Public Health Surveillance using Decentralized Technologies

Bellod Cisneros, Jose Luis; Aarestrup, Frank Møller; Lund, Ole

Published in:
Blockchain in Healthcare Today

Link to article, DOI:
10.30953/bhty.v1.17

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

BLOCKCHAIN™ IN HEALTHCARE TODAY

Public Health Surveillance using Decentralized Technologies

Jose Luis Bellod Cisneros,[1] Frank Møller Aarestrup,[2] Ole Lund[1]

Authors: [1]DTU Bioinformatics, Kgs. Lyngby, 2800, Denmark. [2]DTU Food, Kgs. Lyngby, 2800, Denmark

Corresponding author: Jose Luis Bellod Cisneros. cisneros@bioinformatics.dtu.dk

Keywords: Blockchain, Cosmos Framework, Decentralized Technology, Public Health Surveillance

Category: Use Cases/Pilots/Methodologies

This article describes how blockchain technologies can be used in the context of Public Health Surveillance through decentralized sharing of genomic data. A brief analysis of why blockchain technologies are needed in public health is presented together with a distinction between public and private blockchains. Finally, a proposal for a network of blockchains, using the Cosmos framework, together with decentralized storage systems like IPFS and BigchainDB, is included to address the issues of interoperability in the health sector.

Keywords: Blockchain, Cosmos Framework, Decentralized Technology, Public Health Surveillance

Next-Generation Sequencing Technologies are creating new opportunities in the fields of animal and human health due to the rapid decrease in cost and high-throughput of data generation. When the size and price of sequencing devices drop significantly, public health institutions could use the technology to perform routine clinical diagnostics.

These technologies have the potential to become so widespread that storing genomic information could be a problem due to the sensitivity of the data and the technological and ethical challenges arising from sharing genetic information that might be linked to future health disease for individuals.

In the context of an emerging disease, data sharing becomes critical to act rapidly for fast diagnosis and better treatment. Currently, the technology is still expensive so it's not widely accessible yet to private individuals, but that may change in the near future. Several public institutions like the DNA Data Bank of Japan, GenBank (USA) and the European Nucleotide Archive (UK)

store genomic data and provide free and open access to it. Data providers, like sequencing labs and research institutions, initially keep the data private before publication of the study results, which goes against rapid-sharing protocols. New developments in technologies like Oxpord Nanopore[1] could challenge this by offering in-place real-time analysis that can discard raw data thanks to the use of streaming algorithms.[2] Other factors that influence rapid and open data sharing include patenting and intellectual property, fear of losing control over the data that can be commercialized (outside their borders), reputation and economic damage.

There are several initiatives that aim to create an interoperability network for data sharing like COMPARE[3] and the Global Microbial Identifier that are planning to develop a centralized or confederated solution where all the data are stored. This creates several issues regarding the ownership of an individual's DNA and the related data that comes from the sequencing process but also how to deal with interoperability to connect data consumers and providers when needed, outside the centralized network.

TRADITIONAL PUBLIC HEALTH SURVEILLANCE APPROACH

Researches have until now followed the approach of gathering genomic data locally and, after the analysis and publication are finished, release the data to the community through global repositories. Aarestrup and Koopmans[4] address a set of barriers for the sharing of data pre-publication, freely and in real-time: lack of data standardization, political sensitivities, national regulations and laws, ethical issues and intellectual property rights. Aarestrup and Koopmans suggest that the decreasing cost and accelerated development of Next Generation Sequencing (NGS) can be used as a common language for the exchange of genomic information. To avoid the legal and ethical challenges associated with data sharing, a hybrid public/private publication model will ensure real-time access to the data with the option of temporarily keeping the data private to guarantee that public health authorities can evaluate any issue regarding sensitive data.

