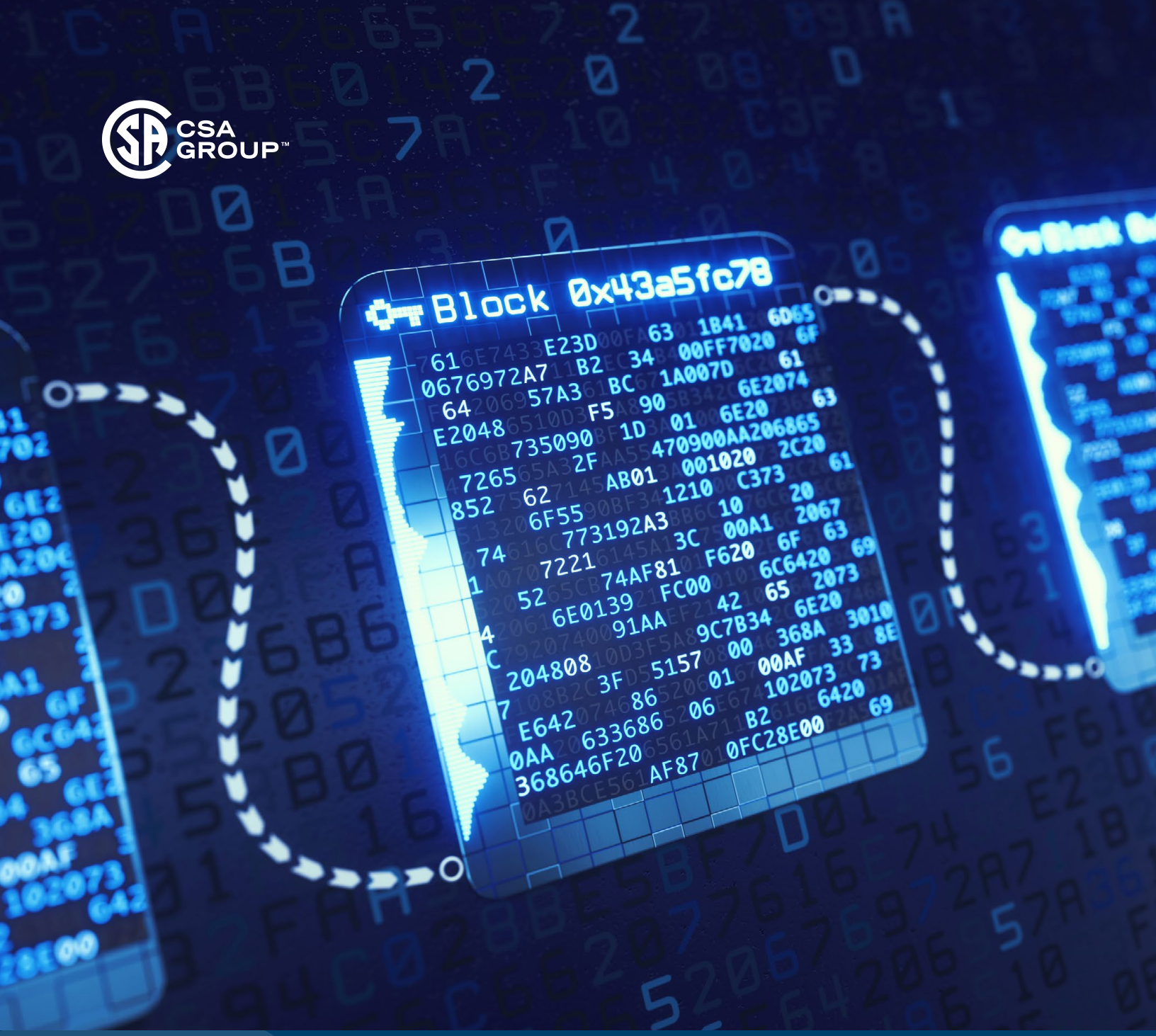


STANDARDS RESEARCH

Blockchain in Health Care

March 2021

Author

Pedro Elkind Velmovitsky, **B.Sc., M.Sc.,** University of Waterloo

Pedro Augusto da Silva e Souza Miranda, **B.Sc., M.Sc.,** University of Waterloo

Laura Xavier Fadrique, **B.Sc., M.Sc., PMP,** University of Waterloo

Plinio Pelegrini Morita, **P.Eng., M.Sc., Ph.D.,** University of Waterloo

Project Advisory Panel

Jim MacFie, Microsoft Canada

Victoria Hailey, The Victoria Hailey Group Corporation (VHG)

Jennifer Teague, **Ph.D.,** CSA Group

Stephen Michell, **B.Math., M.Sc.,** CSA Group

Tania Donovska, **B.Sc., M.Eng., PMP,** CSA Group (Project Manager)

Acknowledgements

This work was supported in part by the MITACS Accelerate program.

Disclaimer

This work has been produced by the University of Waterloo and is owned by the University of Waterloo and Canadian Standards Association. It is designed to provide general information in regards to the subject matter covered. The views expressed in this publication are those of the authors and interviewees. The University of Waterloo and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary

Humans today are experiencing unprecedented longevity, with older adults wishing to age independently, actively, and at home. As a result, there must be a necessary shift in how governments and countries view health care systems. These systems must be more proactive, promoting healthy lifestyles and behaviours, while having the necessary infrastructure to provide support, minimize risks, and allow for successful aging in place.

Globally, society is currently in an age of ubiquitous and smart technologies that can monitor our health effortlessly and in real time, including mobile, wearable, and connected devices. Active Assisted Living (AAL) technologies are used to promote independence and the quality of life of individuals, especially amongst vulnerable and elderly populations. When AAL is applied properly and respects security and privacy, it can facilitate an improved quality of life for older adults that includes better health, increased longevity, and supported independence. Alongside the development of technologies like AAL, we are seeing advancements in new areas of Information and Communication Technologies (ICT), such as Blockchain.

Blockchain technologies have gained in popularity since the development of cryptocurrencies in 2008 and have since been proposed as solutions to solve challenges in several fields. Blockchain can be seen as a tamperproof, decentralized virtual ledger that uses cryptography to ensure security and privacy. By design, Blockchain can provide more interoperability, availability, and robustness. Health care has long been plagued by inefficiencies and limitations, such as difficulties in the collection, sharing, and use of patient data to improve health outcomes – hence the potential value of an immutable ledger in mitigating these issues. Solving these challenges may also allow for a better management of the demands of an increasingly aging population: as innovative and smart technologies collect, share, and analyze older adults' data, they can help them live more independently and risk-free.

Previously, CSA Group published reports on emerging sharing technologies with the Mowat Centre [1] and on the AAL landscape in Canada with the Ubiquitous Health Technology Lab [2]. This current report builds on these previous reports by exploring how Blockchain is being used in industry to mitigate challenges in health care, exploring issues associated with this innovation, and focusing on how the technology can be used to improve AAL technologies as well as current standards in the field and future opportunities.

Insights and results have been obtained by conducting a literature review and consulting with stakeholders through semi-structured interviews. The objective was to identify opportunities and challenges to the application of Blockchain for health care and, more in depth, in the field of AAL. These analyses also provided insights into the development of new standards for the development of solutions using Blockchain and AAL. The goal of this report is to provide a better understanding of the Blockchain areas in which the development of standards can make a difference, specifically in the realm of connected devices and AAL.

Throughout the literature review, the following challenges were identified and grouped into five areas:

1. Electronic Health Records
2. Supply Chain
3. Health Insurance
4. Genomics
5. Consent Management

The interviews were used to confirm the results from our literature review, as well as obtain more information on Blockchain technologies. For example, Blockchain can provide several features to address health care issues, including immutability, decentralization, and security. However, Blockchain technology also has disadvantages that need to be balanced in its implementation, such as scalability issues, redundancy, and complex governance structures.

From the aforementioned challenges, consent management was singled out as one of the most pressing and promising applications of Blockchain in health care. All challenges and issues highlighted throughout the report depend, on some extent, on data sharing between different entities in a trusting and secure manner. To further our understanding of the application of Blockchain in health care, the main findings from the literature review and interviews were used to guide the development of a Blockchain-based consent management platform for AAL data. This platform can potentially increase transparency in the consent management process, enabling more efficient data-sharing.

The interviews conducted by our research team, in combination with the experience in the development of a Blockchain platform, have provided critical insights on current gaps in the availability of standards, guidelines, and best practices for supporting the use of blockchain in the AAL domain. There are currently few standards focusing on AAL technology, Blockchain, and the integration of both. Most stakeholders who are developing Blockchain solutions or who are involved with remote patient sensing are using existing health care and health informatics standards; Blockchain standards are currently in development or have been very recently published. In this report, we provide an overview of relevant Blockchain standards under development, in addition to discussing several opportunities for standards development such as knowledge translation, cybersecurity, governance, and privacy by design.

"While technology has long been explored as a means to help the elderly with daily activities, the research and health care communities are just recently able to capitalize on the benefits of technologies at a scale that allows successful aging in place."

1 Introduction

The world's age distribution is shifting towards an older population. By 2050, for example, Latin America, the Caribbean, and most of Asia, will have a median age of 40 years old, compared to a median age of around 30 today [3]–[5]. In Canada, nearly one in seven people were aged over 65 years old in 2012, and this number is expected to increase to one in four by 2030 [6]. According to the American Association of Retired Persons, 71% of people between the ages of 50 and 64 and 87% of people aged over 65 want to live at home while they age [7].

Successful aging in place requires older adults to be as independent, secure, and as healthy as possible. However, old age is associated with deteriorating health conditions and increases in chronic disease. For instance, it is estimated that 90% of Canadians over 65 years of age have at least one chronic condition [6]. Hence, aging in place can pose risks for the elderly. As seniors are a rapidly growing percentage of the Canadian population, "living longer and healthier lives than previous generations" [6], there is an expectation from this demographic group for active aging in place [8]. Going further, they expect to remain in the community and at home in a safe, comfortable, and independent manner as they age.

We live in a world of global exponential innovation. Referred to as a Fourth Industrial Revolution, emerging technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) [9] are increasingly prevalent in people's daily lives (e.g., smartphones, home assistants, and smart appliances create a connected system of smart devices). While technology has long been explored as a means to help the elderly with daily activities, the research and health care communities are just recently able to capitalize on the benefits of technologies at a scale that allows successful aging in place [2].

The field of Active Assisted Living (AAL) involves the use of Information and Communication Technologies (ICT) to "improve quality of life, bring independence, and enable healthier lifestyles for those who need assistance at any stage of life", particularly vulnerable and aging individuals [2]. Currently, consumer-grade devices are being used as AAL technologies due to their mass availability and ease of implementation. This presents two issues of concern: interoperability and privacy.

Devices used for AAL purposes are often produced by different manufacturers without comprehensive protocols for interoperability with devices from other vendors [2], presenting challenges for data integration. Different smartwatches may require the use of distinct technologies and proprietary platforms. As an example, an Apple Watch will require an iPhone integration (and this integration is limited to the types of data accepted by HealthKit [2]). Researchers wanting to collect data from Apple Watches along with other smartwatches will need to make use of several different technologies and applications. In addition, regarding privacy, the

ubiquitous nature of AAL technologies (which are now extremely common and pervasive in people's lives) increases the complexity of data collection points, making it harder to know exactly what data are being collected and for what purpose. This is particularly concerning for older adults, who traditionally have less advanced technological literacy compared with younger populations [10].

AAL technologies need to be adopted at scale in communities to allow safe and active aging in place. With a large and mature ecosystem of connected AAL devices, manufacturers and regulators could improve upon interoperability and data privacy issues. The current ecosystem is fragmented and composed of several devices that do not connect with each other or have their own data collection and privacy-preserving methods, making integration more difficult. The AAL programme in Europe, for instance, supports and funds projects focusing on the development of AAL technology to solve challenges in aging [11], [12]. As another example, Japan, with the oldest aging population in the world, is focusing on the creation of assistive robotic technologies to assist this population [12]. Canada lags when compared to other countries in the adoption of large-scale AAL platforms, although the country is a part of the AAL Programme and there are several networks of researchers exploring health aging, such as Age-Well [2], [13]. Even countries and regions that are more advanced in terms of large-scale adoption of AAL technologies still face challenges related to privacy, interoperability, and data sharing. Given the fragmentation and immaturity of this growing sector, new solutions are needed to address persistent issues around data governance and privacy arising from data collection, use, and disclosure. One technology that could help increase interoperability while maintaining privacy and enabling the rise of an AAL ecosystem such as the one described is Blockchain.

Blockchain is considered to be a "foundational emerging technology of the Fourth Industrial Revolution" [9] and has gained popularity since its creation due to the development of "cryptocurrencies", such as Bitcoin. Blockchain is a distributed virtual ledger that uses cryptography and consensus mechanisms to ensure that all ledger participants view a single immutable log of information. In other words, it can be seen as a tamper-proof data structure that is ideal to safely track and store events and assets, increasing trust among parties while enabling interoperability of different components.

Currently, the technology's potential to increase transparency and trust in several fields (e.g., environment, energy) is being recognized, including in health care [9], [12]. Given the novel applications of Blockchain in health care and in AAL, mitigating issues such as data sharing, interoperability, security, and privacy, the goal of this project is to explore the potential of Blockchain in the development of AAL technologies. This report focuses on how Blockchain can mitigate or solve current challenges in health care, how the health care industry is perceiving and implementing Blockchain solutions, and if this work relates to AAL and the needs of older populations. The report has a secondary goal of exploring opportunities and challenges for standards implementation to support the use of Blockchain in the health care industry and in the field of AAL.

1.1 What Is Blockchain?

Blockchain is a digital distributed ledger that uses cryptography techniques to record transactions. It is composed of a peer-to-peer (P2P) network of computers called nodes, each possessing the same copy of the ledger. This ensures that all participants accessing the network view one version of the truth [12], [14].

The transaction recorded in the network can be anything, from a financial currency exchange to the transfer of a land title. While different Blockchains usually handle one type of information[1], the underlying concept of Blockchain technologies works the same way: a transaction is time-stamped and then "sealed" inside a block, which is then linked to the chain of existing blocks through a consensus mechanism [12], [14].

1 For example, a transaction in the Bitcoin Blockchain is composed of an amount of Bitcoin, the person sending the Bitcoin, and the person receiving it.

For example, the Bitcoin Blockchain uses a consensus mechanism called Proof-of-Work (PoW), in which the participating nodes in the network try to guess a random number, called a nonce, that is the answer to a mathematical problem. The first node to correctly guess the nonce can use it as a digital key to attach the block with a transaction to the Blockchain in a process called mining; the nodes that try to guess the nonce are called miners, and the winning node receives a reward for maintaining the network through the consensus mechanism (in the case of Bitcoin, the winning node is rewarded with an amount of Bitcoins) [12], [14]. Every transaction in the network is validated this way.

Blocks are linked through a method called hashing, which converts data into an almost arbitrary string of characters. Hashing methods are extremely sensitive to input. For example, if a small piece of information in the inputted data is changed, the generated hash will be completely different. This makes it impossible to reconstruct the original information from a hash. In the case of the Bitcoin Blockchain, the nonce is hashed together with the transaction and the hash of the previous block, generating a new hash. If an attacker tries to tamper with a previously linked block (e.g., trying to remove a block and include a new one with modified information), the hash will be altered and the Blockchain will be broken. This allows Blockchain to be a tamper-proof and immutable ledger [12], [14].

