Viewpoint

Test, Trace, and Put on the Blockchain?: A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Contact Tracing to Combat a Global Pandemic

Moritz Platt[1], BSc, MSc; Anton Hasselgren[2], BSc, MSc; Juan Manuel Román-Belmonte[3], MD, PhD; Marcela Tuler de Oliveira[4], BSc, MSc; Hortensia De la Corte-Rodríguez[5], MD, PhD; Sílvia Delgado Olabarriaga[4], MSc, PhD; E Carlos Rodríguez-Merchán[6,7], MD, PhD; Tim Ken Mackey[8,9], MAS, PhD

[1]Department of Informatics, King's College London, London, United Kingdom

[2]Department of Neuromedicine and Movement Science, Faculty of Medicine and Health Sciences, Norwegian University of Science and Technology, Trondheim, Norway

[3]Department of Physical Medicine and Rehabilitation, Hospital Central de la Cruz Roja San José y Santa Adela, Madrid, Spain

[4]Department of Epidemiology and Data Science, Amsterdam UMC, Amsterdam, Netherlands

[5]Department of Physical Medicine and Rehabilitation, La Paz University Hospital, Madrid, Spain

[6]Department of Orthopaedic Surgery, La Paz University Hospital, Madrid, Spain

[7]Osteoarticular Surgery Research, Hospital La Paz Institute for Health Research, IdiPAZ, Madrid, Spain

[8]Department of Anesthesiology, Division of Infectious Diseases and Global Public Health, School of Medicine, UC San Diego, La Jolla, CA, United States

[9]BlockLAB, San Diego Supercomputer Center, UC San Diego, La Jolla, CA, United States

Corresponding Author:
Tim Ken Mackey, MAS, PhD
Department of Anesthesiology, Division of Infectious Diseases and Global Public Health
School of Medicine
UC San Diego
8950 Villa La Jolla Drive
A124
La Jolla, CA, 92037
United States
Phone: 1 951 491 4161
Email: tmackey@ucsd.edu

Abstract

The enormous pressure of the increasing case numbers experienced during the COVID-19 pandemic has given rise to a variety of novel digital systems designed to provide solutions to unprecedented challenges in public health. The field of algorithmic contact tracing, in particular, an area of research that had previously received limited attention, has moved into the spotlight as a crucial factor in containing the pandemic. The use of digital tools to enable more robust and expedited contact tracing and notification, while maintaining privacy and trust in the data generated, is viewed as key to identifying chains of transmission and close contacts, and, consequently, to enabling effective case investigations. Scaling these tools has never been more critical, as global case numbers have exceeded 100 million, as many asymptomatic patients remain undetected, and as COVID-19 variants begin to emerge around the world. In this context, there is increasing attention on blockchain technology as a part of systems for enhanced digital algorithmic contact tracing and reporting. By analyzing the literature that has emerged from this trend, the common characteristics of the designs proposed become apparent. An archetypal system architecture can be derived, taking these characteristics into consideration. However, assessing the utility of this architecture using a recognized evaluation framework shows that the added benefits and features of blockchain technology do not provide significant advantages over conventional centralized systems for algorithmic contact tracing and reporting. From our study, it, therefore, seems that blockchain technology may provide a more significant benefit in other areas of public health beyond contact tracing.

(JMIR Public Health Surveill 2021;7(4):e26460) doi: 10.2196/26460

XSL•FO
RenderX

KEYWORDS

COVID-19; public health; blockchain; distributed ledger technology; mobile apps; pandemic mitigation; contact tracing; epidemiological monitoring

Introduction

Background

To many global health professionals, the emergence of the COVID-19 pandemic has not come as a complete surprise. The outbreak of SARS that occurred in the autumn of 2002 in Guangdong Province, China—characterized as the first near-pandemic in the era of globalization [1]—marked the beginning of a new century in which global health security events would become more frequent and escalate rapidly across the globe. Following SARS came the global pandemic of H1N1, outbreaks of Middle East Respiratory Syndrome, the Zika virus, and new Ebola outbreaks. These served as early warning signs of what would become the most significant human health emergency since the 1918 influenza pandemic: the current COVID-19 global pandemic that has, as of February 2021, resulted in at least 100 million cases and 2 million deaths worldwide [2].

Throughout this period of accelerated outbreaks of novel, emerging, and re-emerging infectious diseases, calls for sound public health policy and further expansion of public health surveillance capacity to prevent future pandemics have become more frequent and urgent [3]. However, investment in public health infrastructure, such as strengthening state capabilities under the World Health Organization International Health Regulations, did not heed these warnings: experts have painted a bleak picture of outbreak preparedness by characterizing the global pandemic response as cycles of panic succeeded by neglect [4]. Consequently, various systems for disease surveillance, including electronic public health reporting modalities, were challenged by the complex requirements associated with COVID-19-related data. Some of these challenges stemmed from the inability of the relevant public health agencies to receive and share electronic data at a pandemic scale [5], some from the use of inappropriate or outdated tools lacking interoperability [6], and some from failing to meet security and privacy requirements [7].

As COVID-19 cases continue to surge, national governments have attempted to invest in and deploy more robust digital disease surveillance systems. These encompass different forms of technology (eg, digital epidemiology, big data, machine learning, mobile apps, and distributed computing), which are now viewed as critical tools to explore in order to modernize the pandemic response [8]. While a rapid increase in innovation and investment in this area of technology has occurred, many of these technology-centric initiatives have encountered implementation barriers due to nontechnical challenges associated with data governance, user adoption, concerns about accountability and oversight, and patient privacy and social acceptance concerns [7,8]. An emerging technology that has been suggested in this context is blockchain, a form of distributed ledger technology that is maturing in several industries, including in areas of digital cryptocurrencies, financial transaction technology, and growing attention in industrial sectors, such as energy, transportation, supply chain, auditing, and health care [9].

Blockchain Uses in Health Care

The adoption of blockchain, which can be characterized as an append-only distributed database that is coordinated via a peer-to-peer protocol [10], removes the need for central operators and can offer potential improvements over traditional health care information management systems (eg, client-server systems) [9]. Blockchain allows for tamper-proof replication of data in an adversarial environment [11]. The technology is resilient to fault scenarios in which adversaries send conflicting information to different parts of the system [12], even if those adversaries present large numbers of pseudonymous identities with malicious intent [13]. Participants on a blockchain form consensus on whether a proposed record is admissible by adjudicating it using a consensus mechanism [14], thus ensuring only valid records agreed upon by network members are replicated.

Consensus on a blockchain network can be proof based (eg, proof-of-work consensus as used by the Bitcoin blockchain) or voting based (eg, proof-of-authority consensus) [15], with different hybrid forms being an emerging field of research [16]. Regarding access control, blockchain protocol taxonomies differentiate between public or private and permissionless or permissioned networks [17]. Public blockchains are open to participation by anyone, whereas private, or *enterprise*, blockchains employ access control mechanisms. In a permissionless system, all members have the same responsibilities in the consensus protocol, while permissioned networks assign different responsibilities in consensus to participants, depending on their role and authority.

Several use cases have emerged evidencing the potential utility of blockchain in health care data management. These include electronic health record (EHR) management and aggregation, privacy-preserving algorithms for health systems data, integration of blockchain systems with the Internet of Medical Things, enabling distributed patient-provider directories across multiple payers and providers, and enhancing management and security of health supply chains [18-21]. Accompanying this potential, blockchain also faces real-world implementation challenges, including storing and transferring data on- and off-chain, interoperability with other health information systems, managing permission structures, and ensuring scalability [22].

Blockchain has also been suggested as a potential solution in the context of COVID-19 algorithmic contact tracing by promising protection from cyberattacks [23], allowing for global monitoring of social encounters to inform health policies [24], enabling privacy [25,26], preventing the falsification of diagnoses [27], allowing users to retain ownership of personal data [28], and ensuring the trustworthiness of that data [29], while maintaining a record of its provenance [26]. While none of the popular algorithmic contact tracing frameworks on the

XSL•FO
RenderX

market today [30] uses blockchain, the growing number of academic works [23,25,27,31-38] suggests significant interest. Hence, this viewpoint aims to critically examine the potential utility and technical feasibility of blockchain technology for pandemic algorithmic contact tracing. This is accomplished by applying a blockchain evaluation framework that assesses the suitability of using the technology for specific use cases based on seven key questions. The viewpoint concludes with some recommendations of whether blockchain is a viable application for this critical public health use case and other observations about how to leverage this technology in the ongoing fight against COVID-19.

