costs for both patients and healthcare providers. For the patient, knowing possible health treatments and outcomes could be proactive preparation before a clinical visit (Shah *et al.*, 2014). However, these benefits have not been sensed by key stakeholders. Besides ownership, patients' concerns over information privacy and security in the PHC context are longstanding (Lunshof *et al.*, 2008) and not easily overcome by assurances. Therefore, improved patient control of their health records and security appear to be key design challenges.

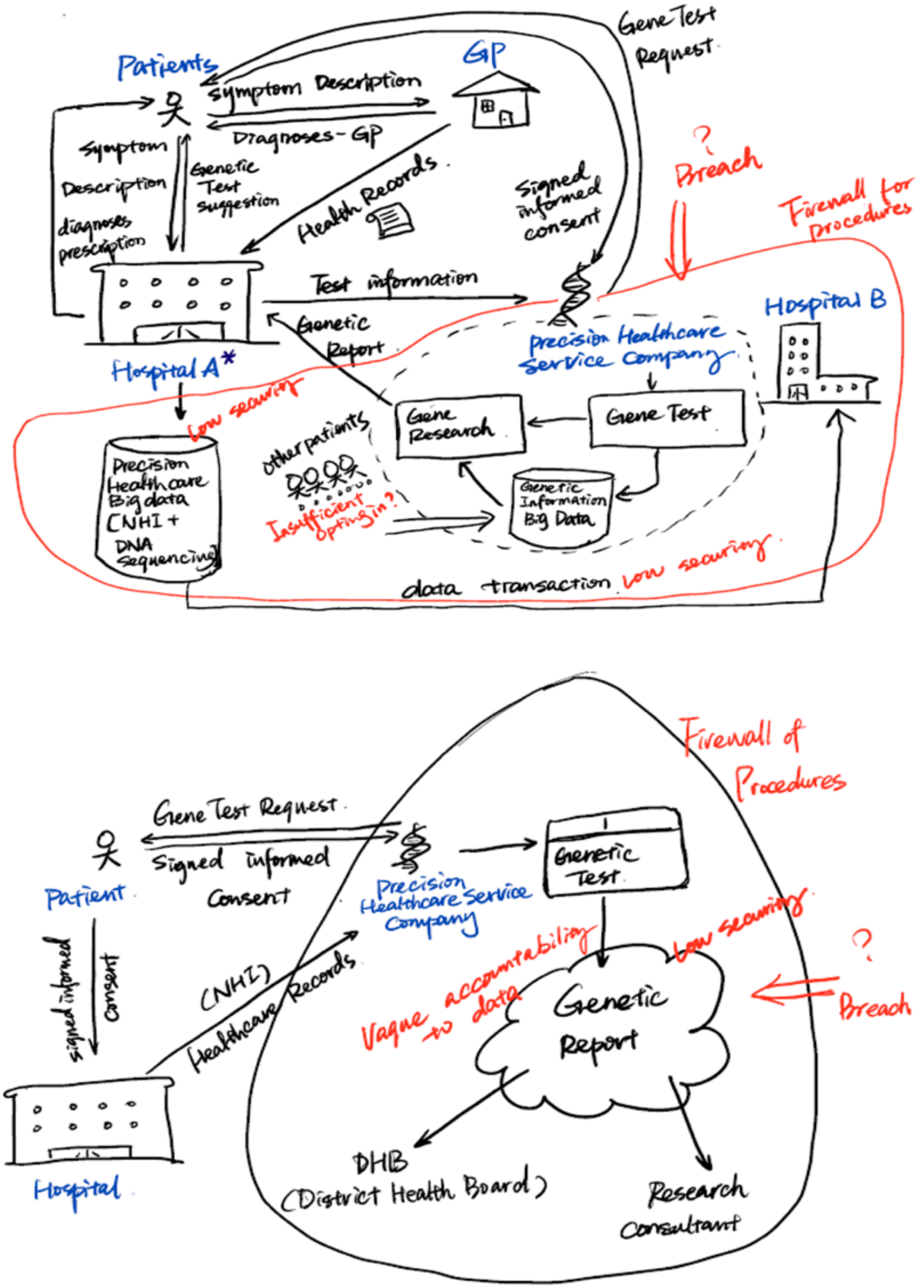

Figure 4. SSM modelling and specification with rich-pictures

Figure 3 illustrates the present ecosystem of PHC in New Zealand as derived by applying SSM. The annotation in red refers to the “problematic situation” from the perspective of key stakeholders that were obtained from the design interviews. The patient first visits a General Practitioner (GP) whenever he or she requires medical attention. By transcribing “health stories” onto the patient’s EHR, GPs primarily evaluate the patient’s health condition and either prescribe medication and treatment or, refer the patient to a hospital for advanced diagnostic tests, specialist care or admission. Within a DHB, the EHRs of the patient are accessible by health practitioners at the hospital. Since NZ is still in the process of implementing a country-wide health records database with NHIs as primary key, there are “islands of automation” with each DHB piloting its own PHC. A key assumption was made of the desirability of a country-wide PHC platform.

During a “consultation”, “enrolled” patients who have opted-in to PHC pilot trials are asked for consent on sharing genome information for the benefit of precision medicine (e.g. treatments for cancer, heart diseases, diabetes, etc.). In some cases, the DHB may need to recruit the patient for genetic research. This, too, requires informed consent. After diagnosis, the test result(s) are sent to PHC service providers, along with redacted EHRs (ie non-PII data) but only their medical information. Currently, patients and their primary providers access PHC services for serious health conditions only. It was evident from our interviews that patients are not being informed about how their data is used for genetic sequencing models and predictive analytics, though such PII is more sensitive than other EHRs. Such types of uses often violate the transparency principles of Fair Information Practices (Teufel, 2008) which established principles for addressing privacy concerns, consistent with the data protection expectations of contemporary societies (Rubinstein, 2013). It is salient that user data in Blockchain are controlled with private and public encryption keys which give patients control over access rights to their EHRs + genetic sequences.

For each of the four scenarios, “rich pictures” co-created, clarified, improved and refined during design interviews were means of obtaining a shared “worldview” as well as an understanding of a “problematic situation” for which design solutions could be formulated. Figure 4 shows rich pictures developed from interviews for two of the four scenarios – “consultation” (top) and “diagnostics” (bottom). Problematic issues with current PHC pilots are again annotated in red. It is clear that the protection of sensitive genome data requires a robust infrastructure with enhanced security. Discussing the four scenarios in sequence across interviews provided for a systems approach to problem modelling as well as solution specification. They were not static but, with successive interviews, dynamically evolved towards the design of a feasible solution. Prior to the formulation of a design solution, the “root definition” of “purposeful action” is more formally stated in Section 4.3.