According to the access structure of Blockchain technologies, they are usually divided into the following types [15]:

- **Public Blockchain:** All nodes in the network can read/write information (Bitcoin and Ethereum are examples of public Blockchains). It is a public ledger. In public Blockchain, information cannot be deleted.
- **Permission (Consortium/Federated) Blockchain:** The nodes consist of a consortium of participants who operate the network and define rules and permissions, including the ability to change or delete information. For example, a Blockchain consisting of health care stakeholders can allow patients to join the network and edit their information, while only health care providers can append new information.
- **Private Blockchain:** A single owner controls the Blockchain and defines rules and permissions.

Blockchain technologies can also be leveraged to allow the implementation of smart contracts. A traditional contract sets terms of agreements between parties to increase trust between them. The contract can be used to ensure compliance in case a party does not follow through with the agreed-upon terms. Smart contracts further increase trust through the introduction of automation by codifying the terms of contracts into software [12], [14]. For example, a smart contract may be implemented to receive input from crop sensors and, in the event of crop damage, the contract would activate an insurance claim [16]. With the help of Blockchain's permanent and distributed ledger, smart contracts can be a powerful tool to increase transparency and trust between parties and remove the need for human intervention and inefficiencies in the process.

2 Objective and Methodology

The objective of this report is to explore the use of Blockchain for improving on some of the challenges currently faced in the health care sector, with a focus on the field of AAL, and to investigate opportunities for standards adoption in these areas. Therefore, in addition to exploring this field, we want to highlight any existing gaps in standards that can facilitate the adoption of Blockchain for AAL. To this end, we followed three exploratory methods: a literature review, interviews with knowledgeable stakeholders, and a practical implementation of a Blockchain proof-of-concept.

A literature review was conducted on the current use of Blockchain solutions in health care to develop an understanding of what these technologies entail, and to identify existing challenges in health care.

For this report, the following research questions were taken into consideration:

1. What are the current challenges faced by the health care industry today that could be addressed by Blockchain technology?

2. For each of these challenges, which Blockchain solutions are being developed by the health care industry?
3. Which of these solutions can also apply to AAL?
4. How can standards contribute to AAL/Blockchain?

Grey literature (comprised of the web pages of companies and solutions reviewed in this project) was reviewed in addition to academic literature (e.g., IEEE and PubMed) and news outlets (e.g., CoinDesk [17], Cointelegraph [18], and Medium [19]). The keywords were a combination of "blockchain", "distributed ledger", "health", "industry", and "health care". Whenever possible, technical reports were reviewed in addition to news articles. Health care companies identified through this review were grouped into common themes to explore how innovators claimed to use Blockchain and what health care challenge was addressed.

The literature review was followed by telephone interviews with key stakeholders in the fields of Blockchain and AAL. The purpose of the interviews was to build on the results of our literature review as well as to confirm, with active participants in the field, that Blockchain was indeed being currently used as stated in the field. Details on the limitations of the technology are not often raised in published documents, so these interviews were also used to explore any disadvantages of Blockchain technologies.

All interviews followed a semi-structured interview guide, which provided the flexibility of adapting questions to each participant's context. Since any future standards for supporting Blockchain technologies are implemented to benefit innovators, we focused on interviewing stakeholders that had experience with this technology. A subset of the interviewees also had experience in applying Blockchain for health care contexts. For this reason, end users of the Blockchain tools were not included in our interviews.

During the literature review, we identified key concepts and themes related to Blockchain and health care. This was followed by a thematic analysis of the interview transcripts by summarizing and prioritizing which areas in the health care industry benefit from the use of Blockchain, as well as any mention of standards (or lack thereof). During the thematic analyses, concepts related to the health care challenges identified during the literature review stage were specifically considered with a focus on how these benefits can translate into the field of AAL. The results are presented according to these themes, with the literature review and stakeholder input being presented together under each theme.

The main findings were used to guide the development of a proof-of-concept in order to better understand the use of Blockchain in health care. The goal of this prototype was to explore the utility of Blockchain in a specific use case, highlighting benefits or limitations of the approach, as well as identifying future research needs and opportunities for the development of standards.

3 Opportunities for the Use of Blockchain in Health Care

The main findings of this research are presented below. Section 3.1 and 3.2 review the benefits and disadvantages of Blockchain according to the interviews and Section 3.3 presents the challenges found in the literature review, followed by an exploration of how health care innovators are using these technologies to address some of these challenges. In this section, we explicitly mention the interviews if a specific topic was highlighted by stakeholders. Section 4 describes how these results led to the development of a Blockchain platform for consent management, and Section 5 describes existing Blockchain standards, as well as current gaps and opportunities for standards development with Blockchain, health care, and AAL. Eleven stakeholders participated in the interviews. Eight stakeholders worked in industry and were involved with security, privacy, and Blockchain; and three stakeholders came from academia.

"The stakeholders interviewed for the project cited auditability, proof of transactions, and immutability as major advantages of Blockchain technologies."

3.1 Benefits of Blockchain

The stakeholders interviewed for the project cited auditability, proof of transactions, and immutability as major advantages of Blockchain technologies. Due to their decentralized structure and consensus mechanism, these technologies can also increase trust in distributed spaces, as all partners involved will have clear, transparent, and trusted records.

Several attributes can be included in the Blockchain, such as titles and legal documents [12], [14]. In the health care domain, one stakeholder pointed out that attributes such as test results, instructions for medical devices, compliance with standards, among others, are possible artifacts to be appended on the Blockchain.

Blockchain technologies are flexible enough to account for different regulations. For instance, it is possible to set up nodes in different regions to comply with geographical regulations such as data not leaving a territory.

Blockchain can also be easily integrated with other technologies such as Artificial Intelligence (AI). Some examples are explored in the next sections. If integration with different tools is needed, developers must take that into account when developing their infrastructure.

One common theme throughout the literature review and stakeholder interviews is that privacy is a major concern for AAL and data collection in general. By providing an unchanging log of events, Blockchain could be an excellent tool for solving this problem through consent management for data collection.

3.2 Disadvantages of Blockchain

Stakeholders were quick to raise current limitations with the technology. Four stakeholders mentioned that, currently, there is a lack of understanding of what Blockchain is (further confounded in that many people think only in terms of cryptocurrencies and financial applications). This leads to the overuse/overhype of the technology, with Blockchain being applied to situations in which it might not be the best solution. One stakeholder mentioned that this immaturity is not different from other new technologies, and innovation requires a trial-and-error period. One difficulty generated out of immaturity is the lack of robust models of how a Blockchain should work (e.g., rules, governance structure, access control) in different applications.

Two stakeholders mentioned a fear of litigation with the adoption of innovative technologies. This is particularly true in the health care domain, in which the quality of life of patients must be maintained, as well as their security and privacy; implementing new technologies that disrupt the current workflow can be a deterrent to adoption.

Scalability was also identified as an issue by three stakeholders. Most current Blockchain implementations cannot handle large volumes of data, and it is generally

accepted that the technology should not be used as a database. This means that typical implementations should not be used, for example, to store health record information or other data types. Rather, the strength of the technology lies in storing a log of events with reference to information off-chain in an immutable way. It is important also that any external data referenced should also be made immutable to maintain the benefits of Blockchain. One way to achieve this is by hashing each document and storing the hash in a block; in this manner, users would be able to check if the data were tampered with in any way.

The immutability of Blockchain technologies can also be a disadvantage, as information included in public Blockchains cannot be deleted. Permissioned or private Blockchains, however, have their own sets of rules regarding appending, updating, and deleting information, as previously mentioned. In addition, it is important to note that time-stamping, validation, and securing records/assets on the Blockchain does not necessarily guarantee data quality, as this comes from the source of data input (e.g., human error, sensor malfunction).

Since current Blockchain implementations often consume large amounts of energy, one stakeholder pointed out that these technologies might be unsustainable as their benefits do not compensate for the damage done to the environment. The mining process and the large number of nodes, typical of cryptocurrency systems, are a large part of the energy use, and other implementations that do not depend on these may consume less energy. Given the novel aspect of the technologies, there is also uncertainty about its usability, especially related to different regions and legislations (e.g., regulation of Electronic Health Records, democratic economies versus authoritarian regimes, geopolitical problems). Therefore, while one of the potential benefits includes flexibility in the technology to deal with distinct regulations, its implementation may be hampered by external factors, as described above.

Two stakeholders pointed out that most Blockchain solutions in health care are in early, prototyping stages, while another stakeholder mentioned one example of a solution already deployed with large hospital chains. Ultimately, a lack of standards for these technologies, and specifically for health care, was a limitation noted by all participants.

Indeed, in our literature review, we found that, with a few exceptions, most solutions seem to be at initial prototyping stage. While their functionalities are already planned and being implemented or tested, there is a lack of wide usage and large-scale adoption of finalized solutions. In addition, these are commercial solutions, which may require a fee or subscription to use them once they are completed.

3.3 Key Health Care Challenges and Use of Blockchain

The literature review, along with the targeted interviews, revealed five key themes around which Blockchain has been explored in health care. The five key challenges reviewed in this report include Electronic Health Records, supply chain (subdivided into drug and food supply chains), health insurance, genomics, and consent management.

The challenges presented in this report represent a sample of issues and are not meant to be exhaustive. For example, there are issues that cross multiple sectors, such as identity management. When needed, these additional challenges will be presented.

3.3.1 Electronic Health Records

The use of Electronic Health Records (EHRs), which contain digital health-related data from patients, has helped to increase the quality and delivery of care [20]. One of the biggest challenges facing the health care industry today is the fragmentation of EHR systems. Typically, health care providers are the primary custodians of health data. As patients interact with different health care providers, their health information becomes dispersed across different platforms. In addition, providers must commit to using a distinct commercial EHR system that often is not interoperable with those from other manufacturers, thereby creating data silos and impeding a complete view of a patient's health data. Ultimately, this impedes communication of health information, which may lead to poorer health outcomes and delivery of care [12], [21]–[23].

Blockchain technologies can create an overarching infrastructure to link patient records. The Blockchain, in this case, acts as a hub containing the location to off-chain storage locations containing patient data. On that note, patients can define rules for access to their records, and access logs can be tracked. Such a solution has the potential to greatly improve interoperability and reduce fragmentation while giving individuals greater control over their health data [14], [24]. For example, MedRec is a solution developed by the Massachusetts Institute of Technology (MIT) in which metadata concerning medical data from several sources is encoded in the Blockchain. Providers can append patient records but patients need to give their permission to providers so that data can be accessed and shared [23], [25]. Table 1 shows other companies working on similar solutions. Some of these also allow the integration of data from new sources, such as sensors and mobile devices. Also, some solutions enable patients to sell anonymized records to data buyers with the Blockchain acting as a broker between data owners and buyers, creating a form of Health Data Marketplace. It is important to note that the majority of examples found for these are in the context of the US system. The test case presented in Section 4 expands on how data ownership can vary and change according to the region.

During the interviews, four stakeholders expressed concerns about the creation of an overarching structure for EHRs, as this can bring about several regulatory, security, and privacy challenges. For example, an attack on a centralized location for medical records can expose patients' entire medical history. It was also generally assumed that a private or permissioned Blockchain needs to be used in such scenarios to minimize regulatory issues. Permissioned Blockchains, formed of a consortium of providers, typically are not meant to silo data, which would decrease interoperability, but to provide regulated access. This is an important example of an area that would benefit from the development of standards for Blockchain implementations, providing guidance and a standardized framework for Blockchain solutions for storing and managing medical records.

Five stakeholders recognized Blockchain's potential to improve analytics of medical records. For example, it could ensure that a feed from EHR systems is securely transferred to a repository of data from different systems and sources (e.g., personal health data). One stakeholder said that it is "the best possible mechanism to integrate disparate sources of information that are stored differently", providing added security and flexibility to data formats. Data on a secure repository enabled by Blockchain could then be analyzed using advanced techniques such as Artificial Intelligence. Also, a centralized record could lead to the development of a "digital health wallet", including information on a patient's health history (e.g., medications, allergies, surgeries). One stakeholder mentioned that Blockchain could not only help with integrating data from different sources and sensors but could also help to ensure that data are deleted accorded to requirements and regulations, logging events related to the data (but not the data itself).

3.3.2 Supply Chain

A huge challenge faced by the pharmaceutical industry is counterfeit drugs, affecting the safety of patients as well as increased costs. As an example of its scale, it is estimated that US$200 billion is lost annually due to counterfeit pharmaceuticals [26]. Recognizing this issue, the Federal Drug Administration's (FDA) Drug Supply Chain Security Act in the US requires that pharmaceutical companies implement product tracing and verification [27]. The challenge of a product's traceability can also be extended to include other products, such as food. A solution that enables the tracking of food products could, for example, help in the identification of food contaminations and trace it back to its source.

The immutable ledger can be used as a record of a product's provenance by storing transactional data of the product's supply chain on the Blockchain. In this way, the product can be traced during all stages of its supply chain, from manufacturing to sale. Table 1 shows examples of companies developing Blockchain solutions to tackle the drug and food supply chain.

Among these, there are companies that use Blockchain technologies to determine if products are being shipped according to appropriate conditions. For example, Modum [28]–[31] is a company that uses sensors to monitor temperature during transportation and uses smart contracts to evaluate if the temperature levels were consistent with regulations.

Five stakeholders raised Blockchain's potential to track products, time-stamp data in a secure way, and tackle counterfeits in the drug supply chain. Pharmaceutical traceability seems to be an optimal use case as legislation favours it and pharmaceutical companies have the resources to implement a Blockchain-enabled solution. Another interesting supply chain example mentioned by a stakeholder is the tracking of medical devices, as Blockchain can record artifacts such as recall management, the efficiency of devices, and the progression of patients associated with the device, amongst others. This information can also be integrated into the medical records of a patient and allow for a complete view of treatments.

3.3.3 Health Insurance

As previously mentioned, most use cases described in this section focus on the United States. In the following discussion, it is assumed that a similar model of the coverage typically offered by employers in the US applies, or one that is not publicly funded. In many cases, insurance in the US is not entirely dissimilar from extended health benefits in Canada, with the difference that often the patient pays for the service out-of-pocket and gets reimbursed by the insurance provider. Given these considerations, the same benefits of Blockchain to the health insurance space in the US may apply to extended health benefits in Canada.

In the context of health insurance in the US, claims management works as follows: (a) a provider offers a service to a patient who is covered by an insurance plan; and (b) the insurer checks the patient's health plan to determine their benefits and pay the necessary values to the provider. Coverage involves increasingly expensive premiums to insurance companies, whose practices and prices are not transparent due to security risks. Health care providers need to comply with bureaucracy during the claims adjudication process, which can take several weeks to be resolved. Additionally, insurance fraud can happen throughout the process [32], [33].

Smart contracts implemented in the Blockchain can minimize inefficiencies and increase trust between payers, providers, and patients. Such a system would also help to minimize insurance fraud and provide more efficient auditability. For example, the company PokitDok developed a private Blockchain that contains references to off-chain file systems [34]–[36]. Much like with EHRs, smart contracts are used to obtain data from health insurance providers and payers in real-time.

Additionally, Blockchain can help with insurance claims management with the ultimate goal to solve claims in real-time with smart contracts: as a service received by a patient from a provider is logged on the Blockchain, smart contracts will determine in real-time how much is owed to each party. PokitDok's goal is to allow real-time status checks of claims.