Algorithmic Contact Tracing

Overview of Conventional and Algorithmic Contact Tracing Approaches

Contact tracing is an epidemiological control measure aimed at identifying all the people with whom an individual who contracted an infectious disease has been in contact, and who are, in turn, at risk of being infected with and transmitting that disease to other close contacts [39]. It has pronounced benefits in controlling infections that remain undetected in the population [40], such as the transmission of COVID-19, in which a large proportion of cases could be asymptomatic [41]. Quick, reliable, and accurate tests to confirm cases are a prerequisite for successful contact tracing [42,43], as, without them, infectious individuals can remain unidentified and continue to serve as human vectors sustaining community transmission. Insufficient testing can lead to underreporting of the true prevalence of the disease and its attack rate, as well as limit the effectiveness of nonpharmaceutical interventions, such as masking, social distancing, and other crucial public health interventions [44]. Contact tracing, however, represents only one single stage in the process of effective outbreak control and response, which is only effective when combined with quarantine and isolation procedures [45].

Contact tracing has a rich history dating back to the late nineteenth century, when UK medical officers responded to infectious disease outbreaks such as smallpox with surveillance systems involving notification, isolation, disinfection, and case finding [46]. The information age brought digital case management systems and other innovations (eg, digital epidemiology via mobile apps, internet surveillance, and disease modeling and forecasting using artificial intelligence) that are now being leveraged by health authorities. Yet, traditional interview-based approaches remain a mainstay [8,47,48]. Here, contact information is collected by health care professionals or volunteers who discover the contact history of individuals affected by an infectious disease through interviews with patients, families, or health care professionals or by analyzing medical records, tracking data, or surveillance data [49].

Where an interview-based contact tracing technique is used, its success relies on the ability of those affected to recollect their contact history. The reliability of such self-reported data is, however, questionable [50]. Moreover, contact with unknown persons cannot be discovered through this approach. Furthermore, conventional contact tracing regimens are labor intensive, are associated with high costs per case, and yield diminishing disease prevalence reductions under incremental investments [51]. Consequently, doubts have been raised about whether these traditional methods alone can be effective in the context of a large-scale pandemic. As a reaction, digital epidemiology methods, including algorithmic contact tracing, have been proposed to reduce virus transmission more effectively [8]. Digital epidemiology, or “the use of data generated outside the public health system for disease surveillance” [8], has been discussed since the 1990s [52]. Most of the early approaches to digital epidemiology use *passive* methods by repurposing data from “a range of sources most of which do not relate to healthcare utilization” [supplementary material, 8]. In contrast, most modalities of algorithmic contact tracing can be considered *active* methods, as users have to enable data monitoring and sharing consciously.

Algorithmic contact tracing automates the conventional contact tracing process by allowing for the collection, aggregation, and analysis of automatically generated data about a case’s contacts by a public health agency, thus eliminating the need for laborious interviews. The large volume and multimodal nature of the clinical informatics systems and epidemiological data that go along with this approach constitute a challenge that new technologies can help address [53]. This applies particularly to algorithms that can quickly assess potential exposure and risk patterns while enabling faster notification to suspected contacts [54]. Countries that have applied algorithmic contact tracing aggressively, by making the use of mobile phone tracing apps compulsory (eg, China and South Korea), were able to reduce daily positive cases more effectively than those that used approaches where participation was voluntary [55]. While it is unclear whether the containment of case numbers can be directly attributed to algorithmic contact tracing, the use of big data to trace individuals is a commonality of the pandemic containment strategies applied by these countries [56]. Further, real-world experiences with the deployment of algorithmic contact tracing illustrate the complexity of the ethical issues associated with these technologies, including the need to balance individual privacy and autonomy concerns with the utility of such data to prevent disease spread during a public health emergency [8,56].

To reiterate, the goal of contact tracing is to identify people that *had contact* with each other, thereby identifying a potential path of exposure and infection. While a definition of what can be considered *contact* in the context of COVID-19 is still evolving [57], active algorithmic contact tracing commonly uses physical proximity and duration of exposure [58] as an approximation. Data gathered for algorithmic contact tracing commonly takes one of three forms: (1) proactively reported data (ie, manual digital check-ins that require participants’ compliance [59]), (2) active sensor data (ie, information about an encounter with a different device utilizing the same tracing app), and (3) passive sensor data (ie, information about the geographic position of the device). These are commonly generated by devices using Bluetooth, including Bluetooth Low Energy; GPS; and Wi-Fi signal strength information [60]. Bluetooth allows for active sensing, delivering information about the proximity of two sensors with submeter accuracy [61,62]. Passive sensing through GPS and Wi-Fi uses

XSL•FO
RenderX

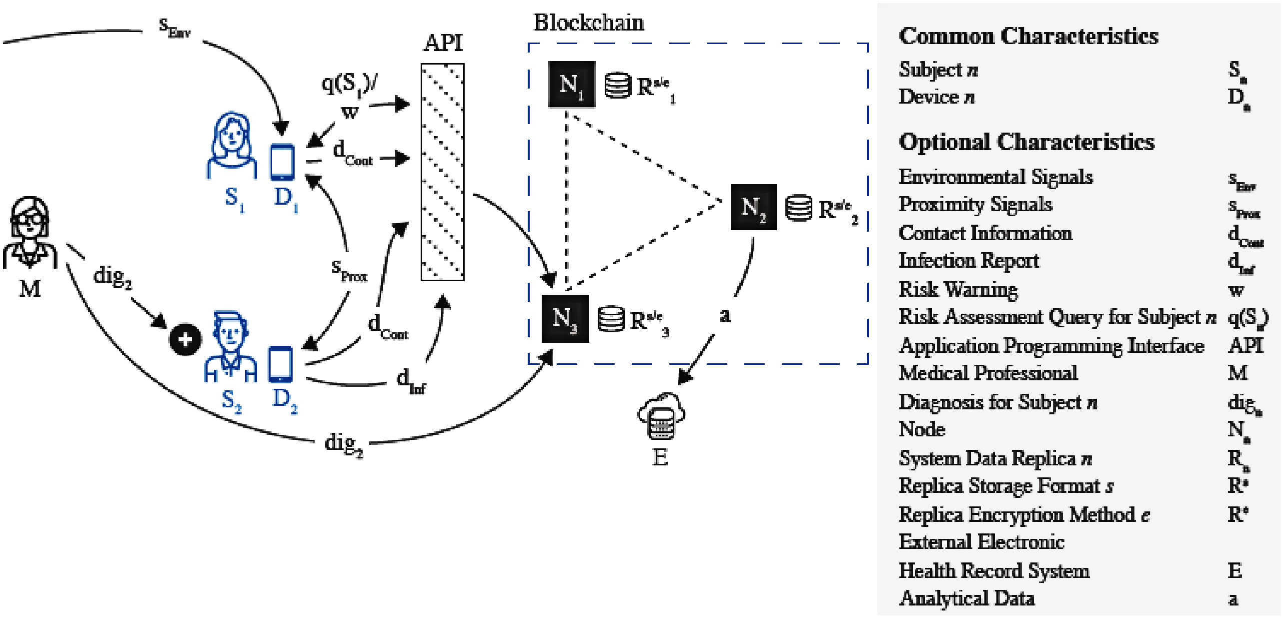
environmental data to approximate the geographic position of a device with relatively high precision under good conditions [63,64], but insufficient precision under suboptimal conditions [65-67]. Based on this information, an algorithmic contact tracing system can reconstruct when individual devices have been close, thereby allowing it to proactively alert those who are identified as being at risk of infection once confirmation of a positive case is made known to the system.

Existing Literature on Blockchain Technology for Algorithmic Contact Tracing

As previously discussed, algorithmic contact tracing is now an emerging use case for blockchain technology. However, little had been published on this topic and its application to infectious disease control before the COVID-19 pandemic, despite prior outbreaks of other diseases. One of the first contributions in this space is by Kangbai et al [68], who proposed a "Blockchain platform to conduct real-time Ebola contact tracing" in the context of the 2018 outbreak of this highly virulent virus in the Democratic Republic of Congo. Subsequently, the COVID-19 pandemic has led to increased interest in the topic and several publications and preprints in the medical and engineering literature. From a systemic perspective, the dominant function of blockchains in algorithmic contact tracing is that of tamper-proof, distributed data stores for managing contact data [23,25,27,31-38]. A less pronounced function is that of a data integration layer that allows for the exchange of medical and public health information from different sources among different actors in health care settings [23,25,27,32]. Data that are exchanged in this way take the shape of certified COVID-19 diagnostic data [23,25,32] or immunization data [27].