4.3 Root definition

In SSM, the root definition is the first step towards developing a “purposeful system”. It comprises notations for the required specification that supports a verbal description. From a security standpoint, several field studies (e.g. Abouelmehdi *et al.*, 2018) have shown that systems with a centralized architecture comprising data warehouses are more vulnerable to cyber-attacks, often resulting in data loss. Therefore, to improve the security features of a healthcare system, a distributed architecture could be feasible, whereby service providers would be able to replicate EHRs from hospitals within a DHB. This minimizes the risk of failure and other hazards derived from complicated data-intensive activities and processes (Xia and Song, 2012). Developing a Peer-to-Peer configuration (such as a Blockchain) to shorten the route of data flows is another workaround. Another key design feature is patients' autonomy over their own genetic information and control over its use within a PHC eco-system. Hence, patients will be able to monitor the access, authorize and account for their EHRs in a transparent, traceable and tamper-proof manner. Compliance through programmable SCs can be enforced as per legal provisions. They could also have oversight of data accesses, which should be immutable. In the absence of a TTP authority, Blockchain functionalities can audit the "actors" and their "activities" with each chain of transactions immutably recorded so as to clarify the accountability of legitimate actions (Caulfield *et al.*, 2008).

As a consequence of identifying the "problematic situation", a programmable "informed consent" which may be implemented by the functionality of a "smart contract" was proposed as a design solution. With a smart contract, signing an informed consent should be the precondition to sharing patients' EHRs + genetic information. In other words, it is an agreement between the patient and data accesses. Hence, all re-use of data will trigger execution of the SC. Each execution being transparently, traceably, tamper-evidently and immutably recorded to assure that patients' data are used in accordance with the SC. Trust is enabled through the comprehensive tracking of data read, write, edit and delete operations and enhanced by validating such operations, either in real-time or batch audits, against the SCs. Hence, the role of SCs as key mechanisms which provide security and privacy to PHC emerged as a key requirement of a solution for the problematic situation. The next step in SSM is to explore key design functionalities of a Blockchain-enabled PHC.

5. Solution design of Blockchain-based PHC

The design of a solution and its validation is a check of whether the design artefacts are acceptable and useful for addressing the challenges identified (Peffers *et al.*, 2007). In SSM, relevance is the key aspect of design validation (Checkland, 1995). It can be learned through listening to and analyzing stakeholders' world-views about the problematic situation and proposed solution. Such an analysis entails both a reflection of issues in the real world and the values of stakeholders (Hanafizadeh and Mehrabioun, 2018). As design input was collected through several role-specific interviews across the healthcare eco-system, the generalization of world-views using procedures and techniques discussed in Section 3 is consistent with scholarly practices (Dorussen *et al.*, 2005). The resulting solution is presented in this section.

5.1 Analysis of models with real world

In general, stakeholders interviewed showed similar concerns towards the adoption of PHC as the literature review had revealed; namely, the key attributes of security and privacy that could be addressed by Blockchain. Further, they understood why low opt-in rates result in weak and imprecise analytic modelling and hence treatments. This was seen as a logical consequence of concerns over trust in the protection of genetic and other health records. The weak data transparency and lack of controls of current PHC services were consistently mentioned across interviews. In short, the world-views of stakeholders converged on the link between trust and patients' choice of opting-in to PHC.

Using the CATWOE technique from SSM, which allows a high-level specification of a complex system's "purposeful action" in terms of its key parameters, such a description of the PHC eco-system is given in Table III. In the PHC eco-system, CATWOE allowed the first-cut identification and subsequent clarification of players, their roles and the values they create and capture. A key design feature of Blockchain-enabled PHC platforms is the notion of Smart Informed Consent by patients for access rights over their health records and genetic information (EHR+). Clients and actors could appreciate that these mechanisms would improve security and privacy in the practice of PHC. Moreover, the technical foundation of the SIC, comprising a programmable pre-approval of which actors could access patients' EHRs + genetic sequences, was accepted. It was evident that the immutable tracking of distributed hyper-ledgers and tamper-proof Blockchains would enhance data transparency. Hence, security concerns could be reduced through the SIC-authorized, tamper-proof, RWED accesses to PHC data. A prototype SIC class diagram is beyond the scope of this study. However, in the exploratory design of an SIC solution, a more granular setting option which includes the RWED access type and time limit was constructed. Some default settings are necessary to implement the pre-emptive tracking of policy violations and compliance of service-level agreements.

Table III. CATWOE of blockchain-enabled PHC

Clients	Patients
Actors	Patients, Providers, Vendors, Payers, Regulators – eco-system perspective Accessors, Participants, Miners – EHR perspective
Transformation	Educational Module in SIC before Patient enrolment Patient-Centered SIC compliant with Medico-Legal Policies Transparent, Traceable, Tamper-proof, Immutable EHR Flows for Compliance Auditing Hybrid Distributed Hyper Ledger: Blockchained SIC Integrated with Off-chained PII EHR Database Clear Metadata Established for the Separation of PII and aggregate models & data
World View	Improving Security and Privacy in order to Enhance Trust and Opt-in rates Raising the Knowledge Level of Patients about Security and Privacy Rights Eliciting Informed Consent for Patients' opt-in and Access Control Reliable and Trusted Regulatory Monitoring
Owner	Health Ministry & DHBs (www.health.govt.nz/our-work/digital-health)
Environment	Governing Private, Permissioned (Consortium) Blockchain
Constraints	Legislation of Data Protection and Medical Ethics – Genetic Data abuse, Incentive Mechanisms, Emerging Technologies for 3TIC

In such a participative, empathic manner, an improved "enrolment" process of SIC's content structure was derived. A "design snapshot" is illustrated as a UML Activity Diagram in Figure 5. Recall that this is the first of four scenarios being explored and serves as an example of how the other three scenarios were similarly discussed. From these iterations, caveats emerged, such as the need for a manual over-ride in exceptional cases (e.g. emergency situations where access was required by providers not pre-approved). The point being made is that design interviews traversed a level of complexity and fuzziness that were not as neat as the UML diagrams might suggest.