Initiatives that focus on the creation of a Health Data Marketplace want to connect service buyers (e.g., patients) and sellers (e.g., providers) without the need of an insurance company to act as an intermediary. The marketplace platform proposed by these companies will allow patients to search and use a health service with crypto tokens from the Blockchain. Companies such as CareX [32], [37], [38], MedicalChain [33], [39], Medoplex [40]–[42], and BlockRx [43], [44] are offering solutions in this space. Indeed, many companies that deal with EHR systems are also looking at the health insurance space. With a Health Data Marketplace platform, the goal is that intermediaries in the process such as insurance companies will not be needed, or their roles will be diminished. According to companies proposing these new solutions, patients would be able to pay directly for services since their price will be greatly diminished, and usually with the use of a crypto token. Several systems propose different ways of earning these tokens. For example, in some situations they might earn crypto tokens by sharing personal data, which could be later used to pay for services. It is also important to note most of these companies' documentation/public information/websites make

"One of the biggest promises in the health care field is the study of genomic data, made available through technological advancements in the field of gene sequencing."

mention of the US health care system (as for example the Medicalchain [33] and Embleema [45] white papers), which seems to indicate their intention to apply their business models in the US, at least at first. As described above, Table 1 presents Blockchain-based companies working on this space.

It is interesting to note that the companies identified in the literature review seem to be in the advanced stages of deploying a Blockchain-enabled insurance platform, while only one stakeholder mentioned he knew of examples in the very early stages of development. While the maturity of the solutions being developed may be higher than other applications, there is still a lack of consensus and guidelines about the minimal components of each system, consequently warranting the development of standards that could benefit the application of Blockchain in health insurance.

3.3.4 Genomics

One of the biggest promises in the health care field is the study of genomic data, made available through technological advancements in the field of gene sequencing [46], [47]. Indeed, the combination of genomics data with socio-environmental data is the basis for precision medicine, a field of research that focuses on the study of personalized benefits and treatments for individuals [48]. However, for researchers to obtain meaningful insights from genomic research, large volumes of data are needed. Privacy and security concerns, a lack of interoperability between data systems, and high costs often limit the scalability and impact of the technology.

The current business model for genomics data collection companies (e.g., 23AndMe, Ancestry) involves individuals using paid services of specialized companies to sequence and obtain their genome. Individuals receive the results of the analysis, while the companies retain the genomic data for their use. Blockchain could provide an opportunity for individuals to connect directly with data buyers (e.g., a company doing genomic research) without the need for intermediaries. In addition, interoperability could be improved by connecting separate genomic datasets, much like MedRec proposes to do with EHRs. Blockchain therefore has the potential to create a Genomic Data Marketplace and to diminish data silos, increasing patient ownership of the data as well as the availability of genomic data for research. For example, Nebula Genomics is creating a marketplace for genomic and health data by developing a Blockchain platform in which individuals can share and sell their data [46]. Data buyers could potentially provide rewards for individuals to sequence their genomes to create their datasets (e.g., providing crypto tokens to individuals with a certain feature to be researched if they sequence and share their genome). Table 1 describes further examples of companies working on similar genomics solutions with Blockchain.

Genomics was not raised by stakeholders as a potential use case for Blockchain, likely due to their background being more focused on cybersecurity, privacy, and standards. Our literature review indicated genomics as a major domain for the use of Blockchain in health care, with opportunities for standards development to guide the implementation of interoperable and secure genomic data sharing infrastructures.

3.3.5 Consent Management

The field of health care is being revolutionized with the addition of novel data sources that can collect diverse, real-time health data, including IoT and AAL technologies. However, the ubiquitous nature of these technologies makes it harder for individuals to know exactly what, where, when, and why their data are being collected and used. Without explicit, informed consent from individuals, data collection and use can violate the privacy and ownership rights of these participants [3], [49].

Blockchain's ledger, applied to the context of consent management, could provide a transparent, tamper-proof, time-stamped log of informed consent, immutably storing information such as from whom data-collection consent was given, and for what period. For example, Hu-Manity.co developed a mobile app with IBM Blockchain to aid individuals to consent to the use of personal information [50], [51]. Bitfury is developing a similar solution to manage consent for research [52], [53]. Additional solutions are mentioned in Table 1.

One of the stakeholders described consent as "one of the most promising use cases" for Blockchain in health care. It can help with data sharing and improve issues related to regulation and security (e.g., with EHRs on the Blockchain). Some companies are also looking at using Blockchain to improve clinical trials (e.g., to validate patient consent and to manage the supply chain during trials).

A related use case involves identity management via Blockchain. By providing a verifiable, immutable, and auditable log of records, Blockchain can also verify and authenticate an individual. In health care, a digital identity enabled by Blockchain can greatly simplify processes [35].

One stakeholder mentioned that access to medical records in correctional facilities is extremely complicated, for example, due to mental illness or lack of trust by inmates. Having immediate access is critical and identity and consent management with Blockchain could help while providing auditability. It could also provide benefits in hospital settings, allowing for more direct access to different EHR systems. A digital and trusted identity could encourage data sharing and interoperability of patient records; aligned with consent management, this could greatly improve traditional workflows in health care.

3.3.6 Practical Exploration of Standards for Blockchain

Blockchain, as a novel technology, imposes multiple challenges to innovators and users globally. The rate of development and implementation of Blockchain solutions has outpaced the development of best practices, processes and standards, leaving innovators and users with a knowledge gap for solution implementation. A consistent theme from the literature review and stakeholder interviews emerged in that adoption of Blockchain to address data issues in the health care system may be improved through the development of standards. This is further discussed in Section 5.

4 Developing a Consent Management Platform Using Blockchain

Drawing on the findings of the literature review and stakeholder interviews, a model of Blockchain implementation was developed as a test case for its use in health care featuring AAL. A lack of interoperability is a critical gap faced by the AAL technology ecosystem, and Blockchain solutions can help to mitigate this issue by integrating heterogeneous data from distinct sources and sensors [2]. This will facilitate data sharing among different devices, technologies and systems, and increase interoperability. Indeed, an EHR-Blockchain platform that acts as a hub to centralize data from different sources, such as the ones mentioned in the previous section, could greatly improve interoperability and diminish data silos. If such a platform can integrate

Table 1: Challenges and Blockchain solutions being developed for health care: findings of the literature review and interviews.

Challenges	Description	Solutions
Electronic Health Records (EHR)	Companies are looking at Blockchain to provide an overarching hub that links together a patient's electronic medical records. In most solutions, access control is in the hands of patients, who must permit a third-party to access the data. Some solutions discuss the integration of health data from alternative sources, such as smart technologies. Some solutions discuss the creation of a Health Data Marketplace, powered by Blockchain, in which patients sell their data for crypto tokens, and even pay for health care services using these tokens.	MedRec [23], [25], [54], PatientTruth [45], [55], CareX [32], [37], [38], MEDIS [56], [57], GEM [58]–[62] , MedicalChain [33], [39]
Supply Chain	Blockchain can enable companies to track and trace a product throughout the supply chain, with an immutable log of events. For health care, this includes drug and food supply chains.	Drug Supply Chain: BlockVerify [26], [63], [64], BlockRx [43], [44], Merck [65], [66], Modum [29]–[31]
Health Insurance	Blockchain can enable the settlement of health insurance claims through smart contracts, as well as more efficient insurance processes (e.g., payments, pharmaceutical and medical benefits check, payment risk calculation).	DokChain [34]–[36], [73]–[79], GEM [61], Payspan [80], [81]
Genomics	Similar to EHR, Blockchain can act as an overarching hub for linking genetic datasets. Blockchain can also connect sellers of genomic data-to-data buyers directly, without the need of any third party, creating a Genomic Data Marketplace.	Nebula Genomics [46], [82], LunaDNA [83]–[87], Shivom [88]–[91], Zenome [47], [92], EncrypGen [93]–[96], Macrogen [97]–[99]
Consent Management	Blockchain can allow a more transparent and efficient consent management process by providing an immutable and time-stamped log of consent, allowing individuals to grant revoke consent for different data types and periods.	My31 app [50], [51], Bitfury [52], [53], HealthVerity Consent [100], Verifiable Audit Trail (tracking of events related to health data) [101]–[105], INSERM/APHP Consent Project [106], Queen's University BlockTrial [107], Patient Control and Consent Blockchain initiative [108]–[110], Ubiquitous Health Technology Lab [12], [111]

data from mobile and wearable sensors as well (as many solutions are proposing to do), Blockchain could further help in integrating data from different sources and increasing data sharing. Further, as mentioned by one stakeholder, Blockchain could help with indicators and proof of data. For example, by logging central events in the AAL data (rather than the data itself), it would be possible to securely and transparently keep track of a patient's progression (e.g., how many falls occurred in a certain period).

One concern with AAL is that target populations, which often include vulnerable and elderly individuals, may not have the capabilities or expertise to interact with complex devices and applications. Blockchain could make these interactions simpler for example, by not requiring repeated logins if the user's identity is verified and trusted in the system.

Guaranteeing the privacy and security of individuals and their collected data are major concerns in the AAL space [2]. One stakeholder aptly posed the question: "Who gets to see that data, and how much permission was given to store it?" This is not an issue with the technology itself, but with consent. Since Blockchain can provide auditable and permanent logs of transactions, it could greatly improve transparency, consent management, and compliance. Specifically, Blockchain can provide a permanent and time-stamped log of user consent for data collection, use, and access.

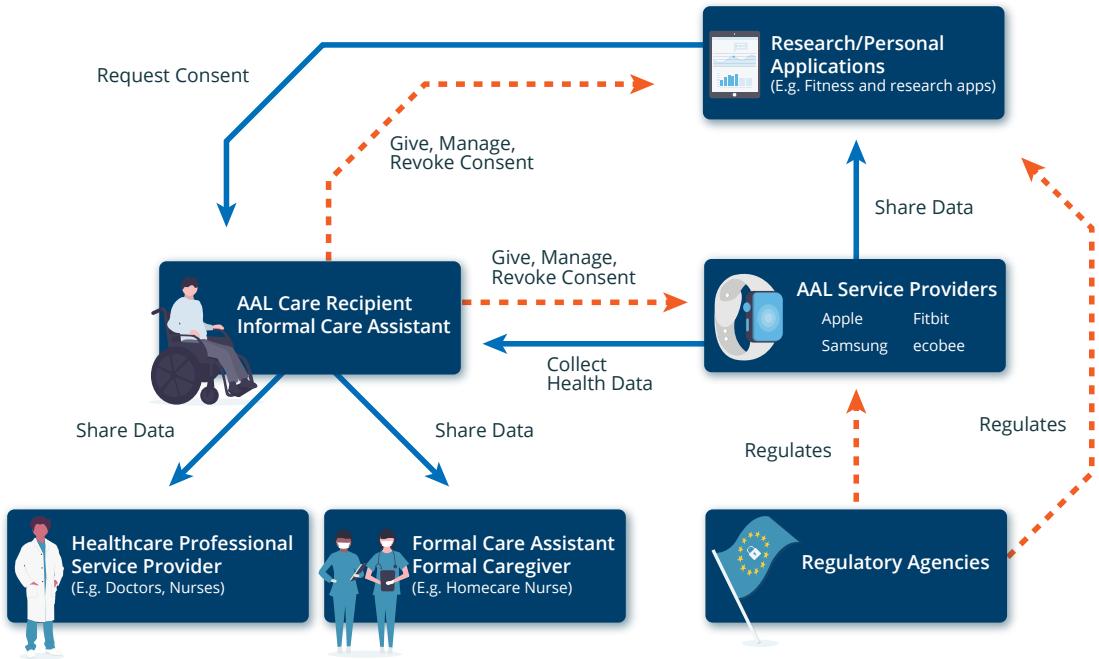
Consent management was highlighted multiple times by stakeholders as one of the most promising use cases in health care, and is a foundation for all other health-data use cases described in the previous sections. For example, interoperability and data sharing are not relevant unless an integrated system for individuals to consent to data collection and analysis is established first. As such, a model of Blockchain implementation was developed as a test case for its use in health care featuring AAL. A proof-of-concept consent management platform was developed to help identify practical issues in its implementation and to provide insight into the decisions, options, and requirements involved in developing such a tool. Through this exploration, the experience would also lend insight into aspects of Blockchain application in this context that might benefit from standardization.

4.1 Modeling the Consent Management Process

A model of the consent management process with AAL technologies was created to better understand the challenges faced in developing solutions with Blockchain and better gauge the benefits and applicability of using these technologies for health data consent management in the AAL space. This model, in turn, enabled the identification of possible trust issues within the process. Through the mapping of trust issues, as described by Gorenflo et al. [112], we can identify potentially effective use cases for Blockchain to satisfy them.

Figure 1 shows the proposed model of the consent management process. In this model, the AAL Care Recipient (or an Informal Care Assistant, such as a family member who takes care of the recipient) uses AAL technology, such as sensors, to track activities of daily living (ADL). In this sense, they are the users of the technology. Users can share the data with their health care provider and formal care assistant (as represented by the arrows), and can give, manage, or revoke consent for their data being collected, used, or disclosed by AAL service providers, who are usually the manufacturers of the technology (e.g., ecobee, Apple, Samsung). In addition, the user also needs to manage their consent for any third-party applications, such as research/personal applications that are receiving their

Figure 1: Relationships and trust issues in the consent management process.



data. An example of such a situation involves the use of an iPhone and connected devices such as wireless scales and smartwatches as part of an AAL ecosystem by seniors. The user's data (e.g., steps, heart rate, weight) are stored in the Apple Health app, which acts as a repository of health data. Several apps installed in the iPhone can, with the user's consent, access this data, for example, a fitness app to track exercises during the week.

The green arrows represent relationships without potential trust issues. Regarding data sharing with health care providers and caregivers, it is assumed that these providers are trustworthy and, therefore, trust issues may not arise. The red dashed arrows in the diagram represent possible trust issues between entities:

- **AAL Care Recipient/Informal Care Assistant + AAL Service Providers:** AAL care recipients/informal care assistants need to trust AAL service providers to ethically collect, use, and disclose their data according to current legislation, including if the AAL service providers are only sharing data with pre-approved third parties.
- **AAL Care Recipient/Informal Care Assistant + Research/Personal Applications:** AAL care recipients/informal care assistants need to trust third-party applications to ethically collect, use, and disclose their data according to current legislation.
- **Regulatory Agencies + AAL Service Providers:** AAL service providers are subject to privacy/regulatory acts from the regions in which the data are being collected. Failing to comply is against the law. Health Canada for example, states that while cybersecurity vulnerabilities in devices are a shared responsibility between the manufacturer, regulator, user, and network administrator, "manufacturers are responsible for continuously monitoring, assessing, and mitigating potential cybersecurity risks associated with their products throughout their life-cycle" [113].

From a regulatory perspective, data collection, use, and disclosure are managed by regulatory agencies. It is important to note that this term is meant to represent general privacy regulation agencies, as there is not typically any specific agency regulating AAL devices. There are several agencies that regulate medical and/or digital health devices. In Canada, Health Canada is the federal regulator of medical devices [113], while the Food and Drug Administration (FDA) is the federal agency responsible for the regulation of devices in the United States [114]. European countries have national authorities for the regulation of devices, and the European Medicines Agency (EMA) assesses certain devices under EU legislation [115].