Proposed algorithmic contact tracing blockchain systems appear as distributed architectures consisting of varying numbers of nodes in a network (see Figure 1). Commonly, these systems do not employ access control but, instead, grant read and write access to the public [23,25,31,33-36,38]. Less commonly, read access is provided to the public but write access is restricted [37], yet other architectures operate as private systems [27,32]. In most public systems, each node stores a replica of all data network-wide. Here, data are potentially encrypted and stored according to a format specific to the protocol used. In some architectures, external entities like hospitals or laboratories access the blockchain to obtain data for analysis [37], potentially correlating them with data held by external EHR systems. The consensus mechanisms used for data replication between nodes are rarely discussed. Where they are, mechanisms are selected either for their performance characteristics [25] or to implement authority-based forms of consensus [23,35,37]. While some proposals do not discuss the role of smart contracts [31,37,38], many employ smart contracts to validate data on the chain [23,32,34-36], mostly to prevent malicious users from inserting fabricated records of positive diagnoses into the system [23,32].

Figure 1. An archetype of a blockchain-based contact tracing environment derived from architectures described in the published literature. EHR: electronic health record.



Common Characteristics	
Subject *n*	S_n
Device *n*	D_n
Optional Characteristics	
Environmental Signals	s_{Env}
Proximity Signals	s_{Prox}
Contact Information	d_{Cont}
Infection Report	d_{Inf}
Risk Warning	w
Risk Assessment Query for Subject *n*	$q(S_n)$
Application Programming Interface	API
Medical Professional	M
Diagnosis for Subject *n*	dig_n
Node	N_n
System Data Replica *n*	R_n
Replica Storage Format *s*	R^s
Replica Encryption Method *e*	R^e
External Electronic Health Record System	E
Analytical Data	a

Proposed blockchain-based algorithmic contact tracing systems (see Figure 1) also generally cater to two types of actors: subjects that use contact tracing apps and, except for cases in which only self-reported data are used [34,36], medical professionals that digitally attest to positive cases [23,25,32]. Through their mobile devices, subjects obtain environmental signals from passive sensors [33], proximity signals from active sensors [23,31,32,34,36-38], or a combination of both [25,27,35,36]. The data received are converted into a target format to be stored on the blockchain, the particulars of which are a key differentiator between protocols. While some protocols disregard information privacy [33], more commonly, the confidential nature of tracing data is recognized and addressed by proposing formats that are deemed to prevent a subject's privacy from being compromised.

The goals of privacy-focused blockchain architectures are as follows: preventing manipulation of diagnostic data [23], preventing impersonation of health authorities [31], protecting the identity of infected persons [25,36], or, most commonly,

XSL•FO
RenderX

precluding mass surveillance through the derivation of movement or contact profiles from stored data [25,31,32,34,35,37,38]. To approach these goals, various models to capture data relevant to contact tracing are proposed. Contact data commonly come in the form of contact lists using one-time pseudonyms [23], pseudonymized user data combined with encrypted location information [25], pseudonymized or encrypted diagnoses [31,32], or encrypted epidemiological data [37].

Irrespective of the format, after being generated on the user's device, contact data are sent to the blockchain. This can happen via submission of a transaction to a public network [23,25,31,33-36,38] or, specifically in the case of private systems where subjects do not have direct access to the blockchain [27,32,37], by passing through an upstream application programming interface that can be operated by government bodies [27,37] or by a consortium of otherwise trustworthy entities [32]. The data are then replicated between nodes. In the case of a positive diagnosis for a subject, there are two alternative patterns. First, subjects can reveal their positive status on the chain proactively, oftentimes by providing some form of proof [23,32]. Second, a pseudonymized diagnosis can be uploaded to the chain [31,33] or endorsed on-chain by an authorized diagnostician [25]. Subjects can then query the blockchain at intervals to obtain a risk assessment based on their previous contacts [32,38] or to receive notifications [23,36,37]. The overall purpose of these proposed systems is to enable decentralized networks that can share trusted data relevant to contact tracing efforts, including self-reported data and environmental signals. Nevertheless, parameters around data storage, computation, and measures to ensure privacy-preserving processing vary and can be further modulated by developers should these be implemented.

Evaluation of Applicability of Blockchain to Algorithmic Contact Tracing

Overview

Based on our review of proposed blockchain system designs for algorithmic contact tracing, we now conduct an in-depth assessment of the potential suitability and technological feasibility for their application to COVID-19 based on a technical evaluation framework. We used the Lo et al [69] framework, which assesses the suitability of applying blockchain for the requirements of general use cases by posing a set of seven questions and associated decision gates to answer the question of whether blockchain or conventional databases are more suitable for a particular technology use case. These questions include the following:

1. Are multiple parties required?
2. Is a trusted authority required?
3. Are operations centralized?
4. Is data transparency or confidentiality required?
5. Is the integrity of transaction history required?
6. Is data immutability required?
7. Is high performance required?

Below, we assess core blockchain features, such as decentralization, information privacy, immutability, data integration, transaction verification, and network performance, aligned with the suitability assessment and applied to the use case of algorithmic contact tracing (see Table 1).

Table 1. Suitability evaluation of the applicability of blockchain technology to algorithmic contact tracing, with comparison to conventional database applications (CDAs).

Consideration for blockchain use cases	Evaluation	Indicated system architecture
Are multiple parties required?[a]	Yes	Blockchain is preferred, but CDA is also applicable
Is a trusted authority required?[a]	Yes	Either blockchain or CDA
Is the operation centralized?[a]	Inconclusive	Possibly CDA, as it inherently supports centralized operations
Is transparency required?[a]	No	CDA
Is transaction history required?[a]	No	CDA
Is immutability required?[a]	No	CDA
Is high performance required?[a]	Inconclusive	Possibly CDA, as it can generally achieve higher throughput
Is integration with other systems required?	Yes	Either blockchain or CDA
Is decentralized data validation required?	No	CDA
Is high data reliability required?	Yes	CDA, as it can generally provide higher reliability of data without need for on-chain and off-chain approaches needed for blockchain

[a] This consideration is based on the framework proposed by Lo et al [69].

XSL•FO
RenderX

Multi-Party Decentralization

The first question Lo et al [69] raise in their framework is whether a use case requires multiple parties to be involved and, if so, whether a trusted authority is required and whether that trusted authority is decentralizable. In this context, assessing whether there is a need to operate a multi-party decentralized authority on a public or private blockchain is the first topic that needs to be addressed. Public blockchains were conceived as a design paradigm that is effective in an adversarial environment in which no central trusted party exists, and where potential malicious writers operate on the same hierarchical level as honest ones [11]. In this sense, public blockchains constitute fully decentralized networks that do not require a single trusted authority to validate transactions. Private blockchains introduce some variation to this paradigm by limiting who can access a network and, in the case of private permissioned blockchains, by limiting who can participate in the consensus protocol on the network. Hence, private blockchains, and iterations of consortium blockchains—where a single entity or group controls access to the blockchain—inherently exhibit a lower degree of decentralization. Still, either paradigm can only exploit its respective strengths where there is distrust between those who write the data and where trusted third parties are absent [70].

The environment in which algorithmic contact tracing is conducted, however, is very different. Even though it is a multi-party environment, it requires a trusted authority (Question 2) to be involved in the validation of critical public health data, particularly in the context of addressing a pandemic. Decentralizing the role of the trusted authority may not bring with it any added benefit. For example, a multi-party public blockchain network, where patients have the same rights and responsibilities—including access to and validation of data—as medical practitioners and health authorities, is not optimal for case detection and investigation, as other potential nodes participating in the blockchain may inherently be less trustworthy. Specifically, contact tracing is generally carried out in an environment with clear hierarchies, expertise, and legal mandates that national authorities lead [56]. Authorities also supervise the reporting of case numbers to other local, national, and international organizations and develop necessary calculations based on the epidemiology of the disease to assess the risk of transmission associated with the date and duration of contact with an infected individual. The hierarchical nature of this public health use case becomes particularly evident when considering the possibility of intervention by law enforcement against individuals who do not comply with public health measures [71]. Health authorities are, therefore, in control of virtually all of the factors contributing to the technical success of an algorithmic contact tracing regimen, fundamentally making it a centralized problem requiring a trusted authority and centralized operation (Question 3), which may make it more suitable for conventional information management systems. Those systems commonly consist of infrastructure built around relational database management systems and application settings [72] that employ access control mechanisms as mandated by legislation and regulations [73].

