frontiers in Blockchain

ORIGINAL RESEARCH
published: 12 February 2021
doi: 10.3389/fbloc.2020.558705

Having Our "Omic" Cake and Eating It Too?: Evaluating User Response to Using Blockchain Technology for Private and Secure Health Data Management and Sharing

Victoria L. Lemieux[1], Darra Hofman[1], Hoda Hamouda[1], Danielle Batista[1], Ravneet Kaur[1], Wen Pan[1], Ian Costanzo[2], Dean Regier[1,3], Samantha Pollard[3], Deirdre Weymann[3] and Rob Fraser[4]*

[1] School of Information, University of British Columbia, Vancouver, BC, Canada, [2] Anon Solutions, Vancouver, BC, Canada, [3] British Columbia Cancer, Vancouver, BC, Canada, [4] Molecular You, Vancouver, BC, Canada

This paper reports on end users' perspectives on the use of a blockchain solution for private and secure individual "omics" health data management and sharing. This solution is one output of a multidisciplinary project investigating the social, data, and technical issues surrounding application of blockchain technology in the context of personalized healthcare research. The project studies potential ethical, legal, social, and cognitive constraints of self-sovereign healthcare data management and sharing, and whether such constraints can be addressed through careful design of a blockchain solution.

Keywords: blockchain technology, usability, self-sovereign identity, privacy, usable security and privacy, distributed ledger technology

OPEN ACCESS

Edited by:
Esteban Eduardo Mocskos, University of Buenos Aires, Argentina

Reviewed by:
Remo Pareschi, University of Molise, Italy
Giuseppe Jurman, Bruno Kessler Foundation (FBK), Italy

****Correspondence:***
Victoria L. Lemieux
v.lemieux@ubc.ca

Specialty section:
This article was submitted to Non-Financial Blockchain, a section of the journal Frontiers in Blockchain

Received: *03 May 2020*
Accepted: *01 December 2020*
Published: *12 February 2021*

Citation:
Lemieux VL, Hofman D, Hamouda H, Batista D, Kaur R, Pan W, Costanzo I, Regier D, Pollard S, Weymann D and Fraser R (2021) Having Our "Omic" Cake and Eating It Too?: Evaluating User Response to Using Blockchain Technology for Private and Secure Health Data Management and Sharing. Front. Blockchain 3:558705. doi: 10.3389/fbloc.2020.558705

INTRODUCTION

There is a news story almost every day about how individuals' personal data are being harvested, shared with, and used by third parties without their consent and in ways that have real potential to cause harm. The result is an erosion of user trust and a reluctance to use services that gather sensitive information (Van Staa et al., 2016; Edelman., 2019). This remains true for a significant percentage of individuals even if they could greatly benefit from receiving a personalized health service that they can use to understand their health risks and maintain or improve their overall health (Shabani et al., 2014; Van Staa et al., 2016; Betts and Korenda, 2018). Individuals' reluctance may stem from uncertainty about how health data services will store and use their data over time (Shabani et al., 2014; Sanderson et al., 2016). Recent revelations about how Facebook, 23&Me, and other platforms use individuals' sensitive personal data validates concerns that consumers' data may be shared with third parties without their informed consent (see, e.g., Geggel, 2018; Rosenberg, 2018).

Some argue that blockchain technology can be used to provide individuals with greater control over their own data [i.e., "self-sovereignty" (Allen, 2016)] as a means to prevent the kind of "databuses" (Wittes, 2011) that have caused individuals to become concerned about their privacy and reduced their trust in sharing health data. On the other hand, blockchain technology is still an emerging technology that, thus far, has proven difficult for all but experts to grasp. Research has shown that blockchain has a usability problem (Krombholz et al., 2016; Eskandari et al., 2018).

Given this reality, it is fair to ask: even if blockchain technology can be designed in a way that gives individuals more sovereignty over their own health information and provides greater privacy protection, will individuals be motivated to adopt the technology and share more of their health information? To shed greater light on the end user's perspective, we developed a technical artifact—the self-sovereign health data management blockchain solution design. We then used the artifact to stimulate a conversation with focus group participants to learn more about how individuals would respond to being given control over their own health data using a blockchain solution to manage and share their data. Our study contributes a greater, though still preliminary, understanding of individuals' attitudes toward self-sovereign blockchain-based health data management and sharing, which can be used by designers of such systems to guide design choices.

BACKGROUND LITERATURE

Advancing Personalized Medicine: Why Both Data Sharing and Data Privacy Matter

Omic science, including genomics, proteomics, exposomics, phenomics, microbiomics, and metabolomics (Horgan and Kenny, 2011), provides insights into health at a molecular level never before possible and has the potential to radically alter healthcare. Omic science establishes a sophisticated, systemic understanding of the "complex, longitudinal, and dynamic nature of biological networks (and their fluctuations in response to social/environment exposures) that fundamentally govern human health and disease" (Holmes et al., 2010, p. 327). Indeed, Bencharit (2012) asserts that "the new era of omics studies... may lead to a true clinical application of personalized medicine."

The undeniable social good that omics could do is not without challenges and risks, however. Privacy for participants in research and in clinical applications is a major concern because "[b]y nature, the genome encodes a sensitive yet heritable signature of an individual that is marked by genetic variation reflecting one's ancestry and disclosing one's susceptibility to health and diseases" (Shi and Wu, 2017, p. 61). Both Canada and the USA have passed genetic non-discrimination acts (e.g., Genetic Non-Discrimination Act, S.C.2017, c.3; Genetic Information Non-Discrimination Act, 29 USC §216(e), 29 USC §1132) in light of the potential medical, professional, legal, and social consequences that individuals might face should their genomic information be disclosed. Other omic information also has the same potential for abuse. Given the very grave potential consequences of unauthorized disclosure of omic data, protecting the privacy of individuals is of paramount importance.