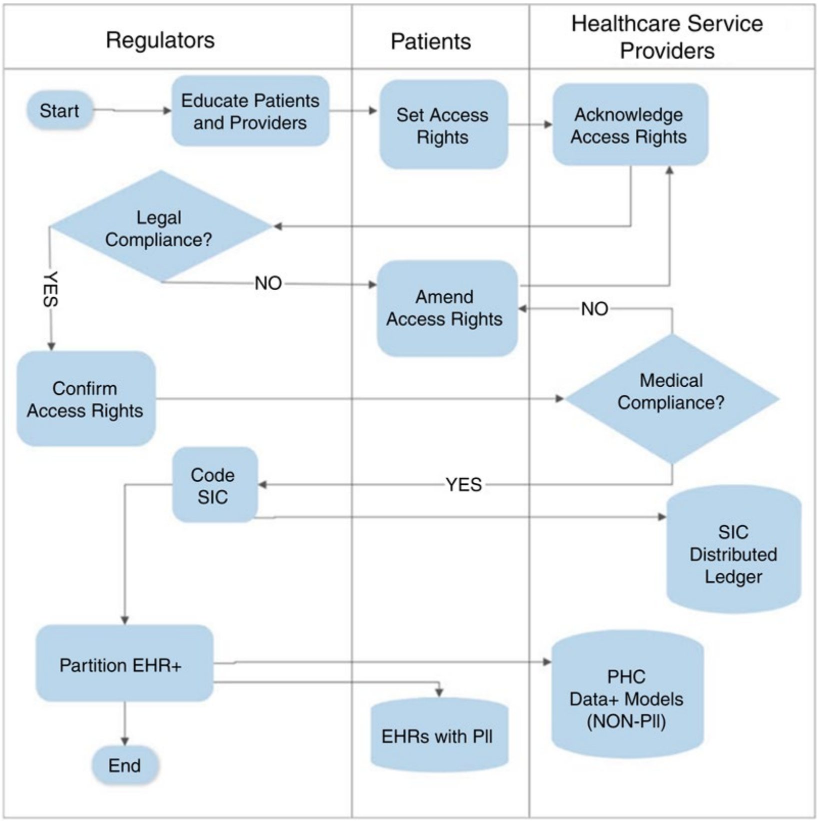

Figure 5. Activity diagram for registering a smart contract (enrolment)

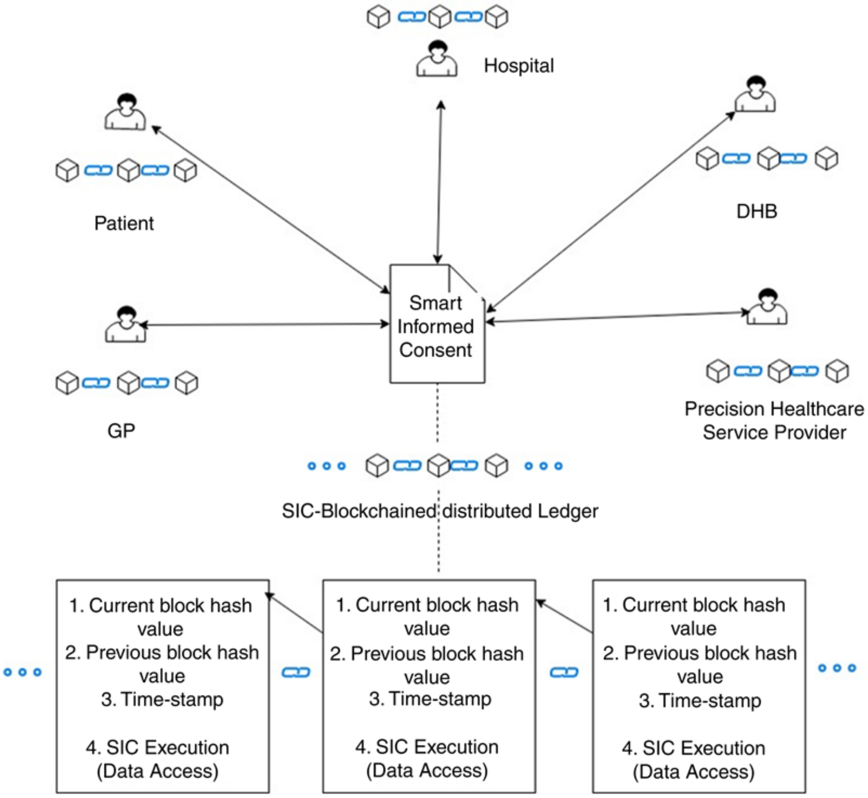

Figure 6. Deployment diagram of authorization setting of SIC

Figure 6 illustrates the SIC interface to clients (Patients) and Actors (Practitioners, Administrators, Vendors) and Figure 7 is a Use-Case Diagram of an SIC-enabled, Blockchain-based PHC. Again, both were generated as design artefacts in a participative, iterative manner for the purpose of exploring, communicating and clarifying how the 3TIC design attributes of Blockchain could enable patients to exercise their rights to data security and privacy. In Figure 6, each block contains the current hash value, the previous block's hash value, time-stamp and application-execution records for RWED access. No records could be edited or deleted (unless explicitly allowed by the regulator), which guarantees the authenticity of each access transactions. The integrated ecosystem of SIC with PHC is illustrated as a Use-Case in Figure 7, where patients have full access to their health + genetic data while other actors have different accessing authorization as per the set medical and legal restrictions. The SIC enforces compliance to such policies.