Information Privacy

Algorithmic contact tracing, while having the potential to be an effective tool for controlling disease transmission [74], has also been characterized, fairly or unfairly, as a potent mass surveillance tool, leading to the fear of the normalization of state-run electronic surveillance [32,75-78]. This can be explained by the nature of the data needed for algorithmic contact tracing, which, as discussed earlier, can manifest as location or contact data. Clarke and Wigan [79] discuss why location data are particularly vulnerable by identifying specific dangers that arise from their collection. Among other factors, they discuss psychological harm through embarrassment, the danger of profiling and suspicion generation through the discovery of behavior patterns, as well as social, cultural, scientific, and economic harm arising from the knowledge or suspicion of being watched [79]. While an in-depth debate of these issues is beyond the scope of this viewpoint, we discuss the influence of blockchain on information privacy by comparison to conventional, centrally managed contact tracing systems. This topic aligns with the blockchain suitability framework's question that is focused on the tension between weighing the benefits of enhanced transparency against the needs of such systems to maintain confidentiality (Question 4) and the impact of these decisions on data governance and network performance.

When operated on a public network, blockchain poses significant challenges for engaging with privacy-sensitive data, including protected health information. While proposed blockchain-based systems for contact tracing commonly address the privacy of tracing data through cryptographic protocols [25,31,32,34,35,37,38], their effectiveness in an adversarial environment has to be approached with concern for three reasons:

1. Cryptanalysis can bring to light deficiencies in cryptographic protocols previously believed to be secure, potentially revealing data that were believed to be protected from attackers [80].
2. Even protocols that apply data hygiene diligently by "minimizing or eliminating personally identifiable data of...subjects" [81] and appear unproblematic with regard to privacy might be vulnerable to abuse by methods not yet known, potentially through correlation with data from other sources not yet considered [82].
3. The cryptographic integrity of today's blockchain protocols is threatened by methods of quantum computing [83].

It is, therefore, inadvisable to make any data related to contact tracing, even if considered harmless or undecryptable by today's methods, available beyond completely trustworthy parties that have a legitimate *need to know*, irrespective of whether data are stored in a conventional or decentralized system.

When operated as a private network, blockchain systems generally have a weak negative effect on information privacy: while more finely grained controls of data access in blockchain are possible through permission structures [84], typically, all nodes in a private blockchain network have visibility of network-wide data. Storing only a hash or a similarly obfuscated datum on-chain and keeping sensitive health-related or

XSL•FO
RenderX

individually identifiable data off-chain, including approaches that use off-chain blockchain storage and computation, can improve confidentiality. However, this requires the application of appropriate hash algorithms and randomization techniques [85]. Moreover, obfuscation can diminish the utility of said data and can inhibit network performance, including when data are encrypted [9,69]. Though privacy-preserving approaches to managing health care data leveraging different combinations of off-chain and on-chain storage are possible, their application requires careful design and mapping to appropriate legal and privacy frameworks specific to particular health care use cases and types of data [9]. Given the highly sensitive nature of contact tracing data, confidentiality considerations appear to outweigh the benefits of blockchain-mediated distributed trust and transparency.

Data Integrity and Immutability

An original principle and key value proposition of blockchain systems is their ability to provide data integrity and immutability through creating provenance by linking of transaction blocks [11], which means that data appended to the blockchain cannot be deleted or changed trivially and can, therefore, be considered final in most circumstances [86]. While alternative designs providing mutability have been proposed [87], the applications discussed here consider blockchain as a near-immutable technology and emphasize this quality. This aligns with key decision points in the assessment of suitability for use cases (Questions 5 and 6). Immutability has practical disadvantages in an algorithmic contact tracing context since data cannot be expunged after the incubation period. This means that contact records that no longer serve the purpose of enabling contact tracing may still be present in such systems, potentially threatening the privacy of those that reported them or negatively impacting blockchain system performance (Question 7).

Further, proposed applications commonly embrace the *tamper-proof* nature of contact tracing data on the blockchain. This is largely due to the abstract threat of an attacker tampering with tracing data or the risk of having a trusted authority as a single point of failure. However, in the context of digital contact tracing, data integrity and immutability are of less concern than accuracy and correctness, which are decisive factors for predicting chains of transmission. By their nature, data on confirmed cases should come from trusted centralized sources (eg, health authorities). Therefore, the need to establish data provenance by ensuring the integrity of the transaction history through establishing consensus system-wide is rendered of low importance. Unlike other health care use cases, such as enabling enhanced track and trace of pharmaceuticals in the global supply chain, contact tracing data are not a physical asset that requires tracking changes to its access, ownership, and transfer [88].

As discussed, common blockchain protocols aim to achieve immutability of data recorded [89] and, should the need for correcting existing records arise, address it by appending updated records to the blockchain. This stands in contrast to centralized data storage systems in which records can simply be deleted or corrected. Consequently, data hygiene is hard to achieve in blockchain-based algorithmic contact tracing systems, as those might retain tracing data for longer than medically necessary, simply because the technical capabilities to delete them are not given. Incorrect or inconsistent testing results, or duplicates occurring during integration and consolidation of contact tracing data from different jurisdictions and agencies, are equally harder to correct in an immutable setting [69].

Performance

Performance (Question 7) is recognized as one of the major challenges for real-world implementation of blockchain systems [90]. This can be attributed to challenges associated with their scalability [91], particularly in the context of modulating between on-chain and off-chain storage and computation [9]. Although scale has been achieved in some blockchain applications in the financial sector by applying partitioning [92] or second-level protocols like *side chains* [93], performance may be negatively impacted by the need to achieve consensus among network members during record creation. Achieving consensus is a complex problem to which different blockchain protocols offer different solutions with varying performance characteristics [94]. In the context of algorithmic contact tracing, throughput (ie, the number of transactions that can be executed per unit of time) can be considered the most relevant approximation of overall performance. What all consensus protocols have in common is that coordination among nodes or members is required, which imposes penalties on throughput in exchange for distributed networks of shared trust. Penalties are particularly severe on major public permissionless blockchains, where data validation and replication are subject to *proof-of-work* or *chain-based proof-of-stake* consensus protocols that are characterized by allowing a throughput of only tens of transactions per second [95].

For example, while permissioned blockchains can provide significant performance benefits over their permissionless counterparts [96], achieving around 1000 transactions per second in some common configurations [97], they are still inferior to traditional replicated databases, particularly when multi-leader strategies with low consistency levels are applied, as these can support throughputs above 15,000 operations per second even under challenging workloads [98]. Therefore, traditional database systems can more effectively address the use case of contact tracing in which data validation, where necessary, can be performed centrally by the appropriate authority. Throughput is critical in the context of algorithmic contact tracing infrastructures, especially where vast populations generate large volumes of contact data rapidly and where privacy requirements will inevitably require off-chain storage and computation. Despite the lack of a standardized workload that would be necessary to conclusively answer this question, it can be speculated that private blockchains may have the capability of handling contact tracing data volumes, at least on a regional scale. Nevertheless, the fact that they do not provide a throughput benefit over traditional database systems minimizes their suitability from a performance perspective.

Other Evaluation Considerations

In addition to the evaluation based on the framework proposed by Lo et al [69], further aspects are relevant for assessing blockchain's suitability for enhancing algorithmic contact

XSL•FO
RenderX

tracing. These aspects include data integration, transaction verification, and data reliability as discussed in this section.

The further processing of data gathered via algorithmic contact tracing is largely a problem of data integration (ie, one of combining tracing data with data from different sources, for example, diagnostic data from COVID-19 testing centers and clinical data from EHRs). Here, blockchain can provide benefits by defining a standardized format for transaction data payloads and standard processing logic via smart contracts. Efforts to address data integration are underway, as exemplified by emerging standards at the intersection of blockchain and pandemic and epidemic surveillance [99]. There are, however, challenges concerning the integration with existing health record management systems, such as the cost of change incurred [100], ensuring regulatory compliance of an integrated information technology environment [101], dealing with privacy and confidentiality policies specific to health information (eg, implications of the Health Insurance Portability and Accountability Act in the United States [102] and the General Data Protection Regulation in the European Union [103]), or the immaturity of proposed standards that is detrimental to achieving interoperability [104].