The rationale behind public health surveillance and interoperability between systems is not new. For example, in[5] several unstructured event-based report systems like the Global Public Health Intelligence Network, HealthMap, and EpiSPIDER are evaluated, concluding that those systems, even though developed separately, are highly complementary. In the European Union (EU) we can find many health systems and databases that are fragmented and lack harmonization of data, methodologies, and common analysis practices due to the fact that each state has the responsibility of regulation of its own healthcare system. Auffray et al.[6] recommend five initiatives to provide a common framework for data interoperability in the EU: launching pilot projects on Big Data, promoting open access and transparency of data, methodologies and publications, creation of a multidisciplinary involvement of all stakeholders in the health care industry, use state-of-the-art mathematical and statistical methods and harmonization of European policy and regulatory frameworks.

PUBLIC HEALTH SURVEILLANCE AND PRIVACY

A new European Regulatory framework is currently being addressed by the third EU

Health Program (2014-2020) aiming, among other things, to the establishment of a common network for public health surveillance and control of emerging diseases.[7] One of the aspects addressed by the EU is data protection through the General Data Protection Regulation (GDPR). This regulation focuses on mandatory safeguards implemented by any organization in charge of storing personal health data but also, under certain circumstances, override a subject's right to ensure that his information has been deleted. Public health research falls under the same category as scientific research and several exceptions are added, like permission of data transfer outside national borders in the case of a contagious disease.

USE CASE EXAMPLE

To give an example of how a data-sharing platform would provide a solution in the context of an emerging disease, suspected from imported cucumbers, the following use case is presented from a researcher's point of view: A Danish scientist uploads a set of DNA samples from an ongoing *E. coli* outbreak that has been detected in Denmark. The genomic data are stored in the university's system where permissions are temporarily granted to a colleague in Germany, where the infected cucumbers are suspected to come from.

The German scientist discovers that the origin of the cucumbers can be traced back to Spain, comparing the DNA data to a supply-chain study that he has access to. The supply-chain is linked to a set of human samples from several Spanish hospitals where patients were admitted with gastroenteritis. The patients can be linked to a restaurant chain in Spain that has locations in Denmark and Germany.

PROBLEM DEFINITION

From this very simple example it can be inferred that the described data-sharing system has several features that need to be addressed in order to stop an ongoing disease:

- Permission-based data sharing.
- Interoperability (data located in several places for political or security reasons).
- Common repository and data modeling, to serve as source of truth.
- Fast access to the data that allows a real-time surveillance system.

In the following we will give a short introduction to blockchain and then discuss how it can address some of the problems identified above.

WHAT IS A BLOCKCHAIN?

A blockchain can be described as spreadsheet duplicated across a network of computers. The data that a blockchain contains is shared and no single no single authority has the "official" or unique source of the data. An analogy would be a Google Sheet, where the document is not stored on Google's servers but served by all the participants, with each new entry going through an agreement protocol (consensus mechanism) that establishes the reconciled state of the document that everybody believes to be the shared true state.

WHY IS A BLOCKCHAIN NEEDED?

Decentralized technologies have the potential to increase research opportunities and clinical effectiveness by providing an open platform that addresses interoperability challenges. The following list of conditions, part of Deloitte's blockchain decision framework,[8]

are discussed here in order to consider a blockchain solution:

Multiple Parties Generate Transactions That Change Information in a Shared Repository

It is estimated that the future growth of sequencing technologies could surpass the amount of data produced by online video platforms, like YouTube, in the next ten years.[9] This rapid production of genomic information will provide the basis for real-time comparison of pathogen data, across different countries and sectors, dramatically increasing the effectiveness of disease control. The future spread of the technology will create a heterogeneous ecosystem with many sources of data that will need a common repository for analysis and comparison.

Parties Need to Trust That Transactions are Valid

Data stored in the system needs to be validated and standardized. Sensitive data like human DNA or any other medical data that can be linked to a person needs to be appropriately checked and secured.

Intermediaries are Inefficient or Not Trusted as Arbiters of Truth

Real-time data sharing, and availability are some of the key features of a surveillance system. Any central system can be hacked, or data can be removed due to failures or system malfunctions. Siloed data are slow to access, and permissions need to be manually granted, or relay on sharing passwords with other users compromising security and privacy. In the context of an outbreak, to act rapidly turns out to be crucial to stop the spread of the disease in order to save lives.