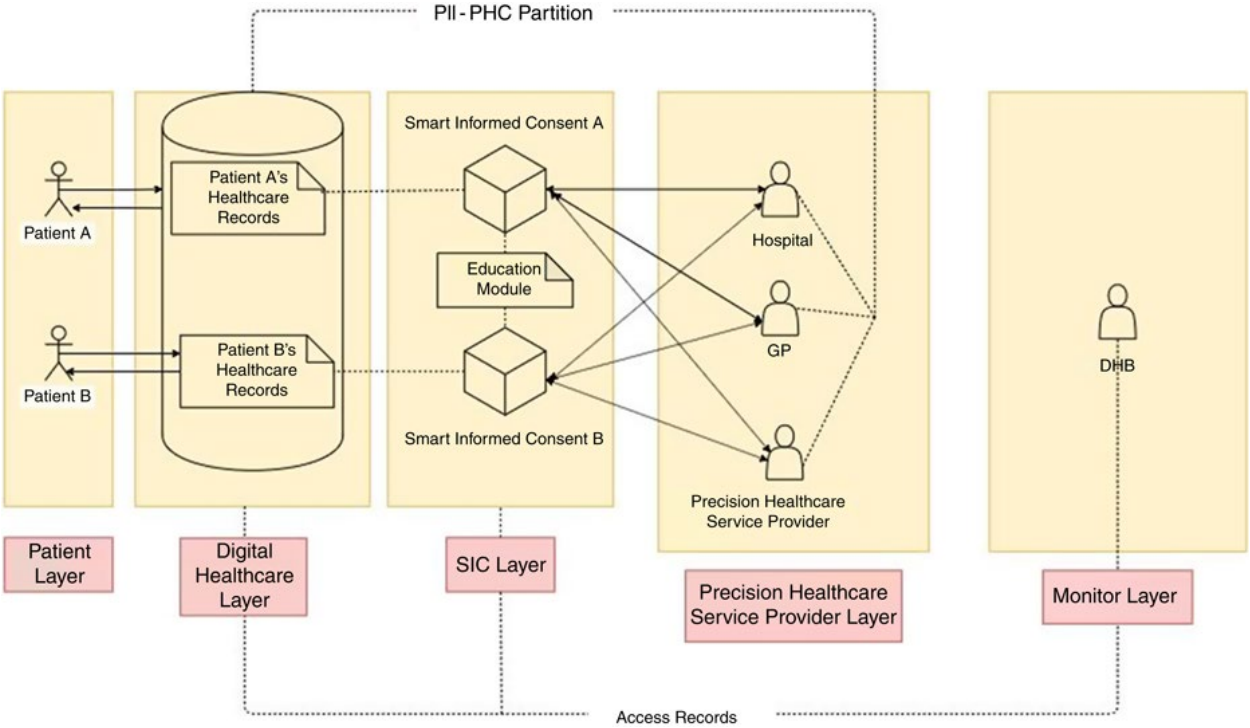

Figure 7. Integrated use case diagram of PHC incorporating SIC

A critical design consideration that emerged was the partititioning of PII and non-PII components of EHRs, expecially genetic information. Personally identifiable data and information are very sentitive aspects of the design of PHCs. Both the European Union (https://gdpr-info.eu/) and the United States (*de facto* – https://medium.com/golden-data/a-guide-to-the-californiaconsumer-privacy-act-ccpa-3a916756ed36) have enacted laws that govern PII security and privacy service obligations. Hence, legal, medical and user requirements were for PII to be "off-chained" to the DHBs, providers, payers or patients.

To illustrate further, the UML artefacts elicited much discussion about the design of adequate SIC controls over the setting of authorisations and access rights in the "enrolment" scenario. This corroborates Halim's (2019) suggestion that: "To share aspects of their data, and to control who has the ability to search or contact them, individual users can simply adjust their permission settings using a so-called ‘dynamic consent platform’, a next-level access control mechanism for healthcare data. The more data there is, e.g. from electronic medical records, genomic data, streamed from wearables or other personal health records, the more need there is for data privacy and access control”. Addressing this aspect, several design ideas and inputs followed from the interviews, captured and refined with these diagrams. It was suggested and affirmed that in order to encourage patients to opt-in to PHC with effective incentive mechanisms, the fear of data sharing should be addressed through “strict, legally-enforcable” SIC controls. Such a shift in the world-view of patients is non-trivial. It should begin with education, defining how PHC could be a public good for the efficient and effective delivery of health services whose benefits accrue to all.

Low adoption of Blockchain has been attributed to the lack of education and awareness of its capabilities (Clohessy and Acton, 2019). However, it is was recognized that education and appealing to altruism may not suffice to significantly increase “informed consent”. Considering the externality of healthcare services, an incentive scheme in the form of trust assurance could be effective in dissuading asymmetric opt-ins and free-riding. On the subject of security and privacy, several world-views pointed to the primary importance of the regulatory role in the ecosystem in order to enhance trust. The argument was raised that enforcement agencies should play a key role in the system to monitor the entire set of functionalities and processes. Regular traceable and tamper audits on SIC compliance must be transparently undertaken by trusted certificate authorities to ensure that PHC services function in compliance with prevailing policies. With reference to the back-end infrastructure of the PHC eco-system, there should be an integrated cloud storage for EHR + genetic sequences. This would be a logical progression to storing country-wide healthcare data on the hyper-ledger of Blockchain.

Such an eco-system may not, as yet, be cost effective, considering the massive data and computational redundancy required in a Blockchain solution. Hence, it will be a great challenge for existing islands of EHRs to migrate to hyper-ledger platforms. Another design idea that emerged was the storing of EHRs “off-chain” in traditional databases while establishing pilots of Blockchain-based SICs as a good starting point. Such a workaround design would have the added benefit of protecting the EHR+ hyper-ledger by keeping the “key” and EHRs secure. Every use of the key could be monitored and RWED transactions would be immutable. Suspicious accesses would be flagged in real-time.

5.2 Design changes and improvements

Based on the design considerations that has emerged, we may logically reason that an effective SIC would reduce the security and privacy concerns of users. Specifically, with respect to the assurance of the “3TIC” design attributes in provisioning security and privacy for PHC. Hence the conceptual feasibility of our proposed solution was established. SSM is more amenable to theory exploration with conjectures such as principles and rules than theory construction with hypothesis. In that sense, the design principles and rules presented are postulates. In the nomenclature of design research, principles are over-arching considerations within which more specific, “how-to” rules may be specified.

Figure 8 captures the fundamental theoretical findings of this exploratory design study in a summary manner. The cardinal design principle for PHC is that security and privacy is enhanced with such functionalities as the 3TIC design attributes of Blockchain. The distributed, decentralized and non-TTP characteristics of Blockchain allow patient-control of access and the off-chaining of PII. Following from this is the principle of confidence and trust which may be fulfilled by first educating stakeholders on the feasibility and limitations of such a solution, and next enforcing the monitoring and compliance of patient-approved SICs. Finally, the principle of demonstration will require that effective PHC outcomes such as lower costs and better treatment must be transparently monitored and validated by trusted authorities so as to promote further adoption. In a nutshell, the extent to which 3TIC design attributes of Blockchain are effectively implemented, leads to corresponding levels of security, privacy and trust.