Data privacy in Canada is addressed by the *Protection and Electronic Documents Act* (PIPEDA), which regulates the collection, use, and disclosure of personally identifiable information (PII)[2] for private sector organizations involved in a commercial activity. This federal act applies to all types of PII [116], [117]. In addition, several provinces have adopted health sector laws dealing with personal health information (PHI), some of which are deemed substantially similar to PIPEDA and take precedence in these provinces [2], [116], [118], [119]. In the US, the *Health Insurance Portability and Accountability Act* (HIPAA), which applies to subsets of health custodians in the US, offers a similar but more comprehensive list of technical, physical, and administrative safeguards, including required and optional mechanisms [120]. In 2018, Europe released the General Data Protection Regulation (GDPR), which focuses on consent and has stricter rules compared to similar legislation and provides the user with more control and ownership over their data. It is likely that the GDPR will influence new updates of PIPEDA [2].

4.2 Implementing the Consent Management Platform

A proof-of-concept of the Blockchain for the consent management platform (CMP) was developed to demonstrate the feasibility of using Blockchain to address trust requirements, improve the consent process, and help identify areas that could be

2 PII is any information that can directly identify an individual.

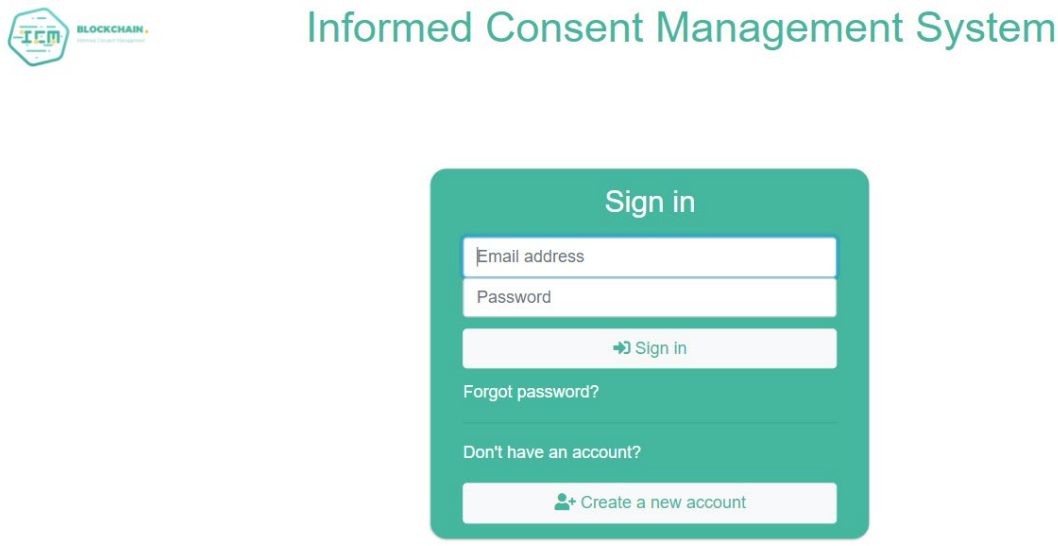
supported by newly developed standards. A set of actors were defined (e.g., health care researchers, pharmaceutical companies) to include those interested in transacting consent information from the AAL care recipients/informal care assistant and any substitute decision-makers (SDM) who may act on behalf of the care recipient to make health decisions [121]. SDMs are particularly important in the context of AAL, as recipients with declining cognitive abilities may require other individuals to make health decisions on their behalf.

The CMP was developed to include a permissioned Blockchain [122] to ensure that only registered network participants[3] can interact with the informed consent information. In addition, patient information is protected from security risks of a public Blockchain solution [123]. A user-friendly interface for informed consent management was also developed, allowing any of the platforms' users to easily interact with the Blockchain without having any previous technology knowledge. Figure 2 shows the login screen of the CMP.

The participants mapped by the CMP are:

- Data producers [15], [124], [125], corresponding to AAL care recipient/informal care assistant. They are the users of the platform.
- Data auditors [126], [127], corresponding to regulatory agencies.
- Data consumers and data custodians [128], [129], [130]–[133], corresponding to AAL service providers and/or research/personal applications.
- While consumers and custodians were not differentiated in the diagram, they were modelled as distinct participants in the system to separate, for example, a group of researchers who wishes to collect data (a consumer) from an institution, such as hospitals or universities (a custodian). In practice, a participant can be both a consumer and a producer (for example, by both collecting data for other entities and using the data themselves).

Figure 2: Consent management platform login screen.



3 Registered network participants are any real-world companies, regulatory agencies, hospitals, and any other health care stakeholder that collects, stores, processes, or shares health care data from AAL patients. As of this version of the platform, new participants can be added to the network at any time by a network administrator.

Data producers (e.g., AAL users, SDMs) are interested in using AAL technologies to monitor their health or the health of a care recipient [12], [130], [134]. To achieve this goal, data producers must provide informed consent to data consumers, thus giving data consumers access to the health records for processing. The CMP allows data consumers to create informed consent requests for AAL users, which then are published on the platform. The created requests are displayed for data producers registered in the platform, allowing them to choose different types of monitoring services and research to participate in. Figure 3 shows the interface that presents to users all the requests for informed consent from different types of data consumers. A green background is added to requests that the user has already consented to.

By selecting a data consumer request, an AAL patient can see a detailed view of it as shown in Figure 4. On the left side of Figure 4, the platform presents a description of the request and additional details. On the right side, the type of data needed by the data consumer's request is displayed. Users can choose what type of data they want to share and for what period. They can also revoke consent at any time. Setting a period for data sharing is important to enforce re-consent requests from data consumers if they wish to continue collecting users' data.

The sliders next to the type of data represent the state of access to that data being "true" or "false". "True" means that consent is granted for the period (date picker fields: "From" and "Until") chosen by the user, and "false" means that consent is denied for that type of data. Once the user finishes defining which data are going to be shared for the request, they click on the button "Update Consent".

By this point in the CMP execution cycle, a transaction is sent to the Blockchain network [122], [135], [136] with the consent information from a specific user to a specific study. When consensus [122], [137] is achieved by the participants of the network, the consent is stored in the Blockchain.

Once stored in the Blockchain, the informed consent information from that request is available to all participants of the CMP associated with the study/request. They can query the Blockchain to retrieve the most recent state of users' informed consent. This ensures that the users (in this scenario, the data producers) are empowered by better controlling how their data are used. Data consumers must always

Figure 3: Consent management platform requests for the informed consent list.

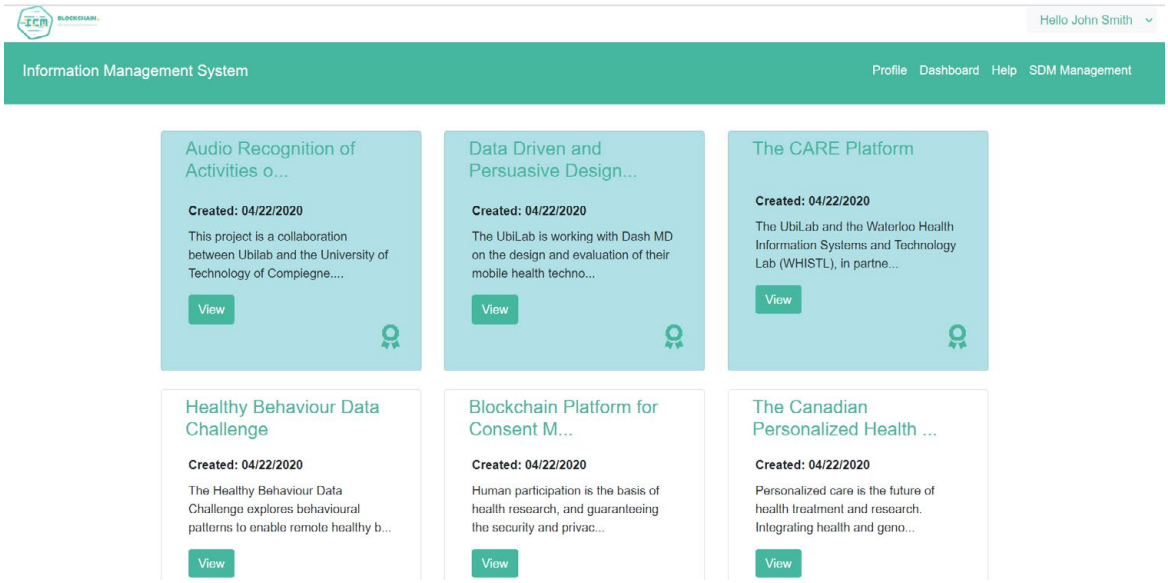
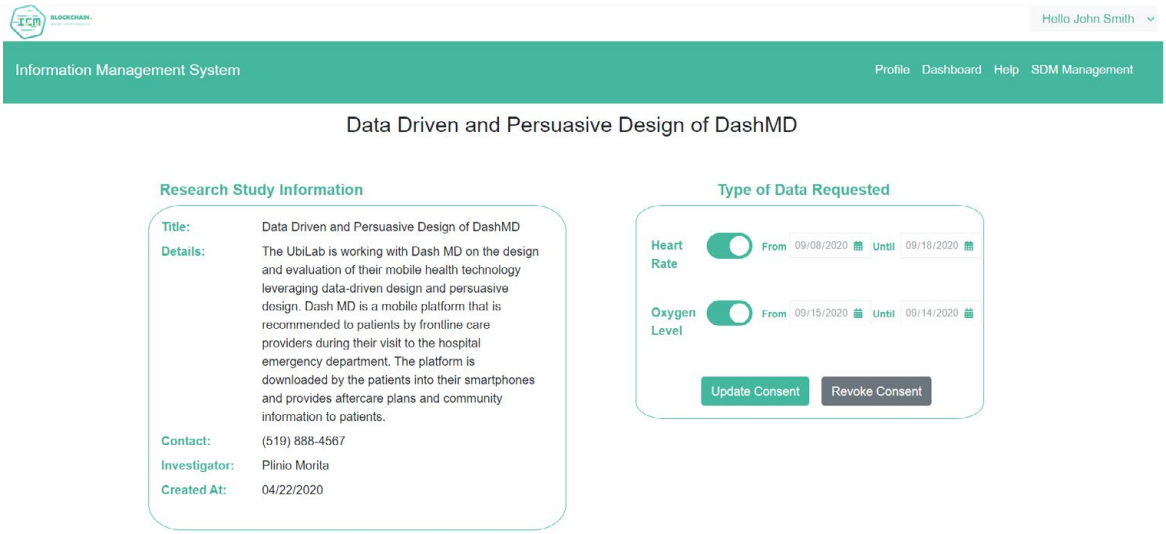


Figure 4: Consent management platform data consumer informed consent request interface.



request reconsent for expired consent forms stored in the Blockchain.

The platform also provides, through the use of Blockchain, the possibility of selecting and managing SDMs. This feature is important for AAL users that desire to elect another person to become their decision-maker. Once the appointed SDM accepts the request, the information about the selected SDM is stored in the Blockchain and becomes available to all participants associated with the study. The transaction is stored on the Blockchain and can be revoked or updated. This feature from the CMP allows AAL care recipients to quickly select trustworthy SDMs immediately. Figure 5 shows the interface that allows users to manage their SDMs. It is worth noting that, for simplicity, one user can be an SDM for multiple users, but each user can only have one SDM.

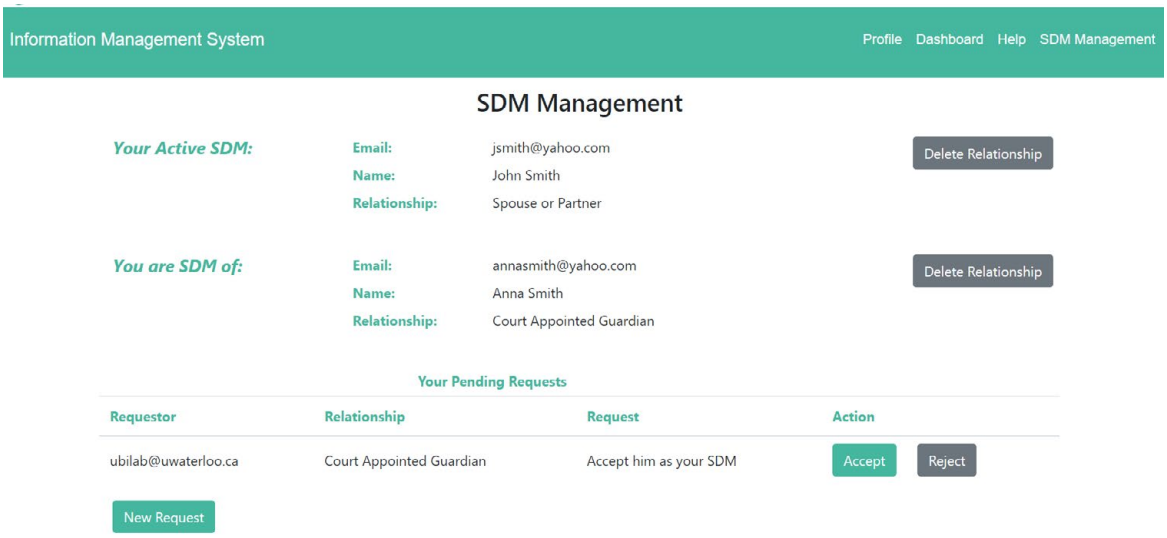
Figure 5 shows the details of the user's current SDM ("Your Active SDM"). Necessary information about the SDM is displayed on the right, followed by a button called "Delete Relationship". This button creates a new transaction with the status of the SDM relationship of that user set to "False". The platform will notify the revoked SDM that they are not allowed to make any further decisions for that user. All decisions over consent now must be performed by the user until they select a new SDM.

The second row from the top shows the details of the user's current SDM ("You are SDM of"). On the right, the user can see details of someone that selected him/her as the SDM. If the "Delete Relationship" button is selected, the user is no longer an SDM for that person. The platforms notify the user that their SDM is no longer available. Finally, a table called "Your Pending Requests" on the bottom shows SDM requests that are pending acceptance by the user.

The prototype of the CMP provides the requirements for the data producers and data consumers. The interests and roles of data auditors (DA) and data custodians in transacting informed consent information with data consumers and producers will be implemented in future iterations. A data auditor represents an organization that enforces laws and regulations [138] over the transactions that take place inside the CMP's Blockchain network. The CMP allows data auditors to use smart contracts [106], [107], [122], [129] as a means to enforce regulations over informed consent and SDM transactions. In the CMP, smart contracts are automated software representations of traditional informed consent and SDM forms [121].

The data auditors must endorse the smart contracts before they are deployed into the Blockchain. Once a contract is deployed, all participants use them to validate a consent transaction and achieve consensus.

Figure 5: Consent management platform that shows the interface for managing substitute decision-maker (SDM) status.



For example, smart contracts can be developed to prevent the sharing of data with non-authorized participants and prevent corrupted data from being stored in the Blockchain. Smart contracts also ensure that data auditors endorse a transaction before it is added to the Blockchain, meaning that the transaction follows laws and regulations properly. Data auditor approval provides the necessary authorization that data custodians need to allow access to user health data.