Enhanced Security Is Needed to Ensure Integrity of the System

Security is crucial in all aspects of the system, especially for patients but also for other actors who store the data. If security is not guaranteed, nodes will not share or have access to the data. Data could be stored, either encrypted or using a secondary structure for the most sensitive information.

What Blockchain Will Be Used?

Public Health and the health sector in general have a lot of pressure from the legislation to ensure that they comply with the current data-protection rules that ensure that people's privacy is protected. This has had a negative effect on interoperability creating incompatibility between data records and inefficient data-sharing systems.

Blockchains are grouped in two in Deloitte's paper, permissioned and public. Public blockchains allow anybody that wants to join the network to get access to all the information that is available. A more restricted version of permissioned blockchain is a private blockchain. Yuan et al[10] regard private blockchains (in their terminology, the ones controlled by a single entity) "[…] in general a bad idea." "[A private blockchain] controlled by a single entity degenerates to a traditional centralized system with a bit of cryptographic auditability sprinkled on top."[10] Private blockchains don't get any of the benefits of a decentralized system so a traditional database, based for example on cryptographic primitives like Merkle trees,[1] that allows for fast verification of data integrity of large data archives, would be a better solution.

A better way to describe a blockchain where nodes are known and controlled is as a federated blockchain (also called consortium blockchain). This solution offers

several advantages over public blockchains. Federated blockchains "allow for transparent governance within the consortium only."[12] This approach avoids all problems related to public goods (i.e. basic societal goods than can't be excluded from anybody's use), like abuse of the system and spam.

Data Upload and Sharing

In a traditional centralized system, data upload and sharing has to go through a single provider for storage and data permission. While storage services like Dropbox, and AWS do not rely on a single server (rather on a distributed network of servers to guarantee a certain uptime, low latency and backup) it is actually a single organization who controls and practically owns the data.

Genomic information is stored in large gigabyte-size files. Blockchain as a data structure is not suitable for storing this information due to scalability and performance. A different type of data are the associated metadata: country, data of sequencing, provider, pathogenic attributes, species...etc. This data are small compared to the genomic data, but it needs to be searchable and organized efficiently for fast retrieval. Some of these attributes are sensitive since they could be linked to patients or reveal private information.

The Interplanetary File System (IPFS) is one of several candidates which aim is to decentralize and improve the way data are stored on the Internet, based on a paradigm called content-addressable storage, where data are addressed not by where it is located but by the content itself. IPFS is able to handle big files, which aligns very well with big genomic data, and, by using an extra layer called Filecoin,[13] addresses the concerns regarding data privacy using strong encryption techniques. Fillecoin also adds an incentive mechanism that enables the creation of a market for data storage that rewards users for storing and providing accessibility to the information.

Another of the benefits of using IPFS's content-based addressing also affects the speed of data transfers. This is where its name, Interplanetary, comes to importance. If we think about a Mars colony requesting data from earth, "with one-way latencies of between 4 and 24 minutes", the first time the information is accessed will cause a significant waiting time. But after that first attempt is completed, any node closer to the Mars's colony will get it locally without having to request it through any interplanetary communication. We can translate this example to a global surveillance framework, where data needed in Tanzania for analysis in an on-going disease doesn't need to ask for it in any of the overseas databases, with the extra penalty of a slow Internet connection. Using IPFS, a Tanzanian researcher can ask the network for the content of the data and any node, physically located closer to where is needed, will serve it faster and with less round-trip requests.

BigchainDB is a "scalable blockchain database: a big-data database with blockchain characteristics including decentralization, immutability and built-in support for creation & transfer of assets."[14] BigchainDB uses MongoDB, making it suitable for storing and retrieval of tabular or document-based metadata. A blockchain that timestamps genomic-sample uploads and monitors a set of parameters set up by researchers on the uploaded data, could trace a pathogen by analyzing how it spreads

from one patient to another through comparison of DNA from different samples, improving the efficiency of the current disease-control systems. In this example, each sample is hashed, along with the attributes defined by the researcher (species, country of origin…etc.).