Smart contracts [14,105] constitute agreements that are executed without the involvement of the concerned parties as part of a blockchain protocol. They are a key component of many distributed applications and can be implemented in various programming languages following different paradigms that come with various security features [106]. The common element is that they allow application developers to encode the logic that governs what constitutes a legitimate transaction on the blockchain. Such logic can validate endorsement policies and rules concerning data integrity, thereby ensuring the added content's correctness. Rules around data audit and system access that in centralized systems are commonly enforced by role-based access control mechanisms [107] could also be executed through smart contracts [108]. Conceivably, in the case of a contact tracing app, smart contracts could be developed by a trusted vendor and audited by a credible authority. Further confidence in its correct execution could be gained through formal verification [109]. Still, even in a flawless implementation, smart contracts can only be exploited partially here. While they provide value as a means of ensuring that confirmed case data originate from trusted sources and have not been tampered with, most contact tracing data are user generated and based on signals from outside of the system (eg, pseudonyms of devices in close proximity or geographic locations). For such data, a smart contract differentiating between a legitimate data set and an illegitimate one can, at best, be heuristic. This diminishes the usefulness of the transaction verification capabilities provided by blockchain technology.

Data reliability can be considered essential in contact tracing, where a loss of recent contact data could lead to participants at risk of infection going unnotified. Nodes on a public blockchain network can leave and join at will without risking data loss. Commonly, data are fully replicated between existing nodes and those who join the network. This technique allows for high degrees of redundancy, especially on public blockchains where the number of replicating nodes can be very large (eg, up to 23,000 in the case of Bitcoin [110]). Private blockchain deployments can run in arbitrary topologies, which makes the degree of redundancy they provide contingent on the configuration chosen by the designer of the system. Redundancy positively influences availability, as clients can select an alternative replica to interact with, in case of failure. This is, however, not a unique benefit of blockchain. High reliability can also be achieved via more traditional centralized data replication protocols used in the context of cloud computing, where data redundancy levels are often configurable [111].

Conclusions

Blockchain, although not in productive use in this context, has increasingly been discussed as a technology to support algorithmic contact tracing efforts targeting COVID-19. A question resulting from this trend is whether this technology can replace or enhance the centralized architectures that are operational today. To address this question, we examined blockchain-based contact tracing concepts discussed in the literature. Upon realizing similarities in their design, we derived an archetypal system architecture capturing their common characteristics. Subsequently, guided by an evaluation framework, we explored the potential benefits of this system architecture over conventional approaches to data storage. The results of this suitability evaluation indicate that blockchain-based protocols as currently presented do not provide benefits significant enough to warrant the prioritization of their implementation. This is primarily due to the incongruity between the centralization of organizational and administrative processes surrounding contact tracing and the decentralized nature of blockchain technology. Further technical arguments in support of this result are concerns about the impact of blockchain on the privacy of personal data, unclear benefits of blockchain's key features (ie, enhancing transparency, data provenance, and immutability), the challenges around integrating blockchain systems with existing sources of the health dataverse in legally compliant ways, and a lack of performance benefits over conventional information management systems. The result of the suitability analysis is reinforced by the fact that conventional, centralized, algorithmic contact tracing systems are already integral parts of the pandemic mitigation strategies of some of the countries that are most successful in controlling the spread of COVID-19. Instead of focusing on algorithmic contact tracing, future efforts to leverage blockchain technology in the fight against COVID-19 could turn to the assessment of other promising use cases for suitability. Health supply chain management, digital immunization passports, and the management of digital identity in the context of COVID-19 patient journeys are areas where blockchain might be more appropriate, not least because investments in technology infrastructure and stakeholder buy-in are more mature here.

XSL•FO
RenderX

Acknowledgments

We thank Peter McBurney for sharing his views on information privacy that inspired us to strengthen the conclusions of this paper. We thank Gennaro Avitabile, Paulo Valente Klaine, Leonie Reichert, and Hao Xu for their helpful comments. This work was partly funded by the Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare (ASCLEPIOS) project (grant 826093) via the European Union's Horizon 2020 research and innovation program.

Authors' Contributions

MP wrote the initial draft of the manuscript. AH, TM, JRB, MTO, and HCR contributed additional content, edits, and references. SDO and ERM contributed edits and references. All authors approved the final draft.

Conflicts of Interest

TM is an employee of S-3 Research LLC, which is a start-up company funded and currently supported by the National Institutes of Health, National Institute on Drug Abuse, through a Small Business Innovation and Research contract for opioid-related social media research and technology commercialization. The author reports no other conflict of interest associated with this manuscript and has not been asked by any organization to be named on or to submit this manuscript. The other authors have no conflicts to declare.

References

1. Morens DM, Fauci AS. Emerging pandemic diseases: How we got to COVID-19. Cell 2020 Sep 03;182(5):1077-1092 [FREE Full text] [doi: 10.1016/j.cell.2020.08.021] [Medline: 32846157]
2. COVID-19 situation update worldwide. European Centre for Disease Prevention and Control. 2021. URL: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases [accessed 2021-02-04]
3. Cherry JD, Krogstad P. SARS: The first pandemic of the 21st century. Pediatr Res 2004 Jul;56(1):1-5 [FREE Full text] [doi: 10.1203/01.PDR.0000129184.87042.FC] [Medline: 15152053]
4. Yamey G, Schäferhoff M, Aars OK, Bloom B, Carroll D, Chawla M, et al. Financing of international collective action for epidemic and pandemic preparedness. Lancet Glob Health 2017 Aug;5(8):e742-e744 [FREE Full text] [doi: 10.1016/S2214-109X(17)30203-6] [Medline: 28528866]
5. Holmgren AJ, Apathy NC, Adler-Milstein J. Barriers to hospital electronic public health reporting and implications for the COVID-19 pandemic. J Am Med Inform Assoc 2020 Aug 01;27(8):1306-1309 [FREE Full text] [doi: 10.1093/jamia/ocaa112] [Medline: 32442266]
6. Downey A. 'Excel-gate' highlights need for 'quality technical capability' in NHS. Digital Health. 2020 Oct 09. URL: https://www.digitalhealth.net/2020/10/excel-gate-highlights-need-for-quality-technical-capability-in-nhs [accessed 2021-03-29]
7. Arriagada Bruneau G, Gilthorpe M, Müller VC. The ethical imperatives of the COVID-19 pandemic: A review from data ethics. Veritas 2020 Aug;46:13-35 [FREE Full text] [doi: 10.4067/s0718-92732020000200013]
8. Mello MM, Wang CJ. Ethics and governance for digital disease surveillance. Science 2020 May 29;368(6494):951-954 [FREE Full text] [doi: 10.1126/science.abb9045] [Medline: 32393527]
9. Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf Process Manag 2021 May;58(3):102535. [doi: 10.1016/j.ipm.2021.102535]
10. Tai S, Eberhardt J, Klems M. Not ACID, not BASE, but SALT: A transaction processing perspective on blockchains. In: Proceedings of the 7th International Conference on Cloud Computing and Services Science.: ACM; 2017 Presented at: 7th International Conference on Cloud Computing and Services Science; April 24-26, 2017; Porto, Portugal p. 755-764. [doi: 10.5220/0006408207550764]
11. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin. 2008. URL: https://bitcoin.org/bitcoin.pdf [accessed 2021-03-29]
12. Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Trans Program Lang Syst 1982 Jul;4(3):382-401. [doi: 10.1145/357172.357176]
13. Douceur JR. The Sybil attack. In: Proceedings of the 1st International Workshop on Peer-to-Peer Systems.: Springer; 2002 Presented at: 1st International Workshop on Peer-to-Peer Systems; March 7-8, 2002; Cambridge, MA p. 251-260.
14. Szabo N. Formalizing and securing relationships on public networks. First Monday 1997 Sep;2(9):1 [FREE Full text] [doi: 10.5210/fm.v2i9.548]
15. Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. J Inf Process Syst 2018;14(1):101-128. [doi: 10.3745/jips.01.0024]
16. Platt M, McBurney P. Self-governing public decentralised systems: Work in progress. In: Proceedings of the 10th International Workshop on Socio-Technical Aspects in Security. 2020 Presented at: 10th International Workshop on Socio-Technical Aspects in Security; September 17, 2020; Guildford, UK URL: https://kclpure.kcl.ac.uk/portal/files/136350337/2020_self_governing_public_decentralised_systems.pdf
17. Oliveira M, Carrara G, Fernandes N, Albuquerque C, Carrano R, Medeiros D, et al. Towards a performance evaluation of private blockchain frameworks using a realistic workload. In: Proceedings of the 22nd Conference on Innovation in Clouds,

XSL•FO
RenderX

Internet and Networks and Workshops (ICIN).: IEEE; 2019 Presented at: 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN); February 19-21, 2019; Paris, France p. 180-187. [doi: 10.1109/icin.2019.8685888]