The data custodians represent participants that are responsible for stored health care data [128], [129]. Custodians must only provide data access to another participant of the CMP if the consent transaction was stored on the Blockchain and is not expired. The Blockchain network provides data custodians with access to its transactions so that they can verify if a data consumer has the proper consent to access a user's data. Figure 6 illustrates the interactions between all the participants of the CMP inside the Blockchain network.

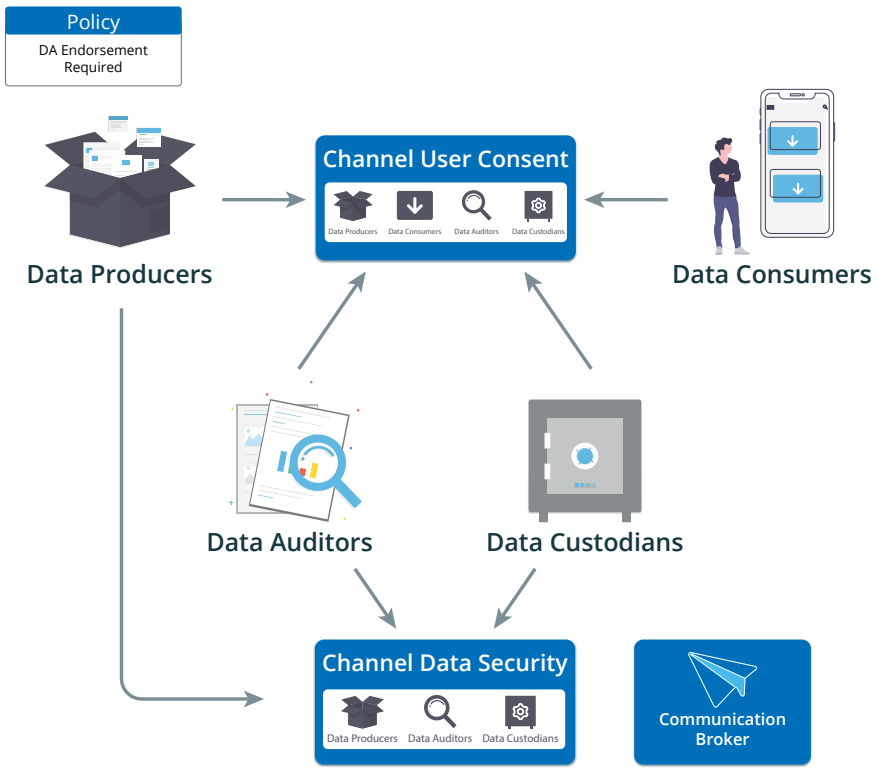
The data auditor organization is also a member of a different channel of communication called Channel Data Security. This channel will hold the members of the network responsible for ensuring that data custodians have the proper consent to store users' health information on their servers. The communication broker is responsible for routing communication between the CMP and the communication channels.

In this network, a consortium [139] is formed by a data producer, a data auditor, a data consumer, and one data custodian. All members of the network have a copy of the Blockchain and smart contracts. When a new consent transaction is sent to the Blockchain, all members execute the proper smart contract over the consent information contained in the transaction to validate it (or not).

In this consortium, a transaction must be endorsed by a data auditor before it is added to the Blockchain. In other words, without the approval of a data auditor, the transaction is rejected (even if the majority of the network has agreed to the transaction). This ensures that no transactions without permission from proper authorities are stored in the Blockchain.

The data custodian, as a member of this channel, knows that the data auditor agreed to that consent if the transaction is valid and stored in the ledger. With the transaction validated, the custodian is authorized to give access to its health care data to the data consumer as long as the custodian respects the restrictions defined by the user or SDM.

Figure 6: Consent management platform Blockchain network participants, consortium, channels, and network policy, which defines that the data auditor's (DA) endorsement for all transactions is mandatory.



4.3 Complexities in the Development of a Blockchain Platform

One consideration when developing a Blockchain network is who will be responsible for hosting the nodes (servers) to operate the network. In a centralized system for AAL technologies, such as a long-term care home that uses connected devices, data would be stored on their private systems and in manufacturers' databases. However, due to Blockchain's decentralized nature, several nodes are needed to operate the network. This issue was highlighted by the interviewed stakeholders, with one stakeholder mentioning that creating a governance structure for Blockchain solutions is very difficult and currently there is no best practice or gold standard for it.

Management of informed consent over a Blockchain network requires defining which member (or members) would be responsible for enforcing regulations and endorsing transactions on the network. For example, a university might be the member responsible for enforcing regulations; this means that the university must endorse all new smart contracts, transactions, and new network members. However, this leaves only one network member vulnerable to legal liabilities, which is not ideal. To overcome such a problem, multiple endorsers at each step of the informed consent lifecycle should be present in the network. Multiple endorsers would balance responsibility, accountability, transparency, and security throughout critical members of the network.

In our system, we propose that a combination of federal and provincial digital health agencies, as represented in Figure 1, should be responsible for integrated networks in different provinces, with at least one agency being the data auditor. An example of a federal agency would be the Canada Health Infoway in Canada [140]; Office of the National Coordinator for Health Information Technology in the United States [141]; and NHS Digital in the UK [142]. Appendix 1 lists provincial digital health agencies in each province that might be possible data auditors for a Blockchain network.

Nonetheless, this increases the complexity of the solution, as for each new endorser present in the network, the complexity of the policies increases since multiple endorsers are now present in the network. In such a network with various endorsers, a smart contract that regulates AAL or informed consent from a study might require endorsements from a unique subset of members of the network. This fact also increases the complexity of the solution since managing such a network requires a dedicated professional to act as an administrator of the network.

Another challenge during proof-of-concept development was ensuring that AAL users did not have to interact with Blockchain directly. Adding this layer of complexity would create a gap of accessibility for our target audience, as older adults typically do not have technology knowledge or experience. For this reason, we proposed the use of Hyperledger Fabric (HF), a permissioned/private Blockchain solution that allows interaction with Blockchain using permissioned applications [122]. These applications are the ones that interact with the Blockchain network, not the end user; this abstraction allows for AAL users to interact with complex systems through user-friendly and accessible interfaces. Further, this abstraction leaves the complexities of managing consent to members of the network.

It is also worth mentioning that our solution stores only informed consent information in the Blockchain, not health data, as our objective is to improve the consent management process. If we were to store EHR from users for instance, our solution would require significantly more infrastructure and a different data management system to be scalable. Moreover, storing health data also increases the liability of our solution regarding laws and regulations.

Our goal is to achieve an electronic informed consent management platform that operates over a Blockchain network consortium and allows for the management of AAL users' informed consent. However, our solution can be extended to offer management of electronic informed consent to other use-cases from the health care domain, including the challenges mentioned in previous sections; whether data are from EHR, supply chain, health insurance, or genomics, the commonality between all clinical research or solutions interested in studying personal health records is the requirement of obtaining and maintaining electronic informed consent from remote participants. Traditional means of obtaining and maintaining informed consent cannot handle large number of participants distributed over large geographical areas and over long periods of time. Our solution offers the electronic infrastructure that researchers need to collect and manage valid informed consent, regardless of which use case or health data type they are dealing with.

During prototype development, we faced challenges regarding the definition of a governance structure for our platform; abstracting the interaction between users and the Blockchain to ensure that individuals without knowledge of the technology could use the platform effectively; and creating a data model that stores all needed information (regarding consent) without scalability issues. We were able to use the Hyperledger Fabric platform, an existing solution in the market which provides the tools and infrastructure to implement a Blockchain network, to achieve our goals.

However, the applicability of the proposed solution in real-world AAL monitoring and research systems is still challenging. Companies and developers that plan to use Blockchain must consider first if this is a suitable solution to achieve their goal. In this work, to ensure that Blockchain can help mitigate trust issues in the consent management process, we first mapped these issues as viewed in Figure 1. Then, we were able to design the platform to minimize them. Once developers are sure that Blockchain is the ideal solution, they will have to model their application by taking into account scalability issues (which will include their data management model) as well as governance model. They will also need to consider interoperability with existing systems and devices as required by the solution, and ensure quality control for all information being stored in the immutable ledger.

5 Standards in AAL and Blockchain

Despite the fact that some standards related to Blockchain were mentioned during the interviews, most stakeholders agreed that there is a lack of standards for Blockchain in health care, particularly when it comes to AAL adoption. Alternative standards on connected devices and health informatics have been used by innovators in the space, in the absence of AAL- and Blockchain-specific standards.

"Despite the fact that some standards related to Blockchain were mentioned during the interviews, most stakeholders agreed that there is a lack of standards for Blockchain in health care, particularly when it comes to AAL adoption."

This section comprises the list of standards, working groups, and technical committees that stakeholders often leverage for their work with AAL technology and/or Blockchain. Opportunities for additional standards and best practices identified by the interviewed stakeholders and through the development of the consent management platform are also discussed.

5.1 Blockchain Standards

Several stakeholders mentioned ISO/TC 307 – *Blockchain and Distributed Ledger Technologies.* This technical committee has three published standards or reports:

- **ISO 22739:2020 – Blockchain and Distributed Ledger Technologies – Vocabulary** is a standard describing the terminology for Blockchain and ledger technologies used for other ISO/TC 307 standards [143].
- **ISO/TR 23455:2019 – Blockchain and Distributed Ledger Technologies — Overview of and Interactions Between Smart Contracts in Blockchain and Distributed Ledger Technology Systems** is a technical report focusing on smart contracts in Blockchain or Distributed Ledger Systems, including how several smart contracts can be implemented and interact [144].
- **ISO/TR 23244:2020 – Blockchain and Distributed Ledger Technologies – Privacy and Personally Identifiable Information Protection Considerations** is a technical report describing privacy and personally identifiable information (PII) issues in the context of Blockchain [145].

In addition, the technical committee has several documents under development that focus on several areas, including privacy and personally identifiable information, reference architecture, and governance [146]. Standards, specifications, or reports under development by this technical committee are listed in Appendix B.

Another initiative mentioned by the stakeholders as a potentially good resource for Blockchain standards was the IEEE Blockchain initiative, which provides several standards covering Blockchain topics such as data exchange, interoperability, and integration with IoT amongst others [147]. These standards, still under development except when noted, include:

- **IEEE 2144.1-2020 – IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management (Published)** – this standard defines a data management framework for Blockchain-based IoT.
- **P2418.1 – Standard for the Framework of Blockchain Use in Internet of Things (IoT)** – this standard "provides a common framework for blockchain usage, implementation, and interaction in Internet of Things (IoT) applications. The framework addresses scalability, security, and privacy challenges with regard to blockchain in IoT" [148].
- **P2418.6 – Standard for the Framework of Distributed Ledger Technology (DLT) Use in Health Care and the Life and Social Sciences** – this standard "provides a common framework for distributed ledger technology (DLT) usage,

implementation, and interaction in health care and the life and social sciences, addressing scalability, security, and privacy challenges" [149]. The goal is to create a standardized and reproducible mechanism in health care focusing on topics such as interoperability, cybersecurity, and compliance with regulatory requirements. This standard was the one standard from IEEE most mentioned in interviews when discussing Blockchain and health care.

- **P2144.1 – Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management** – this standard "defines a framework of blockchain-based Internet of Things (IoT) data management" [150].
- **P2144.2 – Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management** – P2144.2 "defines the functional requirements in data compliance, governance and risk management in the operational process for Blockchain-based IoT data management systems" [151].
- **P2144.3 – Standard for Assessment of Blockchain-based Internet of Things (IoT) Data Management** – P2144.3 "defines the assessment framework for data compliance, governance, and risk management in Blockchain-based IoT data management, provides performance metrics such as availability, security, privacy, integrity, continuance, scalability, etc." [152].

Other standards that are being developed as part of the IEEE Blockchain Initiative are listed in Appendix B.

Ethereum Improvement Proposals (EIP)

While not standards per se, one stakeholder mentioned EIPs as an essential part of the Ethereum Blockchain. An EIP is a design document created by members of the Ethereum community that describes a new feature to improve the Ethereum Blockchain. If approved by the community, the EIP is implemented in the Blockchain [153].

5.2 Opportunities for Standards Development

Following our consultations and platform development, it was identified that there are very few active standards for Blockchain in health care. In the domain of AAL, they are non-existent (although there are standards being developed by IEEE in the field of IoT). Blockchain developers and users currently rely on existing standards focusing on health informatics and IoT to support their use cases.

Existing Blockchain standards are also very recent and do not seem to be widely adopted yet. Indeed, from the documents published by ISO/TC 307, ISO/TR 23244 was published in May 2020 and the standard ISO 22739 was published in July 2020. ISO/TR 23455 was published in September 2019.

According to stakeholders, this is not uncommon for new technologies, and reaching consensus among different domains on the best standards for the industry takes time. With Blockchain, this process may be more complicated as there is a lack of understanding regarding the definition, uses, and limitations of the technology. Opportunities identified for future standards that were deemed essential by stakeholders focused on increased interoperability, enabling the safe and transparent exchange of health data, and compliance with data integrity/privacy regulations. Indeed, these opportunities were in line with several of the main challenges identified in health care today.

For example, currently Electronic Health Records systems do not interact with each other, and standards focusing on how this integration can be achieved using Blockchain would be of great help. Similarly, connected devices collect and store health data using a variety of methods and formats, and also do not integrate well with other sensors. Standards that promote safe and private interoperability, enabling data sharing between devices, individuals, and systems, would go a long way in improving research and applicability of AAL technologies.

The application of privacy by design principles, (e.g., data ownership, access, lifecycle) during the early stages of technology development and use is essential in making this happen. The concept of privacy by design ensures that privacy is proactive, anticipating any privacy issues that may arise, and making sure that countermeasures are embedded in the technology's design [154]. Application of these principles and standards in this direction could be a useful tool to help maintain privacy.

It is interesting to note that the opportunities for standards identified in the interviews are very much in line with standards being developed by ISO/TC 307. Many of the standards or documents under development focus on related issues, from security risks and governance to smart contracts, best practices, and interoperability. In particular, the standard ISO/DIS 23257 is interesting since it considers all these aspects in a reference architecture for distributed ledger systems. Many standards being developed by IEEE can also help with these aspects. However, only one standard to date, P2418.6, focuses on the use of Blockchain for health care. IEEE standards P2144.1, P2144.2, P2144.3, and P2418.1, which deal with IoT, can also help AAL users and developers as they describe topics related to the use of connected devices, although their focus is not on older populations per se and therefore it is not guaranteed that these standards will help AAL practitioners to meet the needs of older populations.

Indeed, as previously mentioned in regard to health care and to AAL, security and privacy are major issues with amplified importance as a result of AAL's frequent use amongst vulnerable populations. Standards that allow the creation of secure, trusted, and verifiable Blockchain systems have the potential to greatly increase the adoption of these systems by the population and enable older adults to age well and in place with the use of technology. While current standards exist that address some of these issues, focusing on health informatics, IoT, or Blockchain, there seems to be a lack of integrated standardized mechanisms that focus on Blockchain applications specifically for Active Assisted Living technologies.

Table 2 provides an overview of the purpose and outcome of opportunities for improvements in the area of Blockchain, health care, and AAL, and lists the challenges in health care that can potentially be improved with these opportunities. These opportunities can be used to further support the development and adoption of standards, regulations, and guidelines. All of the areas mentioned in Table 2 were identified in the literature review and interviews as potential opportunities for improvement in several use cases. During development of the Blockchain for consent management platform, we further identified several needs that could be addressed by some of the items mentioned in Table 2 (marked with CMP on the table).