A list of peers known only by the consortium can be used to create a private network. In this scenario, each user could own IPFS and BigchainDB nodes, or encrypt the information and use nodes owned by others in the consortium to store the data. Data upload will be done via a common user interface that handles both genomic and metadata upload to the IPFS and BigchainDB nodes and registers and timestamps the creation of digital assets in the blockchain (Figure 1). The blockchain will act as the source of truth, the shared state that all participants in the consortium agree to. While some of the information could be kept public if not important, the blockchain will contain hashes or identifiers to the uploaded genomic data.

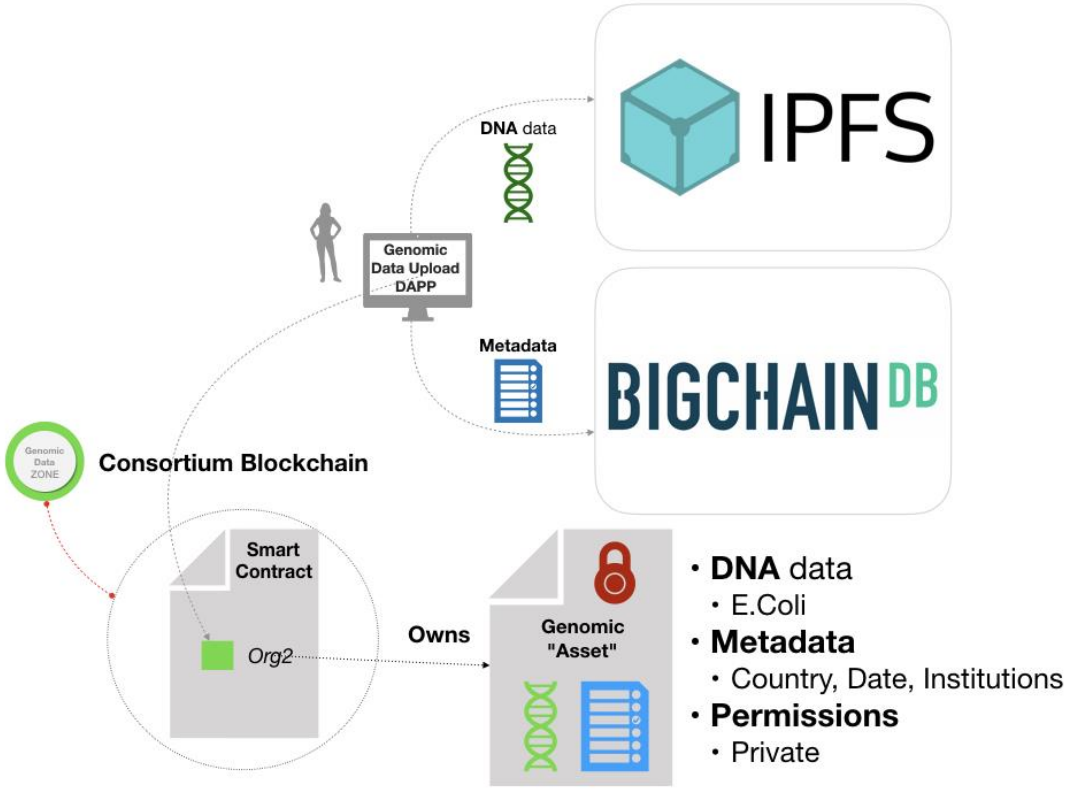

Figure 1. Upload of Genomic Data

This will serve as proof that an event was registered in the system which later can be shared automatically via a set of Smart Contracts (Figure 2) that will act as a validation mechanism (e.g., only the owner can share, sharing happens only with certain users or when certain conditions are met... etc.)

The IPFS and BigchainDB nodes could

monitor the blockchain to listen to "shared transactions" that will whitelist the receiving nodes and replicate the data to them. This pattern creates a problem, known as Data Escapes. How can we prevent users from getting the data and sharing it with unauthorized users? Implementing mechanisms of data-curation could solve this, where data posted would need to go through a validation step that will check if the data was previously uploaded, and then flagged for later review. Since all the transaction regarding access to a genomic resource are registered in the blockchain, it would be easy to narrow down the users that could have shared data without consent of the owner.