Family privacy is also a concern, since omics science extends not just to the individual, but to their family as well (Shi and Wu, 2017, p. 61). After all, genes are heritable—breaching the genetics of one individual may easily reveal private information about those who share that individual's genes. "Clinical genetics guidelines [in the United Kingdom] conceptualize genetic information as confidential to families, not individuals" (Dheensa et al., 2017, p. 1).

Beyond consideration of the consequences of privacy breaches, however, lies a deeper reason to ensure that individuals' privacy is protected. In a world in which we increasingly live online, we are our data and are data are us (Cheney-Lippold, 2018). The philosopher and information ethicist, Luciano Floridi, who views consequentialist ethical frames of reference that focus on judging actions as moral or not based on their outcomes as insufficient (Floridi, 1999), writes that, "Typically, privacy and confidentiality are treated as problems concerning S' ownership of some information, the information being somehow embarrassing, shameful, ominous, threatening, unpopular or harmful for S' life and well-being, yet this is very misleading, for the nature of the information in question is quite irrelevant. It is when the information is as innocuous as one may wish it to be that the question of privacy acquires its clearest value. The husband, who reads the diary of his wife without her permission and finds in it only memories of their love, has still acted wrongly. The source of the wrongness is not the consequences, nor any general maxim concerning personal privacy, but a lack of care and respect for the individual, who is also her information." (Floridi, 1999, p. 53). Thus, we see in Floridi an approach that views an individuals' data as equivalent to the individual themselves, which suggests that to abuse a person's data is tantamount to an assault of their physical being.

Simply locking data away is a poor solution to the need to protect data privacy. "Sharing genetic findings is vital for accelerating the pace of biomedical discoveries and for fully realizing the promises of the genetic revolution" (Erlich and Narayanan, 2014, p. 409). Thus, if omic research is to be utilized to its full potential, solutions must be found to protect privacy while still permitting data sharing and usage.

Blockchain Technology: A Possible Solution to Private and Secure Data Sharing

Blockchain's design and networked, distributed, autonomous, and global operation establish it as a disruptive technology with social, political, and economic implications that far exceed those of other emerging technologies with many potential applications (Economist, 2015; Casey and Vigna, 2018). One of the key applications identified has been in connection with privacy-preserving and secure management of health data.

Swan (2015) notes that, by managing electronic medical records in the blockchain, they "could be analyzed but remain private, with an embedded economic layer to compensate data contribution and use." She also envisions "a standardized secure mechanism for digitizing health data into a "health data commons" where patients could consent to making their health data available for research use in exchange for cryptocurrency. Benchoufi and Ravaud (2017, p. 335) advocate for blockchain to address "reproducibility, data sharing, personal data privacy concerns and patient enrolment," and emphasize "the transparency of the Blockchain ledger—owned by no one, publicly writable by anyone [...] users do not need any third party to trust the system" (Benchoufi and Ravaud, 2017, p. 338). Gropper (2016) proposes the application of a decentralized

identity management solution within the healthcare sector. In a more recent paper, Evangelatos et al. (2020, p. 238) discuss the wide ranging possibilities and challenges of adopting blockchain for digital health, noting that "data-centric, blockchain-driven solutions that have been proven efficient in other data-driven industries have started finding applications in the domains of health care and biomedical sciences as well."

There is, for example, a growing number of projects involving the application of blockchain to omics data for purposes of conducting biomedical research. Ozercan et al. (2018) survey a number of these, including some focused on privacy-aware data sharing such as the Cancer Gene Trust (CGT) being developed by the Global Alliance for Genomics and Health (GA4GH) Consortium[1]; the CrypDist project[2]; Gene-chain by Encrypgen[3], whose founder has now joined forces with Consensys Health[4]; and the Zenome Project (Kulemin et al., 2017). Chen and Shae (2019) discuss development of a blockchain-based system, the Integrated Biomedical Informatics System (IBIS/BRICS) that uses an Ethereum blockchain network to manage and share medical results among a network of organizations involved in biomedical research.

With the level of trust that it can enforce, blockchain also could be considered a path through the complexities of user consent. Meaningful consent is critical if health data is to be used both ethically and legally with "[C]onsent [being] a cornerstone of both biomedical research ethics and data protection law" (Thorogood and Zawati, 2015, p. 693). A number of studies have aimed to apply blockchain technology to giving individuals direct control over access to their medical records and consenting to secondary use of their health data for research purposes. Ekblaw et al. (2016), Ivan (2016), Broderson et al. (2016), Li et al. (2017), Linn and Koo (2016), and Dagher et al. (2018) discuss blockchain-based medical records systems that incorporate user-defined permissioning while still storing patient records in a provider's existing systems. Yue et al. (2017) propose the *Healthcare Data Gateway* application to allow users to control their own health data and permit its use for research purposes. Zhang et al. (2017) present a decentralized application for patient-defined access to structured pieces of their health data record, and Patel (2018) discusses a blockchain-based framework for medical image sharing that allows for patient-defined access permissions. Finally, Hofman et al. (2018) discuss a blockchain prototype for managing user consent in the use of clinical data for precision health research.