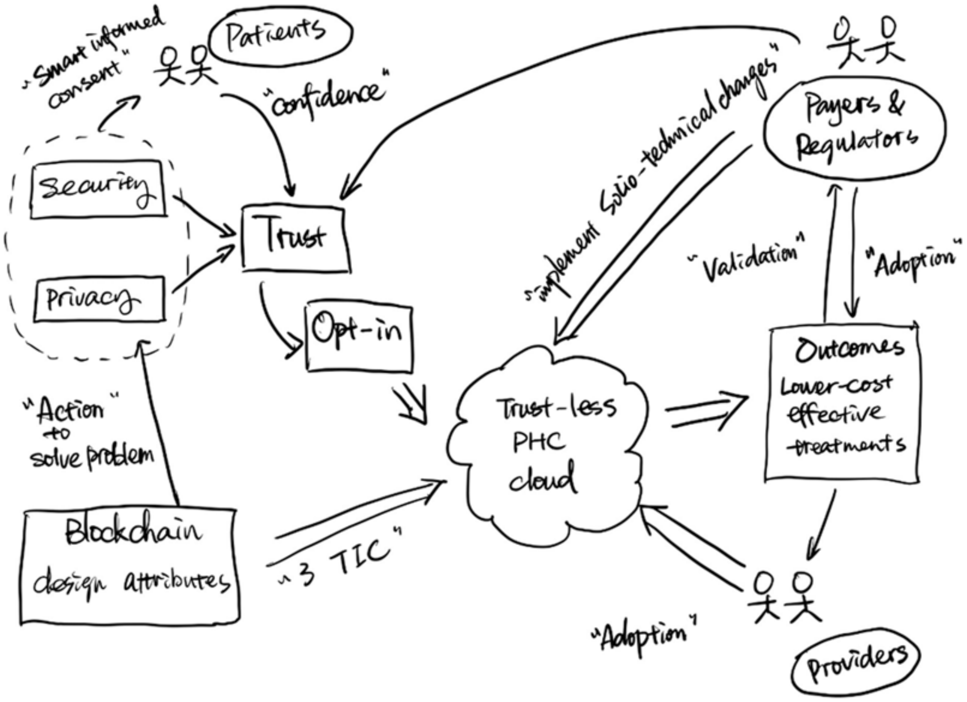

Figure 8. "Real-world" blockchain-based PHC solution

The findings of this study were separately presented to officials of the Canterbury DHB and Callaghan Innovation (www.callaghaninnovation.govt.nz/ – part of the NZ government which funds the commercialization of research). The solution was accepted in principle as feasible. Commitment was secured from an NZ-based health informatics start-up enterprise and funding was approved by Callaghan to refine and commercialize the design of a Blockchain-enabled PHC service founded on the design principles presented in this research. The research has thus entered a proprietary, developmental phase that represents *de facto* industry validation of design artefacts (Vaishnavi and Kuechler, 2015).

6. Discussion and implications

This paper has derived using SSM a set of comprehensive and parsimonious design rules for a Blockchain-based PHC augmented with programmable SCs. As current PHC eco-systems are not capable of justifying how or when patients' data or providers' diagnosis will be utilized, PHC remains an untrusted service to the majority of its potential beneficiaries. This is attributable not only to the subjective perceptions of patients, but also the realization that current practices are unable to provide for adequate security and privacy. As our study revealed, fear of data abuse in legal proceedings, insurance matters and employment prospects also remain patients' concerns. This finding corroborates prior research (cf. Abouelmehdi *et al.*, 2018; Bruynseels *et al.*, 2018; Xia *et al.*, 2017; Yue *et al.*, 2016). Related research also corroborates that Blockchain could be developed to improve the security and privacy levels of trust-less PHC platforms (cf. Agbo *et al.*, 2019; Park *et al.*, 2019; Shuaib *et al.*, 2019; Vazirani *et al.*, 2019; Yaeger *et al.*, 2019). Security and privacy breaches are persistent and costly (Ponemon, 2016) and patients' enrolment in PHC has not increased with its potential. As a consequence, the higher opt-in levels would improve the existing network effects and overall healthcare service level.

Given current sensitivities surrounding "state-sponsored surveillance and technology-driven authoritarianism", almost all the actors interviewed called for deep monitoring of PHC data, governance-assured by a designated authority (TTP?). This would be antithetical to the architecture of Blockchain platforms. Some key security policies should be set as laws and medical directives to regulate EHR+ usage and authorization in PHC eco-systems. It includes agreement on what constitutes meta-data, default data access setting, distinguishing RWED access authorization given to actors and access time limits. Finally, the ethics of incentivising opt-ins in order to discourage "free-riding" remained. Actors did not consider it to be socially acceptable that only clients who opted-in to PHC with their genetic sequences should be allowed the benefits of its predictive treatment and outcomes.

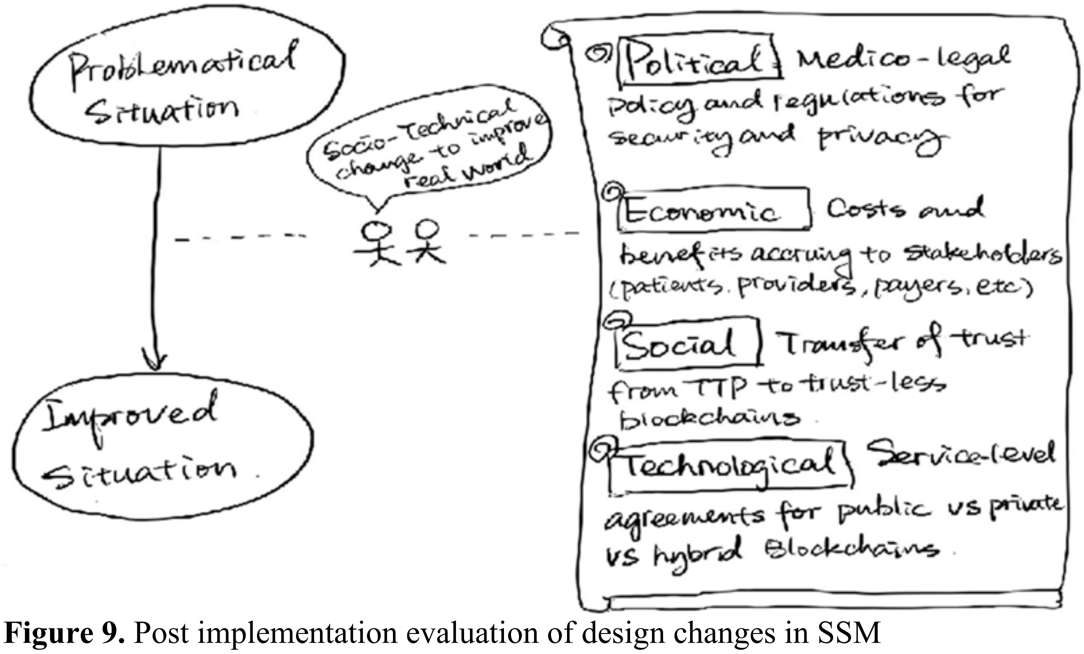

Figure 9. Post implementation evaluation of design changes in SSM

However, in order to be implemented in practice, further design refinements may be required in an agile, iterative manner. In his retrospective account of SSM, Checkland (2000) concedes that the methodology (as opposed to other design methods) was never intended to be academically rigorous but provide a systems thinking approach to action research that considers multiple perspectives and the macroreality of socio-political acceptance. In other words, the efficiency of design mattered less than its efficacy and SSM focusses on design exploration rather than theory construction. Based on Checkland's (2000, p. S34) guidelines, Figure 9 suggests some recommendations that need to be addressed when seeking changes to the problematical situation. Whilst security and privacy are hygiene factors, there are other divers of adoption (Clohessy and Acton, 2019).