These include:

- **Knowledge Translation** – Developers faced challenges explaining the platform in simple terms to individuals not associated with Blockchain technology. Best practices on knowledge translation would greatly help researchers and innovators in this space to explain to a general audience the benefits of their projects, increasing technology adoption.
- **Governance** – As described in Figure 6, in order to develop the network it was necessary to define a governance structure. Having already-set standards, guidelines, and best practices would have been of great help during the development process.
- **Privacy by Design, Regulation Compliance, and Ethics** – Specifications for solutions to be compliant with current privacy regulations would have helped the developers in identifying the need for privacy by design methods early in the development process, as well as ensuring that the ethical handling of personal health data is being considered in the solution.
- **Cybersecurity** – Specifications on cybersecurity methods and how to integrate them with Blockchain systems is essential in the development of a Blockchain system.
- **Solution Guidelines for Blockchain in Health Care** – Developers selected Hyperledger Fabric for the project as this framework seemed the most suited for the prototype, providing an easy way to create a secure Blockchain network and define its participants. However, guidelines that provide developers with the benefits and limitations of each existing development framework for specific use cases in health care would have greatly facilitated the selection of the best framework.

It is important to note that some of these items were guided by the GDPR, which provides information related to Knowledge Translation (e.g., definition of actors involved in the process), Cybersecurity, Privacy By Design, and Ethics, such as the right of the data subjects and anonymization protocols [155].

Table 2: Recommended Standards for Blockchain and AAL Technologies.

Name	Purpose and Outcome	Challenges
Interoperability and Data Sharing	Specifications describing protocols for communication and sharing of data between Blockchain solutions and between novel Blockchain solutions and legacy systems, are essential for large-scale adoption and trust of the technology. This is absolutely necessary for AAL applications, which involve several sources of data.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP
Knowledge Translation	One of the main limitations of Blockchain is that currently, there is a general lack of understanding of what the technology entails. Information on how to perform knowledge translation and educate the intended audience about the potential of Blockchain can be of great help in increasing its adoption in health systems.	EHR, Genomics, Consent Management, CMP
Governance	Governance models of Blockchain networks, such as defining the responsible parties and their responsibilities in a Blockchain network, can aid in the smooth development and implementation of Blockchain-based systems in a health care system. For example, a consortium of hospitals utilizing an integrated Blockchain solution would require clear and transparent governance models.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP
Privacy by Design	Specifications relating to data ownership, access, life cycle, and any additional privacy considerations are essential in the implementation of Blockchain systems. This is especially true in health care, which deals with sensitive patient information, and particularly when considering AAL technologies and vulnerable populations.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP
Scalability	Several current Blockchain implementations cannot handle large volumes of data; developers must be careful in their modelling of a Blockchain-based system to ensure that it can be scalable. This is especially true in challenges dealing with large volumes of data, such as EHR and genomics.	EHR, Genomics
Energy Efficiency	Blockchain solutions can use large amounts of energy; specifications on how to reduce this consumption can be of great help in making solutions sustainable.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management
Regulation Compliance	Blockchain-based solutions for health care must be able to comply with regional regulations on the proper handling of personal health data. For example, solutions that handle health data under GDPR jurisdiction must be able to delete individual data.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP
Terminology/ Vocabulary	Definition of actors and stakeholders for various scenarios of use of the Blockchain technology can help with development and implementation. This is particularly true for AAL.	EHR, Genomics, Consent Management
Ethics	Related to privacy, considerations on ethics related to health care and Blockchain must be considered when implementing any system. Since Blockchain is highly correlated with monetization (e.g., cryptocurrency), ethical boundaries and regulations must be established.	EHR, Genomics, CMP

Name	Purpose and Outcome	Challenges
Cybersecurity	Guidelines pertaining to the methods of data collection, such as encryption, anonymization, access control, among others, can make the handling of personal health data more secure.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP
Solution Guidelines for Blockchain in Health Care	There are currently several frameworks for Blockchain development, the Hyperledger Fabric used here being only one of them. Clear guidelines of the benefits and limitations of each framework, in simple terms, could be of great help in minimizing entrance barriers to the Blockchain industry and in assisting developers to select the best solution.	EHR, Supply Chain, Health Insurance, Genomics, Consent Management, CMP

6 Conclusions

Currently, the development and use of new technologies that collect diverse and real-time health data calls for new solutions that allow for the integration of these data with health care systems and allow different stakeholders in the industry to improve their processes and methods. Among these technologies, Blockchain has recently presented itself as a tool with great potential and popularity in several sectors, including health care. However, as with every new technology, the potential benefits must be weighed against initial over-expectations and limitations of the technology. To this end, one of the main goals of this report was to present an overview of current challenges faced by the health care industry for which Blockchain could provide a viable solution. Through a literature review and interviews with stakeholders, we summarized and discussed the following five challenges:

- **EHR** – Lack of interoperability and data sharing between electronic medical records;
- **Supply Chain** – Tracking and tracing of drug (and food) supply chain products;
- **Health Insurance** – Inefficiencies and the lack of synergy between payers, providers, and patients in terms of health insurance;
- **Genomics** – Lack of interoperability and availability of genomic data; and
- **Consent Management** – Security and privacy of health data collection and difficulty in collecting informed consent.

Blockchain, an immutable ledger in which all participants view a tamperproof log of assets and data, can address some of these challenges and has been explored by a variety of innovators. The immaturity of the field, the sensitivity of the information, and a lack of standards and best practices dealing with Blockchain technology represent barriers to adoption. While standards for Blockchain use are currently in development and address issues such as interoperability, security and privacy, governance, and other technology-related issues, there are very few standards that focus on Blockchain and health care specifically, or on the use of AAL technology [2]. Consent management is of great importance when dealing with AAL technology, as AAL often involves the remote collection and use of health data from several sources.

The Blockchain for consent management platform developed as part of this project demonstrated that these technologies can be used to provide controlled access to informed consent information, as long as the necessary policies and regulations are in place. For many of these aspects, standards-based solutions could help provide greater guidance for the development, implementation, and maintenance of such a system.

In conclusion, the development and implementation of Blockchain solutions can mitigate several issues in health care, such as interoperability, privacy, and data sharing. However, developers must carefully consider trade-offs in the design of their solutions including the governance structure of their networks and their data management approaches. Blockchain can also be of great help in improving the AAL field, particularly when it comes to ensuring that informed consent is being collected and managed in an efficient and ethical manner. Finally, while a number of Blockchain standards are currently in development, several areas for improvement pertaining to Blockchain in health care remain.

References

[1] S. Ditta, J. Thirgood, and M. C. Urban, "The rise of the sharing economy: Exploring standards-based solutions," CSA Group, Toronto, ON, CAN, Feb. 2017. Available: https://www.csagroup.org/wp-content/uploads/CSA_Group_Sharing_Economy_Research_Report.pdf

[2] L. X. Fadrique, D. Rahman, and P. P. Morita, "The active assisted living landscape in Canada," CSA Group, Toronto, ON, CAN, May 2018. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-AAL.pdf

[3] P. Novitzky *et al.,* "A review of contemporary work on the ethics of ambient assisted living technologies for people with dementia," *Sci. Eng. Ethics,* vol. 21, no. 3, pp. 707–765, 2015.

[4] "Population of Latin America and the Caribbean," Worldometer. [Online]. Available: https://www.worldometers.info/world-population/latin-america-and-the-caribbean-population/ (accessed Aug. 17, 2020).

[5] "Population of Asia," Worldometer. [Online]. Available: https://www.worldometers.info/world-population/asia-population/ (accessed Aug. 17, 2020).

[6] Government of Canada, "Government of Canada — Action for seniors report," 2014. [Online]. Available: https://www.canada.ca/en/employment-social-development/programs/seniors-action-report.html

[7] E. Wicklund, "Using telehealth, mHealth technology to help seniors age in place," 2018. [Online]. Available: https://mhealthintelligence.com/features/using-telehealth-mhealth-technology-to-help-seniors-age-in-place

[8] N. Farber, D. Shinke, J. Lynott, W. Fox-Grage, and R. Harrell, "Aging in place: A state survey of livability policies and practices," Dec. 2011. [Online]. Available: https://assets.aarp.org/rgcenter/ppi/liv-com/aging-in-place-2011-full.pdf

[9] PwC, "Building block(chain)s for a better planet," 2018. [Online]. Available: https://www.pwc.com/gx/en/services/sustainability/building-blockchains-for-the-earth.html

[10] M. A. Farage, K. W. Miller, F. Ajayi, and D. Hutchins, "Design principles to accommodate older adults," *Glob. J. Health Sci.,* vol. 4, no. 2. pp. 2-25, 2012.

[11] "AAL Home 2020," AAL Programme. [Online]. Available: http://www.aal-europe.eu/ (accessed Feb. 10, 2020).

[12] F. M. Bublitz *et al.,* "Disruptive technologies for environment and health research: An overview of artificial intelligence, blockchain, and internet of things," *Int. J. Environ. Res. Public Health,* vol. 16, no. 20, pp. 1–24, 2019.

[13] L. Bartlett and H. S. Fowler, "A Canadian roadmap for an aging society," CSA Group, Toronto, ON, CAN, 2019. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Aging-Society-Standard-Roadmap.pdf

[14] D. Pineda and M. C. Urban, *Inside the Black Blocks,* Mowat Centre, Toronto, ON, CAN, Aug. 16, 2018. Available: https://munkschool.utoronto.ca/mowatcentre/inside-the-black-blocks/

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," Proc. – *2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017,* pp. 557–564, Oct. 2017.

[16] D. Furlonger and J. Haner, "What Insurance CIOs Need to Know About Blockchain." Gartner Research, Stamford, CT, USA, May 18, 2016.

[17] "CoinDesk — Leader in blockchain news." [Online]. Available: https://www.coindesk.com/ (accessed May 18, 2020).

[18] "Cointelegraph Bitcoin & Ethereum blockchain news." [Online]. Available: https://cointelegraph.com/ (accessed May 18, 2020).

[19] "Medium – Get smarter about what matters to you." [Online]. Available: https://medium.com/ (accessed May 18, 2020).

[20] "Electronic Health Records | Canada Health Infoway." [Online]. Available: https://www.infoway-inforoute.ca/en/solutions/digital-health-foundation/electronic-health-records (accessed Feb. 12, 2020).

[21] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.,* vol. 135, no. 1, pp. 62-75, Jun. 2019.

[22] R. Sharma, "BLOCKCHAIN: The magic pill to alleviate the pain points of the healthcare industry?," 2018. [Online]. Available: https://www.fccco.org/post/blockchain-in-healthcare.

[23] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. – 2016 2nd Int. Conf. Open Big Data, OBD 2016,* pp. 25–30, 2016.

[24] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *J. Med. Internet Res.,* vol. 21, no. 2, pp. 1–12, 2019.

[25] A. C. Ekblaw, "MedRec: Blockchain for medical data access, permission management and trend analysis," 2017. [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/109658/987247095-MIT.pdf?sequence=1%0Ahttps://dspace.mit.edu/handle/1721.1/109658

[26] B. Siwicki, "The next big thing in pharmacy supply chain: Blockchain | Healthcare IT News." [Online]. Available: https://www.healthcareitnews.com/news/next-big-thing-pharmacy-supply-chain-blockchain (accessed Oct. 9, 2018).

[27] "Drug Supply Chain Security Act (DSCSA), "FDA. [Online]. Available: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa (accessed Feb. 12, 2020).

[28] "Products | modum.io." [Online]. Available: https://www.modum.io/solutions/applications (accessed Oct. 9, 2018).

[29] S. Uhlmann, "Reducing counterfeit products with blockchains," 2017. [Online]. Available: https://www.merlin.uzh.ch/contributionDocument/download/10024

[30] "We are modum | modum.io." [Online]. Available: https://modum.io/ (accessed Oct. 9, 2018).

[31] Modum, "Data integrity for supply chain operations," 2017. [Online]. Available: https://assets.modum.io/wp-content/uploads/2017/08/modum-whitepaper-v.-1.0.pdf

[32] J. Adams, "CareX white paper," 2018. [Online]. Available: https://icosbull.com/eng/ico/carex/whitepaper

[33] A. Albeyatti, "MedicalChain," 2017. [Online]. Available: https://medicalchain.com/en/whitepaper/

[34] "DokChain," PokitDok. [Online]. Available: https://pokitdok.com/dokchain/ (accessed Sept. 26, 2018).

[35] W. B. Smith, "DokChain: Intelligent automation in healthcare transaction processing," 2018. [Online]. Available: https://pokitdok.com/wp-content/uploads/2018/02/DokChain_Whitepaper.pdf

[36] B. Brennan, "DokChain by PokitDoc – Blockchain healthcare," Blockchain Healthcare Review, May 8, 2017. [Online]. Available: https://blockchainhealthcarereview.com/dokchain-by-pokitdoc-blockchain-for-healthcare/.

[37] "CareX – Blockchain platform." [Online]. Available: https://carex.tech/ (accessed Nov. 22, 2018).

[38] E. Stoffregen, "Blockchain healthcare ecosystem in 2018." [Online]. Available: https://medium.com/@erikstoffregen/blockchain-healthcare-ecosystem-d21631024454 (accessed Nov. 22, 2018).

[39] "Medicalchain – Blockchain for electronic health records." [Online]. Available: https://medicalchain.com/en/ (accessed Feb. 27, 2019).

[40] "Citizen health | Rebuilding healthcare for the next generation." [Online]. Available: https://citizenhealth.io/ (accessed Nov. 22, 2018).

[41] "Humantiv | A citizen health development." [Online]. Available: https://citizenhealth.io/humantiv/ (accessed Nov. 22, 2018).

[42] "Medoplex – citizen health." [Online]. Available: https://citizenhealth.io/medoplex/ (accessed Nov. 22, 2018).

[43] Bitcoin Chaser, "BlockRX ICO: Blockchain to prevent counterfeit drugs." [Online]. Available: https://bitcoinchaser.com/ico-hub/blockrx-ico-interview/ (accessed Nov. 7, 2018).

[44] "ICO Alert Report: BlockRx." [Online]. Available: https://blog.icoalert.com/ico-alert-report-blockrx (accessed Nov. 7, 2018).

[45] Embleema, "Embleema whitepaper," 2018. [Online]. Available: https://icocube.io/uploads/Embleema.pdf

[46] D. Grishin, K. Obbad, P. Estep, M. Cifric, Y. Zhao, and G. Church, "Blockchain-enabled genomic data sharing and analysis platform," 2018. [Online]. Available: https://www.nebulagenomics.io/assets/documents/NEBULA_whitepaper_v4.52.pdf

[47] N. Kulemin, S. Popov, and A. Gorbachev, "The zenome project : White paper blockchain-based genomic ecosystem," 2017. [Online]. Available: https://zenome.io/download/whitepaper.pdf

[48] K. Benke and G. Benke, "Artificial intelligence and big data in public health," *Int. J. Environ. Res. Public Health,* vol. 15, no. 12, 2018.

[49] U. Gupta, "Informed consent in clinical research: Revisiting few concepts and areas," *Perspect. Clin. Res.,* vol. 4, no. 1, p. 26, 2013.