While blockchain could be a solution to some of the challenges of securing and protecting patients' health data (Engelhardt, 2017), giving patients greater control over their data using this technology, it is not without its challenges (Gordon and Catalini, 2018). The cryptography and networking involved in blockchain technology can make it difficult for even IT specialists to understand, let alone users (Ljunggren, 2019). Many patients already have difficulty navigating the healthcare system, which raises questions about whether placing the added burden upon them of managing their own healthcare records, and associated consents to access and use of the data within these records, will truly generate a net positive effect (Gordon and Catalini, 2018). Omic data is particularly challenging in terms of meaningful, informed consent. Indeed, omic data represents an extreme form of "the transparency paradox [. . .] If notice (in the form of a privacy policy) finely details every flow, condition, qualification, and exception, we know that it is unlikely to be understood, let alone read. [. . .] An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance" (Nissenbaum, 2010, p. 36). After all, omic research techniques—and therefore research purposes—advance quickly, making it challenging to explain the purpose, risks, and benefits of studies in an accessible way. Indeed, it is difficult to even predict "all the informational benefits and risks of research with complex genomic information" (Thorogood and Zawati, 2015, p. 694). Moreover, some bioethicists also worry about the possibility of coercion if patients are financially incentivized to share their personal health data (Gammon et al., 2018). A blockchain solution can give users greater control over access to their health records and consent to use of their health information, but will they be able to navigate both the complexity of consent in addition to a novel technology? Searching for answers matters.

METHODOLOGY

We followed a multimethod, two-stage methodology to find out more about individual's attitudes and response to the potential for blockchain technology to be used to protect their privacy and enable secure data sharing.

Stage 1: Designing a Self-Sovereign Health Data Management Solution

In the first stage, we set out to design a technical artifact, in the form of a blockchain solution that fundamentally respects users' right to privacy and provides them with the same level of choice and control over the sharing of their omic data as they would expect over the sharing of their bodies. In the context of this study, omic data included over 300 different biomarkers falling into six different categories for individual users for whom detailed health reviews had been completed: metabolites, environment, and diet biomarkers (i.e., for metals, minerals, nutrients, and toxins), proteins, genetics, pharmacogenetics, and phenotypes (i.e., health and lifestyle history). The structure of the data was uniform and the size of the dataset associated with each biomarker was limited (<1 MG).

We decided that blockchain protocols that came closest to our vision were those that supported self-sovereign identity. While other blockchain solutions have been proposed to provide users with more control over and self-management of their health records, as we have described above, most often these solutions require that individuals be assigned an identity in order to access and use a system. These systems also do not place the control and custody of health records fully into the hands of the individuals themselves. Instead, individuals' health

[1]https://www.cancergenetrust.org/docs/about
[2]https://github.com/CrypDist
[3]https://encrypgen.com/blog/
[4]https://consensys.net/blockchain-use-cases/healthcare-and-the-life-sciences/

records and the associated metadata continue to be owned by and in the custody of healthcare providers even if individuals can more easily access their records and make choices about consent to share their health information (see, for example, designs discussed in Azaria et al., 2016; Gordon and Catalini, 2018; Hofman et al., 2018; Chen and Shae, 2019; Leeming et al., 2019; Shahnaz et al., 2019; El Rifai et al., 2020). As such, we hypothesized that individuals may still be concerned about whether such solutions would fully protect their privacy, since there will be a link back to their identity and health records and metadata remain in the custody of a person or entity other than the individual themselves (e.g., a healthcare institution).

Self-sovereign identity (SSI), a variant of decentralized digital identity, leverages the affordances of blockchain technology to increase users' control of their identities in the digital world (Allen, 2016; Aydar and Ayvaz, 2019; Ferdous et al., 2019). It implies that individuals' identities and the data associated with them are neither bestowed, revocable, nor owned by any authority save for the individual herself. Christopher Allen writes that "[s]elf-sovereign identity is the next step beyond user-centric identity [. . .] the user must be central to the administration of identity [with] true user control of that digital identity, creating user autonomy: (Allen, 2016) Young and Vescent (2018) explain that "Self-sovereign identity is a new technology layer that enables individuals and organizations to assert their own identity." Tobin and Reed (2017) describe Self-sovereign identity as the result of trying to satisfy "three basic requirements: (1) Security—the identity information must be protected from unintentional disclosure; (2) Control—the identity owner must be in control of who can see and access their data and for what purposes; and (3) Portability—the user must be able to use their identity data wherever they want and not be tied into a single provider." Bouma (2019) argues that in the old (centralized and federated) models, the locus of control was between the other parties that could make decisions about an individual, whether that individual was in the picture or not (see **Figure 1**). The basic tenets of SSI can be summarized at a high-level as follows: (1) every individual human being is the original source of their own identity; (2) identity is not an administrative mechanism for others to control; and (3) each individual is the root of their own identity and central to its administration (IBM., 2017). Mühle et al. (2018) provide an overview of the SSI architecture, highlighting its user-centric nature. This approach differs from, though it is not incompatible with, Privacy by Design (Cavoukian, 2011) and Global Alliance for Genetic Health (GA4GH)'s Framework for Responsible Sharing of Genomic and Health-Related Data (GA4GH, 2016) wherein data stewards, research ethics boards, and researchers still make decisions about a data subject's data. However, with self-sovereign identity the locus of data ownership, custody, and control of decision-making shifts to the individual.

Although SSI need not be implemented using a blockchain, blockchain-based SSI systems, wherein the blockchain is used as a trust anchor, are becoming more widespread (Mühle et al., 2018; Aydar and Ayvaz, 2019). For example, uPort, a product of ConsenSys AG, that builds upon the Ethereum blockchain, provides a platform for self-sovereign digital identity management. The uPort app permits users to store digital credentials (containing identifying information) and decide with whom and when they share such information[5]. Alastria ID, which leverages several different blockchain protocols, is another example of an SSI project. The project implements contracts and software components that allow its integration with backends of different services that gives users control over the transactions associated with their identity in order to access services[6]. ShoCard is an SSI system that breaks an individual's identity up into discrete attributes, hashes them, and stores them on a blockchain (cited in Aydar and Ayvaz, 2019). Another example of SSI is offered by the Sovrin Network, which utilizes the Hyperledger Indy/Aries protocol and is described as a public utility that enables SSI on the Internet[7]. The artifact built for this study utilizes this protocol.