18. Dimitrov DV. Blockchain applications for healthcare data management. Healthc Inform Res 2019 Jan;25(1):51-56 [FREE Full text] [doi: 10.4258/hir.2019.25.1.51] [Medline: 30788182]
19. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB. A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. J Med Syst 2019 Sep 14;43(10):320. [doi: 10.1007/s10916-019-1445-8] [Medline: 31522262]
20. Mackey TK, Kuo T, Gummadi B, Clauson KA, Church G, Grishin D, et al. 'Fit-for-purpose?' - Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med 2019 Mar 27;17(1):68 [FREE Full text] [doi: 10.1186/s12916-019-1296-7] [Medline: 30914045]
21. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. Int J Med Inform 2020 Feb;134:104040 [FREE Full text] [doi: 10.1016/j.ijmedinf.2019.104040] [Medline: 31865055]
22. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing blockchains for efficient health care: Systematic review. J Med Internet Res 2019 Feb 12;21(2):e12439 [FREE Full text] [doi: 10.2196/12439] [Medline: 30747714]
23. Arifeen M, Al Mamun M, Kaiser MS, Mahmud M. Blockchain-enable contact tracing for preserving user privacy during COVID-19 outbreak. Preprints. Preprint posted online on July 22, 2020 [FREE Full text] [doi: 10.20944/preprints202007.0502.v1]
24. Micali S. Algorand's approach to COVID-19 reporting. Algorand. 2020. URL: https://www.algorand.com/algorand's%20approach%20to%20COVID-19%20Tracing%20042520.pdf [accessed 2021-03-29]
25. Xu H, Zhang L, Onireti O, Fang Y, Buchanan WJ, Imran MA. BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond. IEEE Internet Things J 2021 Mar;8(5):3915-3929 [FREE Full text] [doi: 10.1109/jiot.2020.3025953]
26. Idrees SM, Nowostawski M, Jameel R. Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions. JMIR Med Inform 2021 Mar 09;9(2):e25245 [FREE Full text] [doi: 10.2196/25245] [Medline: 33400677]
27. Bansal A, Garg C, Padappayil RP. Optimizing the implementation of COVID-19 "immunity certificates" using blockchain. J Med Syst 2020 Jul 19;44(9):140 [FREE Full text] [doi: 10.1007/s10916-020-01616-4] [Medline: 32683501]
28. Kalla A, Hewa T, Mishra RA, Ylianttila M, Liyanage M. The role of blockchain to fight against COVID-19. IEEE Eng Manag Rev 2020 Sep 1;48(3):85-96 [FREE Full text] [doi: 10.1109/emr.2020.3014052]
29. Marbouh D, Abbasi T, Maasmi F, Omar IA, Debe MS, Salah K, et al. Blockchain for COVID-19: Review, opportunities, and a trusted tracking system. Arab J Sci Eng 2020 Oct 12:1-17 [FREE Full text] [doi: 10.1007/s13369-020-04950-4] [Medline: 33072472]
30. Martin T, Karopoulos G, Hernández-Ramos JL, Kambourakis G, Nai Fovino I. Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps. Wirel Commun Mob Comput 2020 Oct 17;2020:1-29. [doi: 10.1155/2020/8851429]
31. Klaine PV, Zhang L, Zhou B, Sun Y, Xu H, Imran M. Privacy-preserving contact tracing and public risk assessment using blockchain for COVID-19 pandemic. IEEE Internet Things Mag 2020 Sep;3(3):58-63 [FREE Full text] [doi: 10.1109/iotm.0001.2000078]
32. Avitabile G, Botta V, Iovino V, Visconti I. Towards defeating mass surveillance and SARS-CoV-2: The Pronto-C2 fully decentralized automatic contact tracing system. Cryptology ePrint Archive. Preprint posted online on April 27, 2020 [FREE Full text]
33. Hossain MS, Muhammad G, Guizani N. Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19 like pandemics. IEEE Netw 2020 Jul;34(4):126-132 [FREE Full text] [doi: 10.1109/mnet.011.2000458]
34. Garg L, Chukwu E, Nasser N, Chakraborty C, Garg G. Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model. IEEE Access 2020;8:159402-159414 [FREE Full text] [doi: 10.1109/access.2020.3020513]
35. Lv W, Wu S, Jiang C, Cui Y, Qiu X, Zhang Y. Decentralized blockchain for privacy-preserving large-scale contact tracing. ArXiv. Preprint posted online on July 2, 2020 [FREE Full text]
36. Song J, Gu T, Feng X, Ge Y, Mohapatra P. Blockchain meets COVID-19: A framework for contact information sharing and risk notification system. ArXiv. Preprint posted online on July 20, 2020.
37. Choudhury H, Goswami B, Gurung S. CovidChain: An anonymity preserving blockchain based framework for protection against COVID-19. ArXiv. Preprint posted online on May 15, 2020 [FREE Full text]
38. Liu JK, Au MH, Yuen TH, Zuo C, Wang J, Sakzad A, et al. Privacy-preserving COVID-19 contact tracing app: A zero-knowledge proof approach. Cryptology ePrint Archive. Preprint posted online on May 5, 2020 [FREE Full text]
39. Kirch W. Contact tracing. In: Kirch W, editor. Encyclopedia of Public Health. Dordrecht, the Netherlands: Springer; 2008:164.
40. Eames KTD, Keeling MJ. Contact tracing and disease control. Proc Biol Sci 2003 Dec 22;270(1533):2565-2571 [FREE Full text] [doi: 10.1098/rspb.2003.2554] [Medline: 14728778]
41. Day M. Covid-19: Four fifths of cases are asymptomatic, China figures indicate. BMJ 2020 Apr 02;369:m1375. [doi: 10.1136/bmj.m1375] [Medline: 32241884]