DATA DISCOVERY

The proposed framework for a decentralized genomic infrastructure needs to address a very important question regarding data discoverability. In a centralized system there is only one place that holds the information but, in an open infrastructure, there is an unknown number of locations that the users need to access in order to retrieve the data. Another issue is the question of reputation, how can we trust that the requested data are valid and reliable?

A project called Ocean Protocol introduced a token-curated registry model "for establishing trust in network assets and services through staking and reputation." This registry allows a data marketplace to have reputable actors that are incentivized to keep the network alive and to store the data. These actors are rewarded for providing high-quality data that then gets promoted to higher positions in the registry, signaling its value to data consumers. Anybody can challenge the value, quality or source of these data, and the network will reach an agreement whether to keep or remove the challenged dataset.

Interoperability Proposal

Several solutions (Cosmos, Plasma or Polkadot) have approached the problem of interoperability between blockchains in different forms. Public blockchains might exist as the arbiters of truth when conflicts arise, for example, governance of the protocol or, in the context of sidechains where Bitcoin can provide extra security to the pegged blockchains, as was the case of the national currencies backed by gold in the past. Off-chain storage or federated blockchains could be used to overcome the scalability and performance issues of these public blockchains, moving most of the computation off chain, resulting in cheaper and faster transactions.

Figure 3 shows a proposal for a network of blockchains based on the Cosmos network architecture, powered by Tendermint's consensus mechanism[16] (an adaptation of the Practical Byzantine Fault Tolerance[17] algorithm that uses proof-of-stake[18] to achieve distributed consensus). This system does not spend time solving any computationally difficult cryptographic puzzle to elect the proposer of the next block, making it environmentally efficient and faster than current proof-of-work[19] blockchains.