[50] D. Takahashi, "Hu-manity.co uses IBM blockchain to give you the right to control your personal data," VentureBeat, Sept. 6, 2018. [Online]. Available: https://venturebeat.com/2018/09/06/hu-manity-co-uses-ibm-blockchain-to-give-you-the-right-to-control-your-personal-data/

[51] "IBM - Announcements." [Online]. Available: https://newsroom.ibm.com/2018-09-06-Hu-manity-co-Collaborates-with-IBM-Blockchain-on-Consumer-App-to-Manage-Personal-Data-Property-Rights (accessed May 15, 2020).

[52] A. Alexandre, "New bitfury joint project to manage medical data permissions with blockchain tech," April 2019. [Online]. Available: https://cointelegraph.com/news/new-bitfury-joint-project-to-manage-medical-data-permissions-with-blockchain-tech

[53] Bitfury, "Bitfury announces blockchain-based consent management system; partners with Hancom to distribute Crystal platform." TokenPost. [Online]. Available: https://tokenpost.com/Bitfury-announces-blockchain-based-consent-management-system-partners-with-Hancom-to-distribute-Crystal-platform-1603 (accessed May 15, 2020).

[54] "MedRec." [Online]. Available: https://medrec.media.mit.edu/ (accessed Oct. 3, 2018).

[55] "PatientTruth – Embleema – Blockchain for real-world evidence." [Online]. Available: https://www.embleema.com/patienttruth/ (accessed Nov. 8, 2018).

[56] A. Kovach and G. Ronai, "MyMEDIS: A new medical data storage and access system," 2018. [Online]. Available: https://mymedis.in/documents/MEDIS-White-Paper.pdf

[57] "MEDIS – Globally decentralized medical data store and blockchain-based ecosystem." [Online]. Available: https://mymedis.in/ (accessed Mar. 12, 2019).

[58] I. Allison, "Gem shows off first blockchain application for health claims," *International Business Times,* May 20, 2017. [Online]. Available: https://www.ibtimes.co.uk/gem-shows-off-first-blockchain-application-health-claims-1622574

[59] "Health | Gem." [Online]. Available: https://enterprise.gem.co/health/ (accessed Oct. 4, 2018).

[60] P. Rizzo, "Gem partners with Philips for blockchain healthcare initiative – CoinDesk," April 26, 2016. [Online]. Available: https://www.coindesk.com/gem-philips-blockchain-healthcare/

[61] J. Redman, "Gem Health unveils medical management blockchain platform," Bitcoin. Apr. 27, 2016. [Online]. Available: https://news.bitcoin.com/gem-health-blockchain-medical-mgmt/

[62] J. Shieber, "Gem looks to CDC and European giant Tieto to take blockchain into healthcare," TechCrunch, Sept. 25, 2017. [Online]. Available: https://techcrunch.com/2017/09/25/gem-looks-to-cdc-and-european-giant-tieto-to-take-blockchain-into-healthcare/

[63] "Block Verify." [Online]. Available: http://www.blockverify.io/ (accessed Oct. 9, 2018).

[64] C. Hulseapple, "Block verify uses blockchains to End counterfeiting and 'make world more honest,'" Cointelegraph, Mar. 13, 2015. [Online]. Available: https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest

[65] N. De, "Pharma giant Merck eyes blockchain for fighting counterfeit meds," CoinDesk, Jun. 25, 2018. [Online]. Available: https://www.coindesk.com/merck-proposes-blockchain-platform-for-combat-counterfeiters/

[66] B. Haring, "Blockchain patent filed by pharmaceutical giant Merck & Co.,:"BlockTribune. [Online]. Available: https://blocktribune.com/blockchain-patent-filed-by-pharmaceutical-giant-merck-co/ (accessed Nov. 7, 2018).

[67] A. Stanley, "Ready to rumble: IBM launches Food Trust blockchain for commercial use," Forbes, Oct. 8, 2018. [Online]. Available: https://www.forbes.com/sites/astanley/2018/10/08/ready-to-rumble-ibm-launches-food-trust-blockchain-for-commercial-use/#68bf18817439

[68] IBM, "IBM Food Trust expands blockchain network to foster a safer, more transparent and efficient global food system," Aug. 10, 2018. [Online]. Available: https://newsroom.ibm.com/2018-10-08-IBM-Food-Trust-Expands-Blockchain-Network-to-Foster-a-Safer-More-Transparent-and-Efficient-Global-Food-System-1

[69] IBM Blockchain, "IBM Food Trust," 2018. [Online]. Available: https://www.ibm.com/blockchain/solutions/food-trust

[70] IBM Blockchain, "Walmart's food safety solution using IBM Food Trust built on the IBM blockchain platform," YouTube. [Online]. Available: https://www.youtube.com/watch?time_continue=173&v=SV0KXBxSoio (accessed Sep. 26, 2018).

[71] M. Huillet, "Alibaba's Ant Financial to launch blockchain backend-as-a-service platform," Cointelegraph, Sept. 21, 2018. [Online]. Available: https://cointelegraph.com/news/alibabas-ant-financial-to-launch-blockchain-backend-as-a-service-platform

[72] "Ant Financial is launching a blockchain app to tackle food fraud," CoinDesk. [Online]. Available: https://www.coindesk.com/ant-financial-is-launching-a-blockchain-app-to-tackle-food-fraud/ (accessed Oct. 18, 2018).

[73] "Benefits Management," PokitDok. [Online]. Available: https://pokitdok.com/business/benefits-management/ (accessed Oct. 2, 2018).

[74] "Real-time insurance eligibility verification software," PokitDok. [Online]. Available: https://pokitdok.com/business/insurance-eligibility-verification/ (accessed Oct. 2, 2018).

[75] "Real-time pharmacy benefits and price transparency," PokitDok. [Online]. Available: https://pokitdok.com/business/pharmacy/ (accessed Oct. 2, 2018).

[76] "Healthcare claims processing software," PokitDok. [Online]. Available: https://pokitdok.com/business/claims-management/ (accessed Oct. 3, 2018).

[77] "Autonomous auto-adjudication 101: Blockchains in healthcare," PokitDok. [Online]. Available: https://blog.pokitdok.com/autonomous-auto-adjudication-101/ (accessed Oct. 3, 2018).

[78] "Healthcare propensity to pay," PokitDok. [Online]. Available: https://pokitdok.com/business/payment-risk/ (accessed Oct. 2, 2018).

[79] "Patient access solutions," PokitDok. [Online]. Available: https://pokitdok.com/business/patient-access-solutions/ (accessed Oct. 3, 2018).

[80] "Payspan." [Online]. Available: https://payspan.com/ (accessed Nov. 8, 2018).

[81] Payspan, "How blockchain can connect payers, providers and consumers." [Online]. Available: https://payspan.com/wp-content/uploads/2018/02/Payspan-white-paper-February-2018.pdf (accessed Mar. 3, 2021).

[82] "Nebula Genomics." [Online]. Available: https://www.nebula.org/ (accessed Nov. 12, 2018).

[83] "LunaDNA frequently asked questions." [Online]. Available: https://lunadna.com/faq.html (accessed Nov. 12, 2018).

[84] "About LunaDNA Learn more about the LunaDNA team and company." [Online]. Available: https://lunadna.com/about.html (accessed Nov. 12, 2018).

[85] M. Heltzen, "Interview with Luna DNA's co-founder and president Dawn Barry," AllSeq. [Online]. Available: http://allseq.com/interview-luna-dnas-co-founder-president-dawn-barry/ (accessed Nov. 12, 2018).

[86] B. Bigelow, "Xconomy: Luna DNA uses blockchain to share genomic data as a 'public benefit,'" Xconomy, Jan. 22, 2018. [Online]. Available: https://xconomy.com/san-diego/2018/01/22/luna-dna-uses-blockchain-to-share-genomic-data-as-a-public-benefit/

[87] C. Farr and A. Levy, "Luna Coin project: Sell your genetic data for crypto tokens," CNBC, Dec. 8, 2017. [Online]. Available: https://www.cnbc.com/2017/12/18/luna-coin-project-sell-your-genetic-data-for-crypto-tokens.html

[88] Shivom, "Project SHIVOM (Official Video): Powering the Next Era of Genomics through Blockchain," YouTube. [Online]. Available: https://www.youtube.com/watch?v=jce9vB5zbps (accessed Nov. 14, 2018).

[89] "Shivom: Empowering the next era of genomics, blockchain & precision medicine." [Online]. Available: https://shivom.io/ (accessed Nov. 14, 2018).

[90] W. Thrill, "Shivom: The uncanny synergy of blockchain and genomics," Hackernoon, May 28, 2018. [Online]. Available: https://hackernoon.com/shivom-the-uncanny-synergy-of-blockchain-and-genomics-e1ca7f2a0173

[91] Shivom, "SHIVOM INNOVATION COUNCIL," YouTube. [Online]. Available: https://www.youtube.com/watch?v=UXEz-11inPE (accessed Nov. 14, 2018).

[92] "Zenome - Home." [Online]. Available: https://zenome.io/ (accessed Nov. 15, 2018).

[93] W. Thrill, "EncrypGen uses blockchain technology to store and manage DNA profiles," Hackernoon, Jan. 23, 2018. [Online]. Available: https://hackernoon.com/encrypgen-uses-blockchain-technology-to-store-and-manage-dna-profiles-a920e898b6a8

[94] "EncrypGen: Gene-Chain DNA data marketplace buy sell genomic data." [Online]. Available: https://encrypgen.com/encrypgen-gene-chain-dna-data-marketplace/ (acessed Nov. 15, 2018).

[95] "Marketplace partners – EncrypGen." [Online]. Available: https://encrypgen.com/marketplace-partners/ (accessed Nov. 15, 2018).

[96] "Home – EncrypGen | The DNA Data Marketplace – EncrypGen." [Online]. Available: https://encrypgen.com/ (accessed Nov. 15, 2018).

[97] A. Antonovici, "S Korea's Macrogen to leverage blockchain for genomic data," Cryptovest, Aug. 7, 2018. [Online]. Available: https://cryptovest.com news/s-koreas-macrogen-to-leverage-blockchain-for-genomic-data/

[98] N. Say, "Macrogen develops blockchain platform to share genetic data." [Online]. Available: https://blockonomi.com/macrogen-blockchain/ (accessed Oct. 10, 2018).

[99] S. Ji-young, "Korea's Macrogen, bigster to create blockchain-based medical data platform," *The Korea Herald,* Aug. 6, 2018. [Online]. Available: http://www.koreaherald.com/view.php?ud=20180806000646

[100] "HealthVerity Consent," HealthVerity. [Online]. Available: https://healthverity.com/solutions/healthverity-consent/ (accessed May 21, 2020).

[101] A. Hern, "Google's DeepMind plans bitcoin-style health record tracking for hospitals," *The Guardian,* Mar. 9, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/mar/09/google-deepmind-health-records-tracking-blockchain-nhs-hospitals

[102] M. Suleyman and B. Laurie, "Trust, confidence and Verifiable Data Audit," DeepMind Blog, Mar. 9, 2017. [Online]. Available: https://deepmind.com/blog/trust-confidence-verifiable-data-audit/

[103] "DeepMind." [Online]. Available: https://deepmind.com/ (accessed Mar. 3, 2021).

[104] C. Metz, "Google DeepMind's untrendy play to make the blockchain actually useful," *Wired,* Mar. 2017. [Online]. Available: https://www.wired.com/2017/03/google-deepminds-untrendy-blockchain-play-make-actually-useful/

[105] J. Powles and H. Hodson, "Google DeepMind and healthcare in an age of algorithms," *Health Technol. (Berl).,* vol. 7, no. 4, pp. 351–367, 2017.

[106] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials,* vol. 18, no. 1, p. 335, Dec. 2017.

[107] D. M. Maslove, J. Klein, K. Brohman, and P. Martin, "Using blockchain technology to manage clinical trials data: A proof-of-concept study," *JMIR Med. Informatics,* vol. 6, no. 4, p. e11949, 2018.

[108] D. Wiljer and S. Brudnicki, "Bringing blockchain to healthcare for a new view on data," IBM, Aug. 2019. [Online]. Available: https://www.ibm.com/blogs/think/2019/08/bringing-blockchain-to-healthcare-for-a-new-view-on-data/

[109] Ledger Insights, "Canadian hospital collaborates with IBM for health consent blockchain," 2020. [Online]. Available: https://www.ledgerinsights.com/health-consent-blockchain-university-health-network-uhn/ (accessed May 25, 2020).

[110] University Health Network, "Clinician engagement, Local Impact Awards, budget risk meetings and beyond," 2019. [Online]. Available: https://www.uhn.ca/corporate/AboutUHN/Updates_from_CEO/Pages/Clinician_engagement_Local_Impact_Awards_budget_risk_meetings_and_beyond.aspx (accessed May 24, 2020).

[111] P. E. Velmovitsky and P. P. Morita, "Blockchain platform for consent management in ambient assisted living – Poster presentations," AAL Forum, 2019. [Online]. Available: https://www.aalforum.eu/about/poster-presentations-aal-forum-2019/

[112] C. Gorenflo, L. Golab, and S. Keshav, "Mitigating trust issues in electric vehicle charging using a blockchain," *e-Energy '19: Proceedings of the Tenth ACM International Conference on Future Energy Systems,* 2019, pp. 160–164.

[113] Government of Canada, "Notice: Medical device cybersecurity," Aug. 15, 2018. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/announcements/notice-cybersecurity.html.

[114] "Guidances with digital health content," FDA. [Online]. Available: https://www.fda.gov/medical-devices/digital-health/guidances-digital-health-content (accessed Apr. 29, 2020).

[115] "Medical devices," European Medicines Agency. [Online]. Available: https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices (accessed Apr. 29, 2020).

[116] A. Thorogood, H. Simkevitz, M. Phillips, E. S. Dove, and Y. Joly, "Protecting the privacy of Canadians' health information in the cloud," *Can. J. Law Technol.,* vol. 14, no. 1, 2017.

[117] *Personal Information Protection and Electronic Documents Act* (PIPEDA). 2000. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[118] "PIPEDA in brief – Office of the Privacy Commissioner of Canada." [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ (accessed Nov. 15, 2018).

[119] "Summary of privacy laws in Canada," Office of the Privacy Commissioner of Canada. [Online]. Available: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-3-1 (accessed Jan. 23, 2020).

[120] "HIPAA Compliance Checklist," HIPAA Journal. [Online]. Available: https://www.hipaajournal.com/hipaa-compliance-checklist/ (accessed Jan. 22, 2020).

[121] University Health Network, "Substitute decision makers and naming a power of attorney for personal care information for patients and families," 2018. [Online]. Available: https://www.uhn.ca/PatientsFamilies/Health_Information/Health_Topics/Documents/Substitute_Decision_Maker_and_Naming_an_Attorney_for_Personal_Care.pdf

[122] E. Androulaki *et al.,* "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *EuroSys '18: Proceedings of the Thirteenth EuroSys Conference,* 2018, pp. 1-15.

[123] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Mar. 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[124] C. Grant and A. Osanloo, "Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your 'house,'" *Adm. Issues J. Educ. Pract. Res.,* vol. 4, no. 2, pp. 12–26, 2014.

[125] Y. Omran, M. Henke, R. Heines, and E. Hofmann, "Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective," presented at the 26th IPSERA Conference, Budapest/Balantonfured, Apr. 9-12, 2017.