XSL•FO
RenderX

42. Hasell J, Mathieu E, Beltekian D, Macdonald B, Giattino C, Ortiz-Ospina E, et al. A cross-country database of COVID-19 testing. Sci Data 2020 Oct 08;7(1):345 [FREE Full text] [doi: 10.1038/s41597-020-00688-8] [Medline: 33033256]
43. Salathé M, Althaus CL, Neher R, Stringhini S, Hodcroft E, Fellay J, et al. COVID-19 epidemic in Switzerland: On the importance of testing, contact tracing and isolation. Swiss Med Wkly 2020 Mar 09;150:w20225 [FREE Full text] [doi: 10.4414/smw.2020.20225] [Medline: 32191813]
44. Russell TW, Golding N, Hellewell J, Abbott S, Wright L, Pearson CAB, CMMID COVID-19 Working Group. Reconstructing the early global dynamics of under-ascertained COVID-19 cases and infections. BMC Med 2020 Oct 22;18(1):332 [FREE Full text] [doi: 10.1186/s12916-020-01790-9] [Medline: 33087179]
45. Wilder-Smith A, Freedman DO. Isolation, quarantine, social distancing and community containment: Pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak. J Travel Med 2020 Mar 13;27(2):taaa020 [FREE Full text] [doi: 10.1093/jtm/taaa020] [Medline: 32052841]
46. Mooney G. "A menace to the public health" - Contact tracing and the limits of persuasion. N Engl J Med 2020 Nov 05;383(19):1806-1808. [doi: 10.1056/NEJMp2021887] [Medline: 32877577]
47. Wójcik OP, Brownstein JS, Chunara R, Johansson MA. Public health for the people: Participatory infectious disease surveillance in the digital age. Emerg Themes Epidemiol 2014;11:7 [FREE Full text] [doi: 10.1186/1742-7622-11-7] [Medline: 24991229]
48. O'Shea J. Digital disease detection: A systematic review of event-based internet biosurveillance systems. Int J Med Inform 2017 May;101:15-22 [FREE Full text] [doi: 10.1016/j.ijmedinf.2017.01.019] [Medline: 28347443]
49. Contact transmission of COVID-19 in South Korea: Novel investigation techniques for tracing contacts. Osong Public Health Res Perspect 2020 Mar;11(1):60-63 [FREE Full text] [doi: 10.24171/j.phrp.2020.11.1.09] [Medline: 32149043]
50. Smieszek T, Castell S, Barrat A, Cattuto C, White PJ, Krause G. Contact diaries versus wearable proximity sensors in measuring contact patterns at a conference: Method comparison and participants' attitudes. BMC Infect Dis 2016 Jul 22;16:341 [FREE Full text] [doi: 10.1186/s12879-016-1676-y] [Medline: 27449511]
51. Armbruster B, Brandeau ML. Contact tracing to control infectious disease: When enough is enough. Health Care Manag Sci 2007 Dec;10(4):341-355 [FREE Full text] [doi: 10.1007/s10729-007-9027-6] [Medline: 18074967]
52. Armstrong D. The rise of surveillance medicine. Sociol Health Illn 1995 Jun;17(3):393-404. [doi: 10.1111/1467-9566.ep10933329]
53. Roman-Belmonte JM, De la Corte-Rodriguez H, Rodriguez-Merchan EC. How blockchain technology can change medicine. Postgrad Med 2018 May;130(4):420-427. [doi: 10.1080/00325481.2018.1472996] [Medline: 29727247]
54. Venkataraman N, Poon BH, Siau C. Innovative use of health informatics to augment contact tracing during the COVID-19 pandemic in an acute hospital. J Am Med Inform Assoc 2020 Dec 09;27(12):1964-1967 [FREE Full text] [doi: 10.1093/jamia/ocaa184] [Medline: 32835358]
55. Bianconi A, Marcelli A, Campi G, Perali A. Efficiency of COVID-19 mobile contact tracing containment by measuring time-dependent doubling time. Phys Biol 2020 Oct 09;17(6):065006. [doi: 10.1088/1478-3975/abac51] [Medline: 32750685]
56. Lin L, Hou Z. Combat COVID-19 with artificial intelligence and big data. J Travel Med 2020 Aug 20;27(5):taaa080 [FREE Full text] [doi: 10.1093/jtm/taaa080] [Medline: 32437541]
57. Morawska L, Milton DK. It is time to address airborne transmission of coronavirus disease 2019 (COVID-19). Clin Infect Dis 2020 Dec 03;71(9):2311-2313 [FREE Full text] [doi: 10.1093/cid/ciaa939] [Medline: 32628269]
58. Leith DJ, Farrell S. Google/Apple exposure notification due diligence. In: Proceedings of the CoronaDef Workshop, Network and Distributed System Security Symposium (NDSS). 2021 Presented at: CoronaDef Workshop, Network and Distributed System Security Symposium (NDSS); February 21, 2021; Virtual URL: https://www.ndss-symposium.org/wp-content/uploads/coronadef2021_23005_paper.pdf [doi: 10.14722/coronadef.2021.23005]
59. Hoffman AS, Jacobs B, van Gastel B, Schraffenberger H, Sharon T, Pas B. Towards a seamful ethics of Covid-19 contact tracing apps? Ethics Inf Technol 2020 Sep 28:1-11 [FREE Full text] [doi: 10.1007/s10676-020-09559-7] [Medline: 33013191]
60. Reichert L, Brack S, Scheuermann B. A survey of automatic contact tracing approaches using Bluetooth Low Energy. ACM Trans Comput Healthc 2021 Mar;2(2):1-33. [doi: 10.1145/3444847]
61. Raghavan A, Ananthapadmanaban H, Sivamurugan M, Ravindran B. Accurate mobile robot localization in indoor environments using Bluetooth. In: Proceedings of the 2010 International Conference on Robotics and Automation.: IEEE; 2010 Presented at: 2010 International Conference on Robotics and Automation; May 3-7, 2010; Anchorage, AK p. 4391-4396. [doi: 10.1109/robot.2010.5509232]
62. Bertuletti S, Cereatti A, Caldara M, Galizzi M, Croce U. Indoor distance estimated from Bluetooth Low Energy signal strength: Comparison of regression models. In: Proceedings of the 2016 Sensors Applications Symposium (SAS).: IEEE; 2016 Presented at: 2016 Sensors Applications Symposium (SAS); April 20-22, 2016; Catania, Italy p. 1-5. [doi: 10.1109/sas.2016.7479899]
63. Merry K, Bettinger P. Smartphone GPS accuracy study in an urban environment. PLoS One 2019;14(7):e0219890 [FREE Full text] [doi: 10.1371/journal.pone.0219890] [Medline: 31318933]
64. Jung W, Bell S, Petrenko A, Sizo A. Potential risks of WiFi-based indoor positioning and progress on improving localization functionality. In: Proceedings of the 4th International Workshop on Indoor Spatial Awareness.: ACM; 2012 Presented at:

XSL•FO
RenderX

4th International Workshop on Indoor Spatial Awareness; November 6, 2012; Redondo Beach, CA p. 13-20. [doi: 10.1145/2442616.2442621]

65. Schipperijn J, Kerr J, Duncan S, Madsen T, Klinker CD, Troelsen J. Dynamic accuracy of GPS receivers for use in health research: A novel method to assess GPS accuracy in real-world settings. Front Public Health 2014;2:21 [FREE Full text] [doi: 10.3389/fpubh.2014.00021] [Medline: 24653984]
66. Chadha K. The global positioning system: Challenges in bringing GPS to mainstream consumers. In: Proceedings of the 1998 International Solid-State Circuits Conference.: IEEE; 1998 Presented at: 1998 International Solid-State Circuits Conference; February 5-7, 1998; San Francisco, CA p. 26-28. [doi: 10.1109/isscc.1998.672333]
67. Chen Q, Wang B, Deng X, Mo Y, Yang L. Placement of access points for indoor wireless coverage and fingerprint-based localization. In: Proceedings of the 10th International Conference on Embedded and Ubiquitous Computing.: IEEE; 2013 Presented at: 10th International Conference on Embedded and Ubiquitous Computing; November 13-15, 2013; Zhangjiajie, China p. 2253-2257. [doi: 10.1109/hpcc.and.euc.2013.323]
68. Kangbai JB, Jame PB, Mandoh S, Fofanah AB, George A, Briama A, et al. Tracking Ebola through cellphone, Internet of Things and Blockchain technology. Curr Res Integr Med 2018;1(2):13-15 [FREE Full text] [doi: 10.4172/2529-797x.1000035]
69. Lo S, Xu X, Chiam Y, Lu Q. Evaluating suitability of applying Blockchain. In: Proceedings of the 22nd International Conference on Engineering of Complex Computer Systems.: ACM; 2017 Presented at: 22nd International Conference on Engineering of Complex Computer Systems; November 5-8, 2017; Fukuoka, Japan p. 158-161. [doi: 10.1109/iceccs.2017.26]
70. Wüst K, Gervais A. Do you need a Blockchain? In: Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT).: IEEE; 2018 Presented at: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT); June 20-22, 2018; Zug, Switzerland p. 45-54. [doi: 10.1109/cvcbt.2018.00011]
71. Gostin L, Sapsin J, Vernick J, Teret S, Burris S. SARS and international legal preparedness. Temple Law Rev 2004;77:155-174 [FREE Full text]
72. Ogbuji C. Clinical data acquisition, storage and management. In: Liu L, Özsu M, editors. Encyclopedia of Database Systems. New York, NY: Springer; 2016.
73. Ferreira A, Correia R, Chadwick D, Antunes L. Access control in healthcare: The methodology from legislation to practice. Stud Health Technol Inform 2010;160(Pt 1):666-670. [Medline: 20841770]
74. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 2020 May 08;368(6491):eabb6936 [FREE Full text] [doi: 10.1126/science.abb6936] [Medline: 32234805]
75. Couch DL, Robinson P, Komesaroff PA. COVID-19-extending surveillance and the panopticon. J Bioeth Inq 2020 Dec;17(4):809-814 [FREE Full text] [doi: 10.1007/s11673-020-10036-5] [Medline: 32840859]
76. Csernatoni R. New states of emergency: Normalizing techno-surveillance in the time of COVID-19. Glob Aff 2020 Oct 02;6(3):301-310. [doi: 10.1080/23340460.2020.1825108]
77. Ram N, Gray D. Mass surveillance in the age of COVID-19. J Law Biosci 2020;7(1):lsaa023 [FREE Full text] [doi: 10.1093/jlb/lsaa023] [Medline: 32728466]
78. Taddeo M. The ethical governance of the digital during and after the COVID-19 pandemic. Minds Mach (Dordr) 2020 Jun 12:1-6 [FREE Full text] [doi: 10.1007/s11023-020-09528-5] [Medline: 32836869]
79. Clarke R, Wigan M. You are where you've been: The privacy implications of location and tracking technologies. J Location Based Serv 2011 Sep;5(3-4):138-155. [doi: 10.1080/17489725.2011.637969]
80. Dooley JF. Introduction: A revolutionary cipher. In: History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms. Cham, Switzerland: Springer; 2018:1-11.
81. Fischer-Hübner S. Privacy-enhancing technologies. In: Liu L, Özsu MT, editors. Encyclopedia of Database Systems. New York, NY: Springer; 2017:1-7.
82. Harron K, Dibben C, Boyd J, Hjern A, Azimaee M, Barreto ML, et al. Challenges in administrative data linkage for research. Big Data Soc 2017 Dec 05;4(2):1-12 [FREE Full text] [doi: 10.1177/2053951717745678] [Medline: 30381794]
83. Fedorov AK, Kiktenko EO, Lvovsky AI. Quantum computers put blockchain security at risk. Nature 2018 Nov;563(7732):465-467. [doi: 10.1038/d41586-018-07449-z] [Medline: 30451981]
84. Peng L, Feng W, Yan Z, Li Y, Zhou X, Shimizu S. Privacy preservation in permissionless blockchain: A survey. Digit Commun Netw 2020 Jun:1-13 (forthcoming) [FREE Full text] [doi: 10.1016/j.dcan.2020.05.008]
85. Marx M, Zimmer E, Mueller T, Blochberger M, Federrath H. Hashing of personally identifiable information is not sufficient. In: Proceedings of the 9th Annual Conference of the Security Department.: Gesellschaft für Informatik e.V; 2018 Presented at: 9th Annual Conference of the Security Department; April 25-27, 2018; Konstanz, Germany p. 55-68 URL: https://dl.gi.de/bitstream/handle/20.500.12116/16294/sicherheit2018-04.pdf?sequence=1&isAllowed=y [doi: 10.18420/sicherheit2018_04]
86. Wandhofer R, Berndsen R. Proof-of-work blockchains and settlement finality: A functional interpretation. J Financ Mark Infrastructures 2019;7(4):71-104. [doi: 10.21314/jfmi.2018.111]
87. Politou E, Casino F, Alepis E, Patsakis C. Blockchain mutability: Challenges and proposed solutions. IEEE Trans Emerg Top Comput 2019:1. [doi: 10.1109/tetc.2019.2949510]