Having decided upon an SSI-based solution design, we created a design artifact using prototyping and agile software development. The agile approach draws upon a group-based, collaborative software development methodology that uses iterative, highly context sensitive requirements for identification, design, implementation, and evaluation. Agile development typically involves short, intense sprints wherein cross-functional teams gather in "scrums" to identify requirements, develop code, and evaluate the functionality of a proof-of-concept software application (Agile Alliance, 2013).

Given the focus of the solution design on protecting the users' identity and shifting the locus of control, custody, and decision-making about health data to users of the solution, we also employed user-centered design (UCD) as a general methodological approach to the design and implementation of our prototype. UCD methodology is also widely used when designing health care services (LeRouge and Wickramasinghe, 2013; Xie and Carayon, 2015). UCD ensures the involvement of users and the inclusion of their perspectives in the research, development and assessment phases of a design (Ghulaum Sarwar Shah and Robinson, 2006). The resulting technical artifact is discussed in more detail in **Appendix 1** of this paper.

Stage 2: Focus Group Evaluation of Blockchain Solution Design

To understand end users' perspectives on the use of blockchain technology to manage, control, and share their personal health data, we ran three separate focus groups using our experimental blockchain solution design to seed the discussion. Focus groups are suitable for exploring the attitudes toward new phenomena, such as blockchain, as the relatively open-ended discussions can sensitize researchers to unrealized issues and increase the comprehensiveness of large-scale surveys conducted afterward (Morgan, 2005). In total, 26 individuals participated in our study, with eight in the first focus group, eight in the second group, and 10 in the third group. The focus groups were composed of individuals aged 25–60 years old recruited online.

[5]https://www.uport.me/
[6]https://alastria.io/en/id-alastria/
[7]https://sovrin.org/

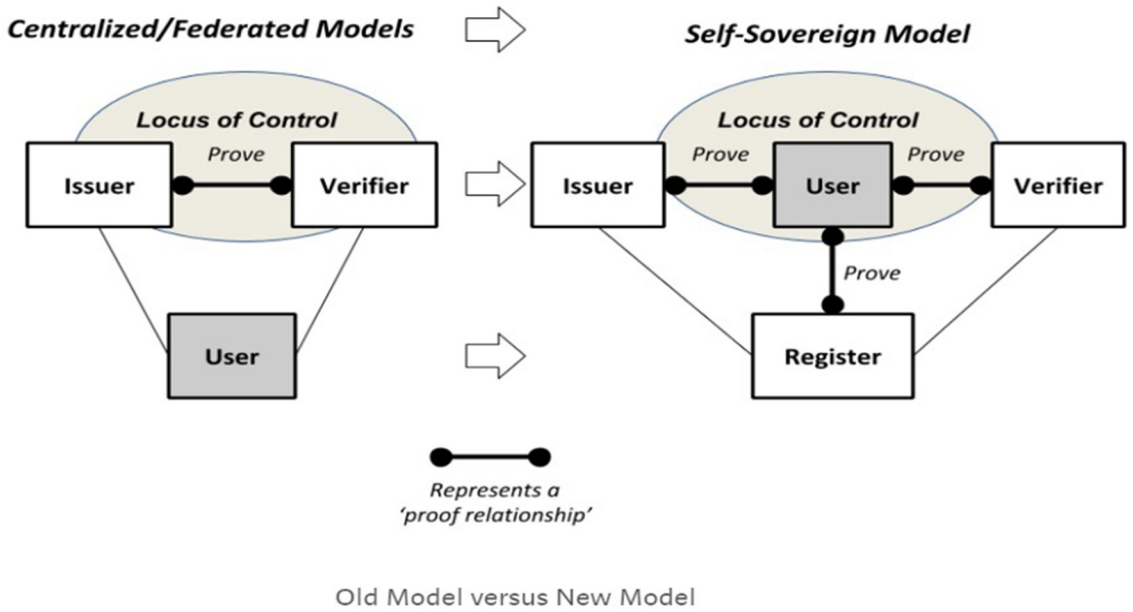

FIGURE 1 | Self-sovereign identity locus of control (Bouma, 2019).

During the focus group, participants were primed with a presentation that contained information about the following topics: consent, management, privacy of personal health data, and blockchain technology.

Then they were shown wireframes of the user interface of the prototype solution and asked a set of semistructured questions relating to their understanding of blockchain technology, their views of data privacy and sharing, and their thoughts on the user interface. The focus groups were audio recorded with participant consent. The audio recordings were transcribed verbatim and then the recordings were destroyed. Transcriptions were pseudonymized and coded for analysis using *NVIVO* 12.0 qualitative analysis software. The research team read the participants' responses and extracted six main codes as shown in **Table 1**.

FINDINGS

Participants' responses flag a number of unresolved challenges to the adoption of blockchains as solutions for private and secure data sharing in healthcare, as well as specific areas for improvement of the blockchain solution design. The following section provides a high-level summary of participants' feedback.

Focus group participants were generally aware of the challenges of data sharing across healthcare providers. For example, they noted that hospitals could not easily share with one another and that moving across jurisdictions often meant losing access to their health records. They also were aware of cases when very sensitive health information had been inadvertently exposed.