[126] "Electronic Health Records," Canada Health Infoway. [Online]. Available: https://www.infoway-inforoute.ca/en/solutions/digital-health-foundation/electronic-health-records (accessed Sep. 27, 2018).

[127] "It's working for you," eHealth Ontario. [Online]. Available: https://www.ehealthontario.on.ca/en/ (accessed Jul. 24, 2020).

[128] J. Fingberg, M. Hansen, H. Krasemann, and J. Wright, "Integrating data custodians in eHealth grids: A digest of security and privacy aspects," paper presented at the Informatik 2006 Conference, Dresden, Germany, Oct. 2-6, 2006.

[129] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access,* vol. 5, pp. 14757–14767, Jul. 2017.

[130] P. P. Morita, "Design of mobile health technology," in *Design for Health: Applications of Human Factors,* A. Sethumadhavan and F. Sasangohar, Eds., New York, NY: Academic Press 2020, pp. 87–102.

[131] S. Goyal, P. Morita, G. F. Lewis, C. Yu, E. Seto, and J. A. Cafazzo, "The systematic design of a behavioural mobile health application for the self-management of type 2 diabetes," *Can. J. Diabetes,* vol. 40, no. 1, pp. 95–104, Feb. 2016.

[132] P. P. Morita *et al.,* "A patient-centered mobile health system that supports asthma self-management (breathe): Design, development, and utilization.," *JMIR mHealth uHealth,* vol. 7, no. 1, p. e10956, Jan. 2019.

[133] M. Sultan, K. Kuluski, W. J. McIsaac, J. A. Cafazzo, and E. Seto, "Turning challenges into design principles: Telemonitoring systems for patients with multiple chronic conditions," *Health Informatics J.,* vol. 25, no. 4, pp. 1188–1200, Dec. 2019.

[134] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, "The rise of consumer health wearables: Promises and barriers," *PLoS Med.,* vol. 13, no. 2, Feb. 2016.

[135] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 09, no. 10, pp. 533–546, Oct. 2016.

[136] "How Fabric networks are structured," Hyperledger Fabric. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html (accessed May 23, 2020).

[137] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM,* vol. 59, no. 11, pp. 15–17, Oct. 2016.

[138] "The 10 privacy principles of PIPEDA: #1 Accountability." PrivacySense.net. [Online]. Available: http://www.privacysense.net/10-privacy-principles-of-pipeda-accountability/ (accessed Jul. 24, 2020).

[139] "Hyperledger Fabric Network," Hyperledger Fabric. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/network/network.html#defining-a-consortium (accessed May 28, 2020).

[140] "About Canada Health Infoway," Canada Health Infoway. [Online]. Available: https://www.infoway-inforoute.ca/en/about-us (accessed Jun. 1, 2020).

[141] "About ONC," Office of the National Coordinator for Health Information Technology. [Online]. Available: https://www.healthit.gov/topic/about-onc (accessed Jun. 1,2020).

[142] "Home," NHS Digital. [Online]. Available: https://digital.nhs.uk/ (accessed Jun. 1, 2020).

[143] ISO, "ISO 22739:2020(en), Blockchain and distributed ledger technologies — Vocabulary." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en (accessed Nov. 11, 2020).

[144] ISO, "ISO/TR 23455:2019, Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems." [Online]. Available: https://www.iso.org/standard/75624.html?browse=tc (accessed Apr. 24, 2020).

[145] ISO, "ISO/TR 23244:2020, Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations." [Online]. Available: https://www.iso.org/standard/75061.html (accessed Nov. 11, 2020).

[146] ISO, "ISO/TC 307, Blockchain and distributed ledger technologies." [Online]. Available: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0 (accessed: Apr. 24, 2020).

[147] IEEE, "Standards, IEEE blockchain initiative." [Online]. Available: https://blockchain.ieee.org/standards (accessed Apr. 24, 2020).

[148] IEEE, "P2418.1, Standard for the framework of blockchain use in Internet of Things (IoT)." [Online]. Available: https://standards.ieee.org/project/2418_1.html (accessed Apr. 24, 2020).

[149] IEEE, "P2418.6, Standard for the framework of distributed ledger technology (DLT) use in healthcare and the life and social sciences." [Online]. Available: https://standards.ieee.org/project/2418_6.html (accessed Nov. 5, 2018).

[150] IEEE, "P2144.1, IEEE draft standard for framework of blockchain-based Internet of Things (IoT) data management." [Online]. Available: https://standards.ieee.org/project/2144_1.html (accessed Nov. 16, 2020).

[151] IEEE, "P2144.2, Standard for functional requirements in blockchain-based Internet of Things (IoT) data management." [Online]. Available: https://standards.ieee.org/project/2144_2.html (accessed Nov. 16, 2020).

[152] IEEE, "P2144.3, Standard for assessment of blockchain-based Internet of Things (IoT) data management." [Online]. Available: https://standards.ieee.or https://standards.ieee.org/project/2144_3.html (accessed Nov. 16, 2020).

[153] "EIP 1: EIP Purpose and Guidelines." [Online]. Available: https://eips.ethereum.org/EIPS/eip-1 (accessed Apr. 24, 2020).

[154] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles." [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (accessed Apr. 24, 2020).

[155] GDPR, "Art. 4 GDPR – Definitions." GDPR.eu, 2021. [Online]. Available: https://gdpr.eu/article-4-definitions/?cn-reloaded=1 (accessed Jan. 20, 2021).

[156] ISO, "ISO/CD TR 3242, Blockchain and distributed ledger technologies – Use cases." [Online]. Available: https://www.iso.org/standard/79543.html?browse=tc (accessed Nov. 11, 2020).

[157] ISO, "ISO/AWI TR 6039, Blockchain and distributed ledger technologies – Identifiers of subjects and objects for the design of blockchain systems." [Online]. Available: https://www.iso.org/standard/81978.html (accessed Nov. 11, 2020).

[158] ISO, "ISO/CD TR 23245.2, Blockchain and distributed ledger technologies – Security risks, threats and vulnerabilities." [Online]. Available: https://www.iso.org/standard/75062.html (accessed Nov. 11, 2020).

[159] ISO, "ISO/WD TR 23249, Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management." [Online]. Available: https://www.iso.org/standard/80805.html (accessed Nov. 11, 2020).

[160] ISO, "ISO/DIS 23257, Blockchain and distributed ledger technologies – Reference architecture." [Online]. Available: https://www.iso.org/standard/75093.html (accessed Nov. 16, 2020).

[161] ISO, "ISO/DTS 23258, Blockchain and distributed ledger technologies – Taxonomy and Ontology." [Online]. Available: https://www.iso.org/standard/75094.html (accessed Nov. 16, 2020).

[162] ISO, "ISO/AWI TS 23259, Blockchain and distributed ledger technologies – Legally binding smart contracts." [Online]. Available: https://www.iso.org/standard/75095.html (accessed Nov. 16, 2020).

[163] ISO, "ISO/PRF TR 23576, Blockchain and distributed ledger technologies – Security management of digital asset custodians." [Online]. Available: https://www.iso.org/standard/76072.html (accessed Nov. 16, 2020).

[164] ISO, "ISO/DTS 23635, Blockchain and distributed ledger technologies – Guidelines for governance." [Online]. Available: https://www.iso.org/standard/76480.html (accessed Nov. 16, 2020).

[165] ISO, "ISO/WD TR 23644, Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management (TADIM)." [Online]. Available: https://www.iso.org/standard/81773.html (accessed Nov. 16. 2020).

[166] ISO, "ISO/AWI TR 23642, Blockchain and distributed ledger technologies – Overview of smart contract security good practice and issues." [Online]. Available: https://www.iso.org/standard/81772.html?browse=tc (accessed Nov. 16, 2020).

Appendix A – Digital Health Agencies/ EHRs in Each Province/Territory

British Columbia

1. Digital Health Hub: http://www.canadadhh.com/
2. Digital Health Circle: https://www.digitalhealthcircle.ca/
3. BC Children's Hospital Digital Health Innovation Lab: https://www.bcchr.ca/dhil
4. BC Health Information Management Professionals Society: https://www.bchimps.org/

Alberta

1. Alberta Netcare: https://www.albertanetcare.ca/
2. MyHealth Records: https://myhealth.alberta.ca/mhr-features

Saskatchewan

1. eHealth Saskatchewan: https://www.ehealthsask.ca/Pages/default.aspx
2. Sunrise Clinical Manager (SCM): https://www.saskatoonhealthregion.ca/locations_services/Services/Digital Health/Pages/Home.aspx
3. Lumeca: https://lumeca.com/

Manitoba

1. LibreMD: https://www.libremd.com/
2. MBTelehealth: https://mbtelehealth.ca/
3. Shared Health Manitoba: https://sharedhealthmb.ca/

Ontario

1. eHealth Ontario: https://www.ehealthontario.on.ca/en/
2. Ontario MD: https://www.ontariomd.ca/
3. Ontario Telemedicine Network: https://otn.ca/

Quebec

1. Quebec Health Record: https://www.quebec.ca/en/health/your-health-information/quebec-health-record/
2. Cristal-Net: http://www.dcicristalnet.com/

New Brunswick

1. Accreon Health Cloud: https://accreon.com/interoperability/
2. eVisitNB: https://www.evisitnb.ca/

Nova Scotia

1. myHealthNS: https://www.myhealthns.ca/
2. NS Medical Devices: https://www.nsmedicaldevices.com/

Prince Edward Island

1. Health PEI: https://www.princeedwardisland.ca/en/information/health-pei/electronic-health-records-ehrs

Newfoundland and Labrador

1. The Newfoundland and Labrador Centre for Health Information (NLCHI): https://www.nlchi.nl.ca/

Yukon Territory

1. eHealth Yukon: http://www.hss.gov.yk.ca/ehealth.php
2. Yukon Hospitals (Telehealth): https://yukonhospitals.ca/yukon-hospital-corporation/telehealth

Northwest Territories

1. NWT HealthNet: https://www.hss.gov.nt.ca/en/services/nwt-healthnet
2. NWT Virtual Care: https://www.nthssa.ca/en/services/nwt-virtual-care

Nunavut

1. Nunavut Department of Health: https://www.gov.nu.ca/health/information/telehealth

Appendix B – Additional Standards

Standards, specifications or reports under development by ISO/TC 307:

- (Technical report) ISO/CD TR 3242 – Blockchain and distributed ledger technologies – Use cases [156]
- (Technical Report) ISO/AWI TR 6039 – Blockchain and distributed ledger technologies – Identifiers of subjects and objects for the design of blockchain systems [157]
- (Technical Report) ISO/CD TR 23245.2 – Blockchain and distributed ledger technologies – Security risks, threats and vulnerabilities [158]
- (Technical Report) ISO/WD TR 23249 – Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management [159]
- (Standard) ISO/DIS 23257 – Blockchain and distributed ledger technologies – Reference architecture [160]
- (Technical Specification) ISO/DTS 23258 – Blockchain and distributed ledger technologies – Taxonomy and Ontology [161]
- (Technical Specification) ISO/AWI TS 23259 – Blockchain and distributed ledger technologies – Legally binding smart contracts [162]
- (Standard) ISO – ISO/PRF TR 23576 – Blockchain and distributed ledger technologies – Security management of digital asset custodians [163]
- (Technical Specification) ISO/DTS 23635 – Blockchain and distributed ledger technologies – Guidelines for governance [164]
- (Technical Report) ISO/WD TR 23644 – Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management (TADIM) [165]
- (Technical Report) ISO/AWI TR 23642 – Blockchain and distributed ledger technologies – Overview of smart contract security good practice and issues [166]

Standards, specifications or reports under development (except otherwise noted) by IEEE Blockchain Initiative [147]:

- P2140.1 – Standard for General Requirements for Cryptocurrency Exchanges (Published)
- P2140.2 – Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges
- P2140.3 – Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges
- P2140.4 – Standard for Distributed/Decentralized Exchange Framework using DLT (Distributed Ledger Technology)
- 2140.5-2020 – IEEE Standard for a Custodian Framework of Cryptocurrency (Published)
- P2141.1 – Standard for the Use of Blockchain in Anti-Corruption Applications for Centralized Organizations
- P2141.2 – Standard for Transforming Enterprise Information Systems from Centralized Architecture into Blockchain-based Decentralized Architecture
- P2141.3 – Standard for Transforming Enterprise Information Systems from Distributed Architecture into Blockchain-based Decentralized Architecture

- P2142.1 – Recommended Practice for E-Invoice Business Using Blockchain Technology
- 2143.1-2020 – IEEE Standard for General Process of Cryptocurrency Payment (Published)
- P2143.2 – Standard for Cryptocurrency Payment Performance Metrics
- P2143.3 – Standard for Risk Control Requirements for Cryptocurrency Payment
- P2145 – Standard for Framework and Definitions for Blockchain Governance
- P2146.1 – Standard for Entity-Based Risk Mutual Assistance Model through Blockchain Technology
- P2146.2 – Standard for External Data Retrieval of Blockchain for Risk Mutual Assistance Model
- 2418.2-2020 – IEEE Approved Draft Standard Data Format for Blockchain Systems
- P2418.3 – Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture
- P2418.4 – Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)
- P2418.5 – Standard for Blockchain in Energy
- P2418.7 – Standard for the Use of Blockchain in Supply Chain Finance
- P2418.8 – Standard for Blockchain Applications in Governments
- P2418.9 – Standard for Cryptocurrency Based Security Tokens
- P2418.10 – Standard for Blockchain-based Digital Asset Management
- P2677.1 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Overarching Framework
- P2677.10 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Access to Personal Data
- P2677.11 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Access to Telecommunications Data
- P2677.12 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Access to Transportation Data
- P2677.20 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Requirements for Blockchain Infrastructure
- P2677.21 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Requirements for Peer-to-Peer Storage Infrastructure
- P2677.22 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Requirements for Grid Computing Infrastructure
- P2677.30 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Personal Application Programming Interface
- P2677.31 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Health care Application Programming Interface
- P2677.32 – Standard for Blockchain-based Omnidirectional Pandemic/epidemic Surveillance: Government Application Programming Interface
- P3201 – Standard for Blockchain Access Control
- P3202 – Standard for Capability Evaluation Requirements of Blockchain Practitioners

- P3203 – Standard for Blockchain Interoperability Naming Protocol
- P3204 – Standard for Blockchain Interoperability – Cross Chain Transaction Consistency Protocol
- P3205 – Standard for Blockchain Interoperability – Data Authentication and Communication Protocol
- P3206 – Standard for Blockchain-based Digital Asset Classification
- P3207 – Standard for Blockchain-based Digital Asset Identification
- P3208 – Standard for Blockchain-based Digital Asset Exchange Model
- P3209 – Standard for Blockchain Identity Key Management
- P3210 – Standard for Blockchain-based Digital Identity System Framework
- P3211 – Standard for Blockchain-based Electronic Evidence Interface Specification
- P3212 – Standard for Blockchain System Governance Specification
- P3214 – Standard for Testing Specification of Blockchain Systems
- P3800 – Standard for a data-trading system: overview, terminology and reference model
- P3801 – Standard for Blockchain-based Electronic Contracts
- P3802 – Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting
- P3803 – Standard for Household Appliance Customer Data Assetization and Commercialization Requirements
- P3806 – Standard for Blockchain-based Hepatobiliary Disease Data Extraction and Exchange

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2021 University of Waterloo and Canadian Standards Association.
All Rights Reserved.