XSL•FO
RenderX

88. Clauson KA, Breeden EA, Davidson C, Mackey TK. Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain. Blockchain Healthc Today 2018 Mar 23;1:1-12 [FREE Full text] [doi: 10.30953/bhty.v1.20]

89. Hofmann F, Wurster S, Ron E, Böhmecke-Schwafert M. The immutability concept of blockchains and benefits of early standardization. In: Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K).: IEEE; 2017 Presented at: 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K); November 27-29, 2017; Nanjing, China p. 1-8. [doi: 10.23919/itu-wt.2017.8247004]

90. Zheng X, Zhu Y, Si X. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. Appl Sci 2019 Nov 06;9(22):4731. [doi: 10.3390/app9224731]

91. Sohrabi N, Tari Z. On the scalability of blockchain systems. In: Proceedings of the 2020 IEEE International Conference on Cloud Engineering (IC2E).: IEEE; 2020 Presented at: 2020 IEEE International Conference on Cloud Engineering (IC2E); April 21-24, 2020; Sydney, Australia p. 124-133. [doi: 10.1109/ic2e48712.2020.00020]

92. Dang H, Dinh T, Loghin D, Chang E, Lin Q, Ooi B. Towards scaling blockchain systems via sharding. In: Proceedings of the 2019 International Conference on Management of Data.: Association for Computing Machinery; 2019 Presented at: 2019 International Conference on Management of Data; June 30-July 5, 2019; Amsterdam, the Netherlands p. 123-140. [doi: 10.1145/3299869.3319889]

93. Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo KR. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. J Netw Comput Appl 2020 Jan;149:102471. [doi: 10.1016/j.jnca.2019.102471]

94. Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor 2020;22(2):1432-1465. [doi: 10.1109/comst.2020.2969706]

95. Lepore C, Ceria M, Visconti A, Rao UP, Shah KA, Zanolini L. A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics 2020 Oct 14;8(10):1782. [doi: 10.3390/math8101782]

96. Dabbagh M, Choo KR, Beheshti A, Tahir M, Safa NS. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. Comput Secur 2021 Jan;100:102078. [doi: 10.1016/j.cose.2020.102078]

97. Hao Y, Li Y, Dong X, Fang L, Chen P. Performance analysis of consensus algorithm in private blockchain. In: Proceedings of the 2018 Intelligent Vehicles Symposium.: IEEE; 2018 Presented at: 2018 Intelligent Vehicles Symposium; June 26-30, 2018; Changshu, China p. 280-285. [doi: 10.1109/ivs.2018.8500557]

98. Haughian G, Osman R, Knottenbelt W. Benchmarking replication in Cassandra and MongoDB NoSQL datastores. In: Proceedings of the 27th International Conference on Database and Expert Systems Applications.: Springer; 2016 Presented at: 27th International Conference on Database and Expert Systems Applications; September 5-8, 2016; Porto, Portugal p. 152-166. [doi: 10.1007/978-3-319-44406-2_12]

99. Standard for blockchain-based omnidirectional pandemic/epidemic surveillance: Overarching framework. IEEE Standards Association. 2020. URL: https://standards.ieee.org/project/2677_1.html [accessed 2021-03-29]

100. Pirtle C, Ehrenfeld J. Blockchain for healthcare: The next generation of medical records? J Med Syst 2018 Aug 10;42(9):172. [doi: 10.1007/s10916-018-1025-3] [Medline: 30097733]

101. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Blockchain vehicles for efficient medical record management. NPJ Digit Med 2020;3:1 [FREE Full text] [doi: 10.1038/s41746-019-0211-0] [Medline: 31934645]

102. Colin D, Young B. Blockchain and the protection of patient information in line with HIPAA. Int J Cyber Res Educ 2019;1(1):63-68. [doi: 10.4018/ijcre.2019010107]

103. Van Humbeeck A. The Blockchain-GDPR paradox. J Data Prot Priv 2019;2:12.

104. El-Gazzar R, Stendal K. Blockchain in health care: Hope or hype? J Med Internet Res 2020 Jul 10;22(7):e17199 [FREE Full text] [doi: 10.2196/17199] [Medline: 32673219]

105. Smith. The contract net protocol: High-level communication and control in a distributed problem solver. IEEE Trans Comput 1980 Dec;C-29(12):1104-1113. [doi: 10.1109/tc.1980.1675516]

106. Harz D, Knottenbelt W. Towards safer smart contracts: A survey of languages and verification methods. ArXiv. Preprint posted online on November 1, 2018 [FREE Full text]

107. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform 2013 Jun;46(3):541-562 [FREE Full text] [doi: 10.1016/j.jbi.2012.12.003] [Medline: 23305810]

108. Cruz JP, Kaji Y, Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access 2018;6:12240-12251. [doi: 10.1109/access.2018.2812844]

109. Mavridou A, Laszka A, Stachtiari E, Dubey A. VeriSolid: Correct-by-design smart contracts for Ethereum. In: Proceedings of the 23rd International Conference on Financial Cryptography and Data Security.: Springer; 2019 Presented at: 23rd International Conference on Financial Cryptography and Data Security; February 18-22, 2019; Frigate Bay, St. Kitts and Nevis p. 446-465. [doi: 10.1007/978-3-030-32101-7_27]

110. Park S, Im S, Seol Y, Paek J. Nodes in the Bitcoin network: Comparative measurement study and survey. IEEE Access 2019;7:57009-57022. [doi: 10.1109/access.2019.2914098]

111. Li W, Yang Y, Yuan D. Literature review. In: Reliability Assurance of Big Data in the Cloud: Cost-Effective Replication-Based Storage. Waltham, MA: Morgan Kaufmann; 2015:9-17.

XSL•FO
RenderX

Abbreviations

ASCLEPIOS: Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare
EHR: electronic health record

Edited by T Sanchez; submitted 12.12.20; peer-reviewed by A Wilder-Smith, F Coelho, P Miranda, Z Yan; comments to author 18.01.21; revised version received 20.02.21; accepted 08.03.21; published 06.04.21

Please cite as:
Platt M, Hasselgren A, Román-Belmonte JM, Tuler de Oliveira M, De la Corte-Rodríguez H, Delgado Olabarriaga S, Rodríguez-Merchán EC, Mackey TK
Test, Trace, and Put on the Blockchain?: A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Contact Tracing to Combat a Global Pandemic
JMIR Public Health Surveill 2021;7(4):e26460
URL: https://publichealth.jmir.org/2021/4/e26460
doi: 10.2196/26460
PMID: 33727212

©Moritz Platt, Anton Hasselgren, Juan Manuel Román-Belmonte, Marcela Tuler de Oliveira, Hortensia De la Corte-Rodríguez, Sílvia Delgado Olabarriaga, E Carlos Rodríguez-Merchán, Tim Ken Mackey. Originally published in JMIR Public Health and Surveillance (http://publichealth.jmir.org), 06.04.2021. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in JMIR Public Health and Surveillance, is properly cited. The complete bibliographic information, a link to the original publication on http://publichealth.jmir.org, as well as this copyright and license information must be included.

XSL•FO
RenderX