Hence, we suggest several potentially fruitful avenues for future research. Using a PEST "world view", researchers could consider Blockchain-based PHC from a cost-benefit point-of-view by comparing such systems with non-Blockchain alternatives. Some examples of costs include direct costs associated with implementing Blockchain-based PHC as well as costs associated with potential security and privacy breaches. Estimates suggest that the costs to enter and store data in Blockchain systems are significantly less than those associated with cloud services such as AWS (Reynoso, 2017). In addition to economic costs and benefits, it would be important to look at non-economic costs and benefits such as the social costs of not sharing full health records with a PHC eco-system and psychological benefits associated with patients' confidence in the diagnostics of Blockchain-based PHC. The design of dashboards, benchmarking and prescriptive analytics are also worthy of research.

One limitation of this research was its scope that was limited to the modelling of New Zealand's healthcare ecosystem. As an emerging technology, use-cases of Blockchain in other domains of high impact (e.g. public services and food safety) would be important contributions to knowledge. Thus, this paper is positioned as an exploratory study to investigate Blockchain and its application in a significant context such as PHC. The issue of scalability has been noted as a major limitation of Blockchain applications (Shuaib *et al.*, 2019). The carbon footprint associated with large volumes of duplicate data and ensuing latency are symptoms of the inherent functionalities of the technology. Smart Contracts for off-chaining, partitioned and hybrid blockchains could be further specified to address the performance required by PHC. It would be contentious to explore if an incentive mechanism could be applied in a form like granting PHC coins (a crypto-currency that rewards data contributions that may be used as credits for PHC services) to increase the opt-in rates of patients.

Another area concerns a comparison of Blockchain-based PHC with current big data-based applications favoured by Managed Health-Care Organisations in terms of externalities and a "tragedy of the commons". For instance, it is argued that traditional big data-based applications allow scientists to use such data in research and improve human well-being. Huge volumes of patient data help detect drug interactions as well as design drug therapies. Some state and federal health information exchanges provide information on individual patients, which can contribute to effective drug regulation and cost reductions. They may also reduce indirect costs associated with lower precision (Zimmerman, 2019). Further research could examine how Blockchain-enabled PHC may potentially transform these sources of externalities, by shifting the locus of control from the institution providing healthcare to health consumerism from patients (Kshetri, 2018).

Finally, further research on the applications of emerging technologies in PHC could also investigate the development of PHC portfolios which "sense" patients' healthcare data from IoT and wearable devices, analyse them with genetic information and improve with powerful machine learning models[2]. If PHC opt-in rates increase with the incorporation of Blockchain and augmented technologies, the concept of a Digital Twin (Bruynseels *et al.*, 2018) could be a disruption in personalized healthcare equivalent to 3D printing in manufacturing. However, no matter the good intentions, the entry of genetic sequences into health treatments and outcomes must proceed with deep ethical reflection (Brothers and Rothstein, 2015). A critique of "good practices" across industry players and government policies would shed insights on the challenges and pitfalls of implementing EHR+PHC.

In closing, the research reported in this paper suggests that while there remain significant implementation issues for effective Blockchain-enhanced PHC, it is worthy of further research. We conjecture that the decentralized and distributed nature of Blockchain is congruent with the patient-driven design of PHC.

Notes

1. www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

2. See for example, recent WHO guidelines on digital health interventions: www.who.int/news-room/detail/17-04-2019-who-releases-first-guideline-on-digital-health-interventions

References

Abouelmehdi, K., Beni-Hessane, A. and Khaloufi, H. (2018), "*Big healthcare data: preserving security and privacy*", Journal of Big Data, Vol. 5 No. 1, pp. 1-18, doi: 10.1186/s40537-017-0110-7.

Agbo, C.C., Mahmoud, Q.H. and Eklund, J.M. (2019), "*Blockchain technology in healthcare: a systematic review*", Healthcare, Vol. 7 No. 2, p. 56, doi: 10.3390/healthcare7020056.

Andersen, K., Nielsen, J. and Kim, S. (2019), "*Use, cost, and digital divide in online public health care: lessons from Denmark*", Transforming Government: People, Process and Policy, Vol. 13 No. 2, pp. 197-211, available at: https://doi.org/10.1108/TG-06-2018-0041

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E. and Truscott, A. (2016), Blockchain: Securing a New Health Interoperability Experience, Accenture LLP.

Brothers, K.B. and Rothstein, M.A. (2015), "*Ethical, legal and social implications of incorporating personalized medicine into healthcare*", Personalized Medicine, Vol. 12 No. 1, pp. 43-51, doi: 10.2217/pme.14.65.

Bruynseels, K., Santoni de Sio, F. and van den Hoven, J. (2018), "*Digital twins in health care: ethical implications of an emerging engineering paradigm*", Frontiers in Genetics, Vol. 9, p. 31, doi: 10.3389/fgene.2018.00031.

Burniske, C., Vaughn, E., Shelton, J. and Cahana, A. (2016), "*How blockchain technology can enhance EHR operability*", available at: www.hyperledger.org/wp-content/uploads/2016/10/ARKInvest_and_GEM_Blockchain_EHR_Final.pdf (accessed 9 August 2018).

Buterin, V. (2014), "*A next-generation smart contract and decentralized application platform*", available at: www.fullhodl.com/wp-content/uploads/2017/12/Ethereum_white_paper.pdf (accessed 9 August 2018).

Caulfield, T., McGuire, A.L. and Cho, M.K. (2008), "*Research ethics and the challenge of whole-genome sequencing*", Nature Reviews Genetics, Vol. 9 No. 2, pp. 152-156, doi: 10.1038/nrg2302.

Checkland, P. (1995), "*Model validation in soft systems practice*", Systems Research, Vol. 12 No. 1, pp. 47-54, doi: 10.1002/sres.3850120108.

Checkland, P. (2000), "*Soft systems methodology: a thirty-year retrospective*", Systems Research and Behavioral Science, Vol. 17 No. S1, pp. S11-S58.

Checkland, P. and Poulter, J. (2010), "Soft systems methodology", in Reynolds, M. and Holwell, S. (Eds), Systems Approaches to Managing Change: A Practical Guide, pp. 191-242, doi: 10.1007/978-1-84882-809-4_5.

Checkland, P. and Scholes, J. (1999), Soft Systems Methodology in Action, New ed., Wiley, New York, NY and Chichester.

Clohessy, T. and Acton, T. (2019), "*Investigating the influence of organizational factors on blockchain adoption*", Industrial Management & Data Systems, Vol. 119 No. 7, pp. 1457-1491, available at: https://doi.org/10.1108/IMDS-08-2018-0365

Colijn, C., Jones, N., Johnston, I.G., Yaliraki, S. and Barahona, M. (2017), "*Toward precision healthcare: context and mathematical challenges*", Frontiers in Physiology, Vol. 8, p. 136, doi: 10.3389/fphys.2017.00136.