Individuals saw value in using a blockchain-based solution as a means to support privacy-preserving data sharing. However, some individuals expressed reluctance to use such a platform until it has been thoroughly tested and more widely adopted. Areas of ongoing concern included who they would be sharing with and for what purpose, supporting findings from previous studies indicating that transparency is needed to win individuals' trust in sharing their health information (New et al., 2018). Generally, participants expressed willingness to consent to having university researchers use their data or to share data with government agencies in the event of a public health crisis but were reluctant to share with pharmaceutical companies or insurers for fear of being discriminated against. This highlights the importance of designing upfront information about the type of organization requesting access and a clear explanation of their reason for wanting to use individuals' health data. Individuals also wanted assurances that researchers or other users of their data would not be able to reuse data for another purpose without their consent or assemble data about them from disparate sources to create a health profile about them [a "mosaic effect" (Wittes, 2011)]. Participants were not universally hesitant to engage with a more experimental platform; as one focus group participant put it: "... someone has to start, right? There would be falls and all that and there would be corrections, I'm willing to be on the beta."

One cognitive constraint leading to possible lack of trust was in connection with the way that the cryptographic proofs operated. Focus group participants expressed a lack of understanding and need for more transparency about the manner in which cryptography-protected privacy and validated claims, with one participant referring to the proofs as a "black box." This suggests a need for informational tools and techniques,

TABLE 1 | Analytic codes extracted from focus group participant statements.

Code	Description
Compensation and rewards	Types of rewards related to data sharing and the impacts of having them.
Ethics	Ethical issues and concerns in relation to health data sharing, use, and control.
Health data	Discussions about health data.
Access	Questions and answers related to centralized and decentralized access, equity, and difficulties.
Control	Discussion about the relevance of personal data control, data expiration, and ownership.
Sharing	Health data sharing with or without consent, who to share with, and benefits and risks of sharing (not including ethical issues and concerns).
Privacy	Discussion about privacy issues, ownership, and anonymization.
Systems design	The usability and design of the platform; suggestions for improvement.
Trustworthiness, security, and comfort	Discussion about the trustworthiness, security, and level of comfort with using decentralized system.

such as decision aids that could support participants' choices to engage with the platform (Joseph-Williams et al., 2014) or algorithmic transparency. Unlike in artificial intelligence (AI) solutions where solution designers have often resisted requests to reveal their algorithms in order to protect their interests (Diskopolous, 2016), there is a longstanding practice of algorithmic transparency in cryptography. Kerchoff's principle, one of the guiding axioms of cybersecurity solution design, specifies that a cryptosystem should be secure even if everything about the system, except the private key, is public knowledge (Stewart et al., 2008). Thus, cybersecurity solution designers have much stronger incentives for revealing their cryptographic algorithms than do AI researchers, suggesting that this cognitive barrier can be overcome.

Focus group participants generally liked the idea of having greater control and custody of their personal data, though one participant did express concern: "My first impression was 'crap, now I have to keep track of it all'." Another participant said they would share the power of control and consent with immediate family members in case anything happened to them. Universally, participants did not want to bear the risk, typical of current blockchain solutions, of losing access to their data if they lost their private cryptographic key. They were all willing to give up some self-sovereignty for the ability to have a way to regain access.

In terms of usability of a decentralized cryptosystem, individuals expressed a number of concerns. In particular, some participants identified the risk of exclusion of non-tech savvy and older users. However, another participant in an older age demographic noted: "... actually today older people have more access to smartphones then they have had in the last 5 or 10 years." Another noted, "I think it will come to a stage that it will be much easier to use for older people." Participants also expressed concern about the understandability of consent terms and conditions, pointing to the fact that these statements can be very complex and difficult to interpret, which is consistent with the findings of previous studies. They requested that terms and conditions be presented in understandable language upfront in the handshake process, not at step 5 as in the technical prototype they were shown.

In relation to the offering of a reward, most individuals felt comfortable with this idea but did express some concern about potential effects in relation to the scale and granularity of data being shared and the use to which the data would be put. For example, one study participant wondered: "would that become a barrier for researchers who didn't have that kind of [money], that a company has to compensate people, and how would that affect the landscape of information sharing?" Another said, "I would also worry that the outcomes would then be skewed because if you're putting forth opportunities for compensation, then especially if you're talking $50 or less, who are you attracting? Are you really attracting a broad enough range of people that have data that's applicable to whatever the study is, so I don't like that idea." As a result, participants generally expressed a preference for smaller rewards functioning more as honoraria rather than market-based compensation. Others wanted to know more about the form a reward would take. For example, if provided in the form of a gift card, participants wondered if, they could be traced back to the research study. As a result, some participants expressed a preference for the reward in the form of cryptocurrency, like bitcoin, or even food. Overall, users noted that they have higher levels of trust in the process knowing that a research ethics board has reviewed the study design, including the issue of compensation, even if that meant the platform was not fully decentralized.

Although our study examines individuals' attitudes to the use of blockchain solutions in the context of health records self-management and sharing, we suggest that our findings could be generalizable to many similar blockchain-based SSI solutions, such as those described in Aydar and Ayvaz (2019) (i.e., those that rely on Decentralized Identifiers (DIDs) and Verifiable Credentials). For instance, individuals expressed a strong preference to know who they are sharing their data with and for what purpose, which suggests that SSI solutions would benefit from always providing such information to individuals as part of requests for data sharing from other individuals or entities. Our findings also reveal that individuals do not have a clear understanding of how SSI solutions operate, including how they might differ from other blockchain solutions for self-management of records (i.e., those that assign identities as part of access control, where the individuals' records remain under the control of a third party, or where their information may be stored on a blockchain). This lack of understanding may

affect individual choices concerning the adoption of SSI vs. other types of blockchain solutions for data self-management. Finally, our study supports the finding that concern about private key management is as much a barrier to adoption for blockchain-based SSI solutions as it is for other blockchain solutions. Our study suggests that users would rather relinquish some sovereignty than have to deal with the complexity of private key management. This finding also indicates that users of blockchain solutions might still favor convenience over privacy and security, as has been found to be the case with other novel technologies (see, e.g., Lau et al., 2018).