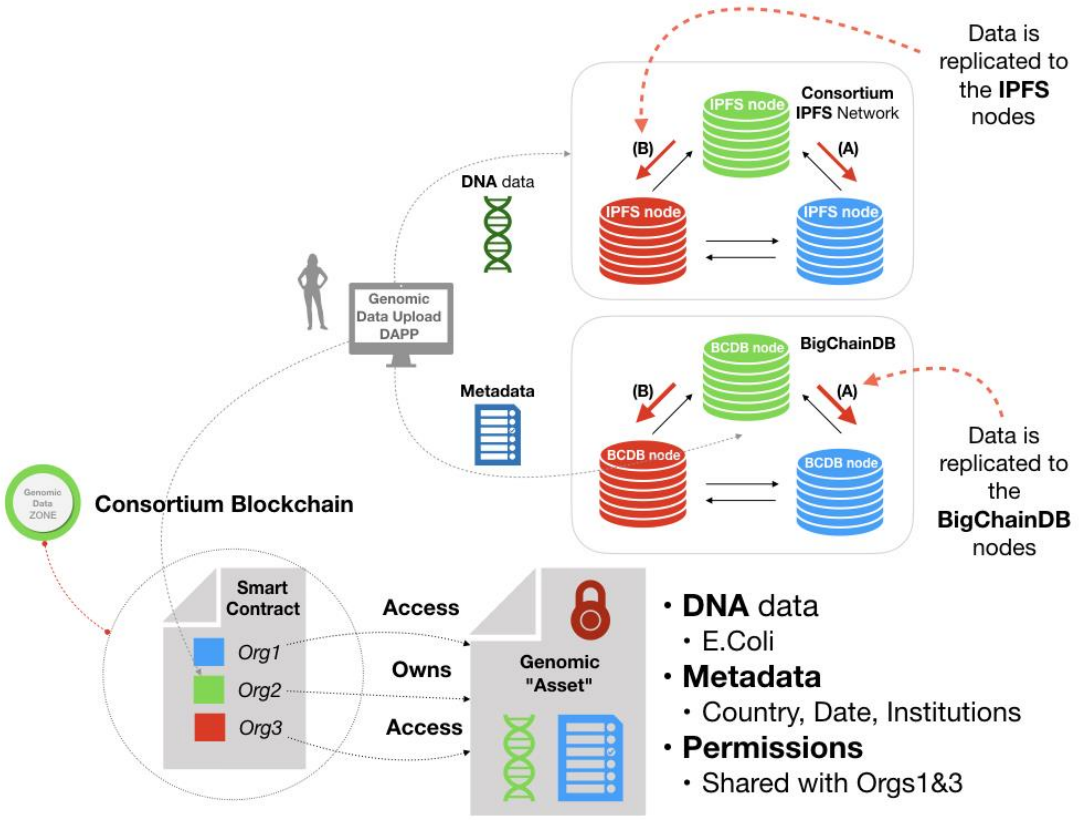

Figure 2. Sharing uploaded data

Zones belong to organizations made up of several partners (public hospitals in the same country). They can be considered as blockchains (federated or public) and are independent of each other. Hubs act as exchanges that coordinate sharing information through transfer of tokens between zones and Hubs external to the consortium that manages the network.

The central Hub would provide the basis for user-management access, and to keep a global state across all Zones. The Hub would take care of how data sharing of biological data are granted (tokens representing permissions to access the data), provide the infrastructure to be connected to other zones (Ethereum, private chains…) and implement governance mechanism to coordinate all participants in the network.

The system could work as follows. Each Zone would be implemented using Tendermint's Application Blockchain Interface (ABCI) that uses a set of Smart Contracts for handling permission and access to the blockchain and File distributed storage servers (IPFS) that allows for data uploading. Tendermint's ABCI allows for more flexibility since the application logic can be implemented in any programming language. This flexibility is what allows for Cosmos to create a common mechanism for different ABCIs to talk to each other.

The consortium will create a template ABCI app that can be used or changed by other members of the consortium, granted that they keep Tendermint's communication protocol unchanged. This ABCI will be the basis for each zone with the following features:

- Permission management (via Monax's implementation of the Ethereum Virtual Machine on top of Tendermint's consensus engine),
- Data upload interfaces to a decentralized storage network for genomic data and associated metadata through IPFS and BigchainDB nodes,
- A set of seed nodes to bootstrap the network,
- Smart contracts to handle registry and sharing of data,
- Real-time monitoring of new data (biological samples) pushed into the zone,
- Consortium members with validation access can access the data.

The role of the Central Hub is critical when aiming to connect to other organization who are willing to participate in the data sharing but reluctant to agree to the governance model of a specific network or worried about privacy and security. The flexibility of Tendermint's design allows for zones and hubs to communicate state changes "via an inter-blockchain communication (IBC) protocol, a kind of virtual UDP or TCP for blockchains."[20]

Cosmos also provides a governance mechanism based on validators and delegators. Validators are the equivalent of miners and their task is to keep the network running and to commit new blocks. Delegators are token holders that delegate their task to others and share the rewards of validating new blocks. Each zone has an independent governance mechanism and the hub or the other zones have no control of it. Validators and delegators use their tokens to vote on proposals to change or upgrade the network.

DECENTRALISED DATA ANALYSIS

Some of the initiatives that are building systems for public health surveillances like COMPARE or GMI rely on a centralized system where all the data are aggregated and compared. This allows for a very fast comparison and monitoring since all the data resides in one place and therefore there is no need to move it from one place to another.

The decentralized system for data upload and sharing described above relies on data to be physically moved to different locations in order to be accessed. In the context of an outbreak, moving genomic data, possibly several or even hundreds of samples of gigabyte size in a short amount of time is not feasible, especially if data are coming from places with very low internet connectivity.

Other reason not to move the data would be when legislation, privacy or data protection goes against the data to be moved outside a geographical jurisdiction or public health institution.

Microsoft has recently released the Coco Framework. Coco is an open source project aimed to provide confidentiality and scalability to enterprise consortiums where actors are known and controlled. One of the most interesting additions that Coco brings to the enterprise blockchain space is the integration of trusted execution environments (TEEs) like Intel SGX and Windows Virtual Secure Mode (VSM). This set of machine operations allow to create a private enclave with privileged access to memory and computation, all protected from other processes running in the same CPU by a cryptographic key.