Das, J., Holla, A., Mohpal, A. and Muralidharan, K. (2016), "*Quality and accountability in health care delivery: audit-study evidence from primary care in India*", The American Economic Review, Vol. 106 No. 12, pp. 3765-3799, doi: 10.1257/aer.20151138.

Dorussen, H., Lenz, H. and Blavoukos, S. (2005), "*Assessing the reliability and validity of expert interviews*", European Union Politics, Vol. 6 No. 3, pp. 315-337.

Frey, L.J., Lenert, L. and Lopez-Campos, G. (2014), "*EHR big data deep phenotyping. Contribution of the IMIA Genomic Medicine Working Group*", Yearbook of Medical Informatics – Journal Article, Vol. 9 No. 1, pp. 206-211.

Gauld, R. (2016), "*Healthcare system restructuring in New Zealand: problems and proposed solutions*", Asia Pacific Journal of Health Management, Vol. 11 No. 3, pp. 75-80, doi: 10.24083/apjhm.v11i3.163.

Halamka, J.D., Lippman, A. and Ekblaw, A. (2017), "*The potential for blockchain to transform electronic health records*", Harvard Business Review, available at: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records (accessed 8 August 2018).

Halim, S. (2019), "*Shivom: a precision medicine data secure-sharing and analysis ecosystem*", Health Europa, available at: www.healtheuropa.eu/shivom-precision-medicine/90476/ (accessed 8 August 2018).

Hallwright, J. and Carnaby, E. (2019), "*Complexities of implementation: Oxfam Australia's experience in piloting blockchain*", Frontiers in Blockchain, Vol. 2, p. 10, doi: 10.3389/fbloc.2019.00010/full.

Hanafizadeh, P. and Mehrabioun, M. (2018), "*Application of SSM in tackling problematical situations from academicians' viewpoints*", Systemic Practice and Action Research, Vol. 31 No. 2, pp. 179-220, doi: 10.1007/s11213-017-9422-y.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "*Design science in information systems research*", MIS Quarterly, Vol. 28 No. 1, pp. 75-105.

Huang, D. and Dobbie, G. (2017), "*Precision driven health context review report*", available at: www.precisiondrivenhealth.com/media/1201/orionhealth_pdh_contextreviewreport.pdf (accessed 9 August 2018).

Jithesh, P.V. and Scaria, V. (2017), "*From genomes to genomic medicine: enabling personalized and precision medicine in the Middle East*", Personalized Medicine, Vol. 14 No. 5, pp. 377-382, doi: 10.2217/pme-2017-0048.

Kshetri, N. (2018), "*Blockchain and electronic healthcare records*", IEEE Computer, Vol. 51 No. 12, pp. 59-63.

Laurenza, E., Quintano, M., Schiavone, F. and Vrontis, D. (2018), "*The effect of digital technologies adoption in healthcare industry: a case based analysis*", Business Process Management Journal, Vol. 24 No. 5, pp. 1124-1144, available at: https://doi.org/10.1108/BPMJ-04-2017-0084

Libakova, N.M. (2015), "*The method of expert interviews as an effective research procedure of studying the indigenous peoples of the north*", Humanities & Social Sciences, Vol. 8 No. 1, pp. 114-129.

Littig, B. and Pöchhacker, F. (2014), "*Socio-translational collaboration in qualitative inquiry: the case of expert interviews*", Qualitative Inquiry, Vol. 20 No. 9, pp. 1085-1095.

Love-Koh, J., Peel, A., Rejon-Parrilla, J.C., Ennis, K., Lovett, R., Manca, A. and Taylor, M. (2018), "*The future of precision medicine: potential impacts for health technology assessment*", PharmacoEconomics, Vol. 36 No. 12, pp. 1439-1451, doi: 10.1007/s40273-018-0686-6.

Lu, Y.-F., Goldstein, D.B., Angrist, M. and Cavalleri, G. (2014), "*Personalized medicine and human genetic diversity*", Cold Spring Harbor Perspectives in Medicine, Vol. 4 No. 9, p. a008581, doi: 10.1101/cshperspect.a008581.

Lunshof, J., Chadwick, R., Vorhaus, D.B. and Church, G.M. (2008), "*From genetic privacy to open consent*", Nature Reviews Genetics, Vol. 9 No. 5, pp. 406-411, doi: 10.1038/nrg2360.

Mackey, T.K., Kuo, T.-T., Gummadi, B., Clauson, K.A., Church, G., Grishin, D., Obbad, K., Barkovich, R. and Palombini, M. (2019), "*'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare*", BMC Medicine, Vol. 17 No. 1, p. 68, doi: 10.1186/s12916-019-1296-7.

Mehta, N. and Pandit, A. (2018), "*Concurrence of big data analytics and healthcare: a systematic review*", International Journal of Medical Informatics, Vol. 114, pp. 57-65, doi: 10.1016/j.ijmedinf.2018.03.013.

Mettler, M. (2016), "*Blockchain technology in healthcare: the revolution starts here*", 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (HealthCom), September, pp. 1-3.

Naerland, K., Müller-Bloch, C., Beck, R. and Palmund, S. (2017), "*Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments*", ICIS 2017 Proceedings. Presented at the 38th International Conference of Information System, Seoul, available at: https://aisel.aisnet.org/icis2017/HCI/Presentations/12

Nguyen, L., Emilia Bellucci, E. and Nguyen, L.T. (2014), "*Electronic health records implementation: an evaluation of information system impact and contingency factors*", International Journal of Medical Informatics, Vol. 83 No. 11, pp. 779-796, available at: https://doi.org/10.1016/j.ijmedinf.2014.06.011

O'Hara, K. (2017), "*Smart contracts - dumb idea*", IEEE Internet Computing, Vol. 21 No. 2, pp. 97-101, doi: 10.1109/MIC.2017.48.

Palvia, S., Sharma, R. and Conrath, D. (2001), "*Socio-technical framework for post-implementation quality assessment of computer information systems*", Industrial Management and Data Systems, Vol. 101 No. 5, pp. 237-251.

Park, Y.R., Lee, E., Na, W., Park, S., Lee, Y. and Lee, J.H. (2019), "*Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility*", Journal of Medical Internet Research, Vol. 21 No. 2, e12533, doi: 10.2196/12533.

Patil, H.K. and Seshadri, R. (2014), "*Big data security and privacy issues in healthcare*", IEEE International Congress on Big Data, pp. 762-765, doi: 10.1109/BigData.Congress.2014.112.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "*A design science research methodology for information systems research*", Journal of Management Information Systems, Vol. 24 No. 3, pp. 45-77.