Our study is revealing of individuals' attitudes to adoption of blockchain, specifically SSI blockchain solutions, for self-management and sharing of health records; however, our work is preliminary and has a number of limitations. The number of individuals participating in our focus groups was relatively small and was not representative of any population. Our focus groups also did not include people actively working in healthcare records management. It would be interesting to include such professionals in our future work to uncover any differences in perceptions with those held by the individuals whose records they manage. In addition, health data is quite heterogeneous in structure, size, and perceived sensitivity, ranging from geolocation tracings in areas of epidemic risk to huge genomic sequencing files. Would users still want the responsibility of self-managing their health records if they had to take responsibility for large files or to protect the security of highly sensitive disease information? Our study only looked at specific data types and thus we are unable to say whether individuals might react differently to self-management of health records using blockchain when different types of data are involved. This remains as future work.

CONCLUSION

No single solution can solve the challenges of protecting participant's privacy—of respecting their autonomy and dignity—in complex, revealing areas such as omic science. However, blockchain technology could solve a number of the technical and social limitations of our current systems for onboarding participants and collecting, storing, and disseminating data. As Dove et al. (2012, p. 439) remind us, "open innovation models, such as open access, open source, expert sourcing, and patent pools" are one of the primary means of "overcoming the 'transfer problem' in omics research that continues to hinder the full realization of concrete applications for human health" (Dove et al., 2012, p. 439). One of the major hindrances to the full embrace of open innovation in omic science is the very real danger to patient privacy should their data be subjected to unauthorized access or disclosure. Blockchain technology could let us have our omic cake and eat it too, by permitting the data to be studied while remaining private. Nevertheless, the above evaluation flags a number of ongoing areas of concern and future research challenges.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

ETHICS STATEMENT

The studies involving human participants were reviewed and approved by University of British Columbia Behavioral Research Ethics Board. The patients/participants provided their written informed consent to participate in this study.

AUTHOR CONTRIBUTIONS

VL led the research project. VL, HH, RK, WP, and IC contributed to the conceptualization and prototyping of the blockchain solution design. VL, DH, HH, DB, SP, DR, and RF contributed to the conceptualization of the ethical, legal, social and cognitive issues in use of blockchain technology. VL, DH, HH, and SP contributed to the writing of the paper. All authors reviewed, contributed to editing, and approved the content of this paper.

FUNDING

The research presented in this article was partially funded by Mitacs (Grant Numbers IT12057 and IT16076).

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2020.558705/full#supplementary-material

REFERENCES

Agile Alliance (2013). What Is Agile Software Development? Retrieved from: http://www.agilealliance.org/agile101/

Allen, C. (2016). The Path to Self-Sovereign Identity. Life with Alacrity (blog). Retrieved from: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed April 25, 2016).

Aydar, M., and Ayvaz, S. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. *arXiv [Preprint] arXiv:*1906.09791.

Azaria, A., Ekblaw, T., Vieira, and Lippman, A. (2016). "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on IEEE* (Washington, DC: IEEE Computer Society Conference Publishing Service (CPS)), 25–30. doi: 10.1109/OBD.2016.11

Bencharit, S. (2012). Progresses and challenges of omics studies and their impacts in personalized medicine. *J. Pharmacogenomics Pharmacoproteomics* 3:10001e105. doi: 10.4172/2153-0645.1000e105

Benchoufi, M., and Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials* 18:335. doi: 10.1186/s13063-017-2035-z

Betts, D., and Korenda, L. (2018). Inside the patient journey: Three key touch points for consumer engagement strategies. Retrieved from: https://www2.deloitte.com/insights/us/en/industry/health-care/patient-engagement-health-care-consumer-survey.html (accessed September 25, 2018).

Bouma, T. (2019). Self-Sovereign Identity: Shifting the Locus of Control. Retrieved from: https://medium.com/@trbouma/self-sovereign-identity-shifting-the-locus-of-control-10da1c8757ad (accessed March 2, 2019).

Broderson, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., and Truscott, A. (2016). Blockchain: Securing a New Health Interoperability Experience. Retrieved from: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_block-~chain_challenge_response_august8_final.pdf

Casey, M. J., and Vigna, P. (2018). *The Truth Machine: The Blockchain and the Future of Everything*. New York, NY: St. Marten's Press.

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Retrieved from: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Chen, Y. W., and Shae, Z. Y. (2019). "Blockchain for pre-clinical and clinical platform with big data," in: *Application of Omics, AI and Blockchain in Bioinformatics Research (Advanced Series in Electrical and Computer Engineering Book 21)*, eds J. P. Tsai and K. L. Ng (Hackensack, NJ: World Scientific Publishing Pte Ltd.), 29–46. doi: 10.1142/9789811203589_0003

Cheney-Lippold, J. (2018). *We are Data: Algorithms and the Making of our Digital Selves*. New York, NY: NYU Press. doi: 10.2307/j.ctt1gk0941

Dagher, G. G., Mohler, J., Milojkovic, M., and Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology Dagher, *G.* G., Mohler, J., Milojkovic, M. and Marella, P. B. *Sustainable Cities Soc.* 39, 283–297. doi: 10.1016/j.scs.2018.02.014

Dheensa, S., Fenwick, A., and Lucassen, A. (2017). Approaching confidentiality at a familial level in genomic medicine: A focus group study with healthcare professionals. *BMJ Open* 7:e012443. doi: 10.1136/bmjopen-2016-012443

Diskopolous, N. (2016). Accountability in algorithmic decision making. *Commun. ACM* 59, 56–62. doi: 10.1145/2844110

Dove, E. S., Ozdemir, V., and Joly, Y. (2012). Harnessing omics sciences, population databases, and open innovation models for theranostics-guided drug discovery and development: Omics sciences, databases, and open innovation. *Drug Dev. Res.* 73, 439–436. doi: 10.1002/ddr.21035

Economist (2015). Blockchains: The great chain of being sure about things. Retrieved from: https://tinyurl.com/y76dovsm (accessed October 31, 2015).

Edelman. (2019). *Edelman Trust Barometer. Annual global survey*. Retrieved from: https://www.edelman.com/trust-barometer/

Ekblaw, A., Azaria, A., Vieira, T., and Lippman, A. (2016). *MedRec: Medical Data Management on the Blockchain*. Retrieved from: http://dci.mit.edu/assets/papers/eckblaw.pdf

El Rifai, O., Biotteau, M., de Boissezon, X., Megdiche, I., Ravat, F., and Teste, O. (2020). "Blockchain-based personal health records for patients' empowerment," in *International Conference on Research Challenges in Information Science* (Cham: Springer), 455-471. doi: 10.1007/978-3-030-50316-1_27

Engelhardt, M. A. (2017). Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. *Technol. Innovation Management Rev.* 7, 22–34. doi: 10.22215/timreview/1111

Erlich, Y., and Narayanan, A. (2014). Routes for breaching and protecting genetic privacy. *Nat. Rev. Genet*. 15, 409–421. doi: 10.1038/nrg3723

Eskandari, S., Clark, J., Barrera, D., and Stobert, E. (2018). A first look at the usability of bitcoin key management. *arXiv preprint arXiv*:1802.04351. doi: 10.14722/usec.2015.23015

Evangelatos, N., Upadya, S. P., Venne, J., Satyamoorthy, K., Brand, H., Ramashesha, C. S., et al. (2020). Digital transformation and governance innovation for public biobanks and free/libre open source software using a blockchain technology. *Omics* 24, 278–285. doi: 10.1089/omi.2019.0178

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7, 103059–103079. doi: 10.1109/ACCESS.2019.2931173

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. *Ethics Inform. Technol.* 1, 33–52. doi: 10.1023/A:1010018611096

GA4GH (2016). Data Sharing Lexicon. Global Alliance for Genomics & Health. Retrieved from: https://www.ga4gh.org/wp-content/uploads/GA4GH_Data_Sharing_Lexicon_Mar15.pdf (accessed March 15, 2016).

Gammon, K. (2018). Experimenting with blockchain: can one technology boost both data integrity and patients' pocketbooks? *Nat. Med.* 24, 378–381. doi: 10.1038/nm0418-378

Geggel, L. (2018). 23 and Me is Sharing Genetic Data with Drug Giant. Retrieved from: https://www.scientificamerican.com/article/23andme-is-sharing-genetic-data-with-drug-giant/ (accessed July 28, 2018).

Ghulaum Sarwar Shah, S., and Robinson, I. (2006). User involvement in healthcare technology development and assessment: Structured literature review. *Int. J. Health Care Quality Assurance* 19, 500–515. doi: 10.1108/09526860610687619

Gordon, W. J., and Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput. Struct. Biotechnol. J.* 16, 224–230. doi: 10.1016/j.csbj.2018.06.003

Gropper, A. (2016). "Powering the Physician-Patient Relationship With HIE of One Blockchain Health IT," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. (Gaithersburg, MD: ONC/NIST).

Hofman, D., Lam, K., Shannon, C., Assadian, S., McManus, B., Ng, R., et al. (2018). "Building trust & protecting privacy: analyzing evidentiary quality in a blockchain proof-of-concept for health research data consent management," in *Proceedings of the IEEE Blockchain Conference* (Washington, DC: IEEE Computer Society). doi: 10.1109/Cybermatics_2018.2018.00275

Holmes, C., McDonald, F., Jones, M., Ozdemir, V., and Graham, J. E. (2010). Standardization and omics science: technical and social dimensions are inseparable and demand symmetrical study. *Omics* 14, 327–332. doi: 10.1089/omi.2010.0022

Horgan, R. P., and Kenny, L. C. (2011). 'Omic' technologies: Genomics, transcriptomics, proteomics and metabolomics. *Obstet. Gynaecol.* 13, 189–195. doi: 10.1576/toag.13.3.189.27672

IBM. (2017). *Self-Sovereign Identity: Unraveling the Terminology*. Retrieved from: https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-unraveling-the-terminology/

Ivan, D. (2016). "Moving toward a blockchain-based method for the secure storage of patient records," in *Presented at the ONC/NIST Use of Blockchain for Healthcare and Research Workshop* (Gaithersburg, MA). Available online at: https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf

Joseph-Williams, N., Newcombe, R., Politi, M., Durand, M. A., Sivell, S., Stacey, D., et al. (2014). Toward minimum standards for certifying patient decision aids: a modified Delphi consensus process. *Med. Decis. Making* 34, 699–710. doi: 10.1177/0272989X13501721

Krombholz, K., Judmayer, A., Gusenbauer, M., and Weippl, E. (2016). "The other side of the coin: User experiences with bitcoin security and privacy," in *International Conference on Financial Cryptography and Data Security*. (Berlin: Springer), 555-580. doi: 10.1007/978-3-662-54970-4_33