Ponemon, L. (2016), "*Nearly 90 percent of healthcare organizations suffer data breaches, new Ponemon study shows*", available at: www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data (accessed 10 August 2018).

Privacy-Commissioner (2011), "*On the record: a privacy guide to health information policy*", 3rd ed., available at: https://privacy.org.nz/assets/Files/Health-toolkit/On-The-Record.pdf (accessed 9 August 2018).

Rabah, K. (2017), "*Challenges & opportunities for blockchain powered healthcare systems: a review*", Mara Research Journal of Medicine and Health Sciences, Vol. 1 No. 1, pp. 45-52, available at: https://pdfs.semanticscholar.org/ab2c/36d77953212f87b4671f53d0ec94bb80f0c3.pdf

Reynoso, R. (2017), "*BanQu uses blockchain to fight poverty*", available at: https://medium.com/coinforward/banqu-uses-blockchain-to-fight-poverty-6b6fa8263fc9 (accessed 9 August 2018).

Rubinstein, I.S. (2013), "*Big Data: the end of privacy or a new beginning?*", International Data Privacy Law, Vol. 3 No. 2, pp. 74-87, doi: 10.1093/idpl/ips036.

Schatz, D., Bashroush, R. and Wall, J. (2017), "*Towards a more representative definition of cyber security*", The Journal of Digital Forensics, Security and Law, Vol. 12 No. 2, pp. 53-74.

Sedgwick, P. (2015), "*A comparison of sampling error and standard error*", British Medical Journal, Vol. 351, doi: 10.1136/bmj.h3577.

Shah, S.G.S., Fitton, R., Hannan, A., Fisher, B., Young, T. and Barnett, J. (2014), "*Accessing personal medical records online: a means to what ends?*", International Journal of Medical Informatics, Vol. 84 No. 2, pp. 111-118, doi: 10.1016/j.ijmedinf.2014.10.005.

Shuaib, K., Saleous, H., Shuaib, K. and Zaki, N. (2019), "*Blockchains for secure digitized medicine*", Journal of Personalized Medicine, Vol. 9 No. 3, p. 35, doi: 10.3390/jpm9030035.

Singh, A., Parizi, R.M., Zhang, Q., Raymond Choo, K.-K. and Dehghantanha, A. (2020), "*Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities*", Computers & Security, Vol. 88, doi: 10.1016/j.cose.2019.101654.

Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A. and Soursou, G. (2019), "*Applications of blockchain technology in medicine and healthcare: challenges and future perspectives*", Cryptography, Vol. 3 No. 1, p. 3, doi: 10.3390/cryptography3010003.

Staker, R. (1999), "*An application of checkland's soft systems methodology to the development of a military information operations capbility for the Australian defence force*", available at: www.dtic.mil/dtic/tr/fulltext/u2/a362560.pdf (accessed 9 August 2018).

Stephanie, F.L. and Sharma, R.S. (2016), "*Health on a cloud: modeling digital flows in an E-health ecosystem*", Journal of Advances in Management Sciences & Information Systems, Vol. 2, pp. 1-20.

Teufel, H. II (2008), "*Privacy policy guidance memorandum, Memorandum Number*", The Privacy Office US Department of Homeland Security.

UML 2.5.1 (2017), "*Unified modelling language version 2.5.1*", available at: www.omg.org/spec/UML/; www.smartdraw.com/uml-diagram/ (accessed 9 August 2018).

Underwood, S. (2016), “*Blockchain beyond bitcoin*”, Communications of the Association for Computing Machinery, Vol. 59 No. 11, pp. 15-17.

Vaishnavi, V. and Kuechler, W. (2015), Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd ed., ISBN 978-1-498715-25-6, CRC Press, Boca Raton, FL, p. 415.

Van Poucke, S., Thomeer, M., Heath, J. and Vukicevic, M. (2016), “*Are randomized controlled trials the (G)old standard? From clinical intelligence to prescriptive analytics*”, Journal of Medical Internet Research, Vol. 18 No. 7, p. e185, doi: 10.2196/jmir.5549.

Vazirani, A.A., O’Donoghue, O., Brindley, D. and Meinert, E. (2019), “*Implementing blockchains for efficient health care: systematic review*”, Journal of Medical Internet Research, Vol. 21 No. 2, e12439, doi: 10.2196/12439.

Williams, T. (2019), “*The growing cybersecurity war on the healthcare industry*”, Technopedia, available at: www.techopedia.com/the-growing-cybersecurity-war-on-the-health-care-industry/2/32093 (accessed 25 November 2019).

Wynn, R.M., Adams, K.T., Kowalski, R.L., Shivega, W.G., Ratwani, R.M. and Miller, K.E. (2018), “*The patient in precision medicine: a systematic review examining evaluations of patient-facing materials*”, Journal of Healthcare Engineering, Vol. 2018, pp. 1-10, doi: 10.1155/2018/9541621.

Xia, C. and Song, S. (2012), “*Resource allocation in hierarchical distributed EHR system based on improved poly-particle swarm*”, 2012 5th International Conference on Biomedical Engineering and Informatics, New York, NY, October, pp. 1112-1116.

Xia, Q., Sifah, E.B., Smahi, A., Amofa, S. and Zhang, X. (2017), “*BBDS: blockchain-based data sharing for electronic medical records in cloud environments*”, Information, Vol. 8 No. 2, p. 44, doi: 10.3390/info8020044.

Yaeger, K., Martini, M., Rasouli, J. and Costa, A. (2019), “*Emerging blockchain technology solutions for modern healthcare infrastructure*”, Journal of Scientific Innovation in Medicine, Vol. 2 No. 1, p. 1, doi: 10.29024/jsim.7.

Yue, X., Wang, H., Jin, D., Li, M. and Jiang, W. (2016), “*Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control*”, Journal of Medical Systems, Vol. 40 No. 10, pp. 1-8, doi: 10.1007/s10916-016-0574-6.

Zhang, Q., Parizi, R.M. and Choo, K.K.R. (2018), “*A pentagon of considerations towards more secure blockchains*”, IEEE Blockchain Technical Briefs, September.

Zimmerman, L. (2019), “*Precision medicine: a view from the trenches*”, The Startup, available at: https://medium.com/swlh/precision-medicine-a-view-from-the-trenches-f0c10990c7b5 (accessed 9 August 2018).

Acknowledgements

The authors are grateful to the numerous participants in the SSM portion of the research who must remain anonymous as per the requirements of the research ethics agreement. Many thanks are also due to the reviewers and Editor of IMDS for their constructive comments and input which has led to a much improved article. Paula Wingreen proof-read the first submission and Adil Bilal provided research support for the Nvivo analytics.

Corresponding author: Ravi Sharma can be contacted at: rs.sharma.sg@gmail.com