Kulemin, N., Popov, S., and Gorbachev, A. (2017). The Zenome Project: blockchain-based genomic ecosystem. Available online at: https://zenome.io/download/whitepaper.pdf

Lau, J., Zimmerman, B., and Schaub, F. (2018). Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum. Comput. Interaction* 2, 1–31. doi: 10.1145/3274371

Leeming, G., Cunningham, J., and Ainsworth, J. (2019). A ledger of me: personalizing healthcare using blockchain technology. *Front. Med.* 6:171. doi: 10.3389/fmed.2019.00171

LeRouge, C., and Wickramasinghe, N. (2013). A review of user-centered design for diabetes-related consumer health informatics technologies. *J. Diabetes Sci. Technol.* 7, 1039–1056. doi: 10.1177/193229681300700429

Li, X., Jiaing, R., Chen, T., Luo, X., and Wen, Q. (2017). A survey on the security of blockchain systems. *Archivx.Org*. arXiv:1802.06993.

Linn, L. A., and Koo, M. B. (2016). "Blockchain for health data and its potential use in health it and health care related research," in *Presented at the ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, (Gaithersburg, MA). Available online at: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/11-74-ablockchainforhealthcare.pdf

Ljunggren, N. (2019). *Improving the Usability of Secure Information Storing Within Blockchain Applications*. Retrieved from: https://lup.lub.lu.se/student-papers/search/publication/8972293

Morgan, D. L. (2005). *Focus Groups: Encyclopedia of Social Measurement*. Kimberly K, ed. New York, NY: Elsevier, 51–57. doi: 10.1016/B0-12-369398-5/00039-6

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* 30, 80–86. doi: 10.1016/j.cosrev.2018.10.002

New, J. P., Leather, D., Bakerly, N. D., McCrae, J., and Gibson, J. M. (2018). Putting patients in control of data from electronic health records. *BMJ* 360:j5554. doi: 10.1136/bmj.j5554

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books. doi: 10.1515/9780804772891

Ozercan, H. I., Ileri, A. M., Ayday, E., and Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. *Genome Res.* 28, 1255–1263. doi: 10.1101/gr.207464.116

Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* 25, 1398–1411. doi: 10.1177/1460458218769699

Rosenberg, M. (2018). How Trump Consultants Exploited the Facebook Data of Thousands. New York Times. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (accessed March 17, 2018).

Sanderson, S. C., Linderman, M. D., Suckiel, S., Diaz, G. A., Zinberg, R. E., Ferryman, K., et al. (2016). Motivations, concerns and preferences of personal genome sequencing research participants: Baseline findings from the HealthSeq project. *Eur. J. Hum. Genetics* 24, 14–20. doi: 10.1038/ejhg.2015.118

Shabani, M., Bezuidenhout, L., and Borry, P. (2014). Attitudes of research participants and the general public towards genomic data sharing: a systematic literature review. *Expert Rev. Mol. Diagnostics* 14, 1053–1065. doi: 10.1586/14737159.2014.961917

Shahnaz, A., Qamar, U., and Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access* 7, 147782–147795. doi: 10.1109/ACCESS.2019.2946373

Shi, X., and Wu, X. (2017). An overview of human genetic privacy. *Annals New York Acad. Sci.* 1387, 61–72. doi: 10.1111/nyas.13211

Stewart, J. M., Tittel, E., and Chapple, M. (2008). *CISSP: Certified Information Systems Security Professional Study Guide*. New York, NY: John Wiley & Sons, Inc.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. New York, NY: O'Reilly Media, Inc.

Thorogood, A., and Zawati, M. H. (2015). International guidelines for privacy in genomic biobanking (or the unexpected virtue of pluralism). *J. Law Med. Ethics* 43, 690–702. doi: 10.1111/jlme.12312

Tobin, A., and Reed, D. (2017). *The Inevitable Rise of Self-Sovereign Identity*. Seattle, WA: Sovrin Foundation.

Van Staa, T. P., Goldacre, B., Buchan, I., and Smeeth, L. (2016). Big health data: the need to earn public trust. *British Med. J.* 354:i3636. doi: 10.1136/bmj.i3636

Wittes, B. (2011). *Databuse: Digital Privacy and the Mosaic*. Retrieved from: https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/

Xie, A., and Carayon, P. (2015). A systematic review of human factors and ergonomics (HFE)-based healthcare system redesign for quality of care and patient safety. *Ergonomics*, *58*(1), 33–49. doi: 10.1080/00140139.2014.959070

Young, K., and Vescent, H. (2018). 10 things you need to know about Self Sovereign Identity, part 1. He Paypers Insight into Payments. Retrieved from: https://www.thepaypers.com/expert-opinion/10-things-you-need-to-know-about-self-sovereign-identity-part-1/774556 (accessed August 28, 2018).

Yue, L., Junqin, H., Shengzhi, Q., and Ruijin, W. (2017). "Big data model of security sharing based on Blockchain," in *2017 3rd International Conference on Big Data Computing and Communications* (BIGCOM) (Washington, DC: IEEE), 117–121 doi: 10.1109/BIGCOM.2017.31

Zhang, P., White, J., Schmidt, D. C., and Lenz, G. (2017). *Applying Software Patterns to Address Interoperability in Blockchain-Based Healthcare Apps*. Retrieved from: https://arxiv.org/pdf/1706.03700.pdf

Conflict of Interest: VL, RF, and RK declare a connection with Molecular You, a company that is developing the blockchain solution discussed in this paper for commercial purposes. IC was employed by Anon Solutions, a sub-contractor of Molecular You.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.