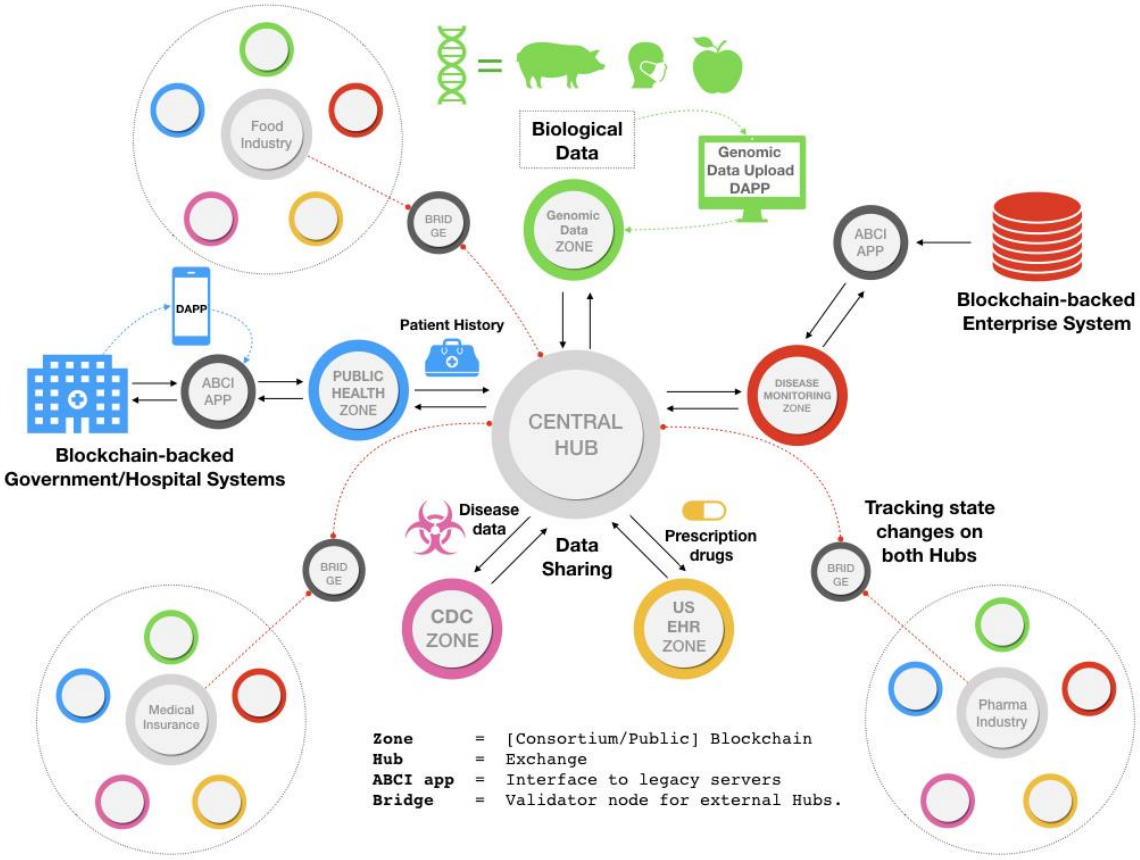

Figure 3. Proposal for a Public Health Network based on Cosmos

In Figure 4-5 we can see a proposal of a system that still relies on the data being stored in a decentralized way but that has been encrypted with private keys being stored in a TEE. This is controlled by an Oracle (i.e. external service that monitors the blockchain) (figure 5) that listens to sharing transactions and uploads the encrypted data to the TEE.

The users who participate in the sharing transaction control the private keys that live in the TEE, making them the only ones who can see the decrypted data. The Enclave will then run the computation on the data and later encrypt the results that will be sent back to the users.

This approach still relies on the transfer of data that could be prohibitive if it were big genomic data. An alternative approach to gathering the data in one place and run the analysis, is to use what it's called federated learning where a machine learning model is sent encrypted (with keys living in the TEE) to all the places that store the data. The model will improve each time, but nobody will be able to access the improved model until it has finished its learning process. Only then it can be then decrypted it when it comes back to the TEE and encrypted again with the public keys of the users that requested the analysis.

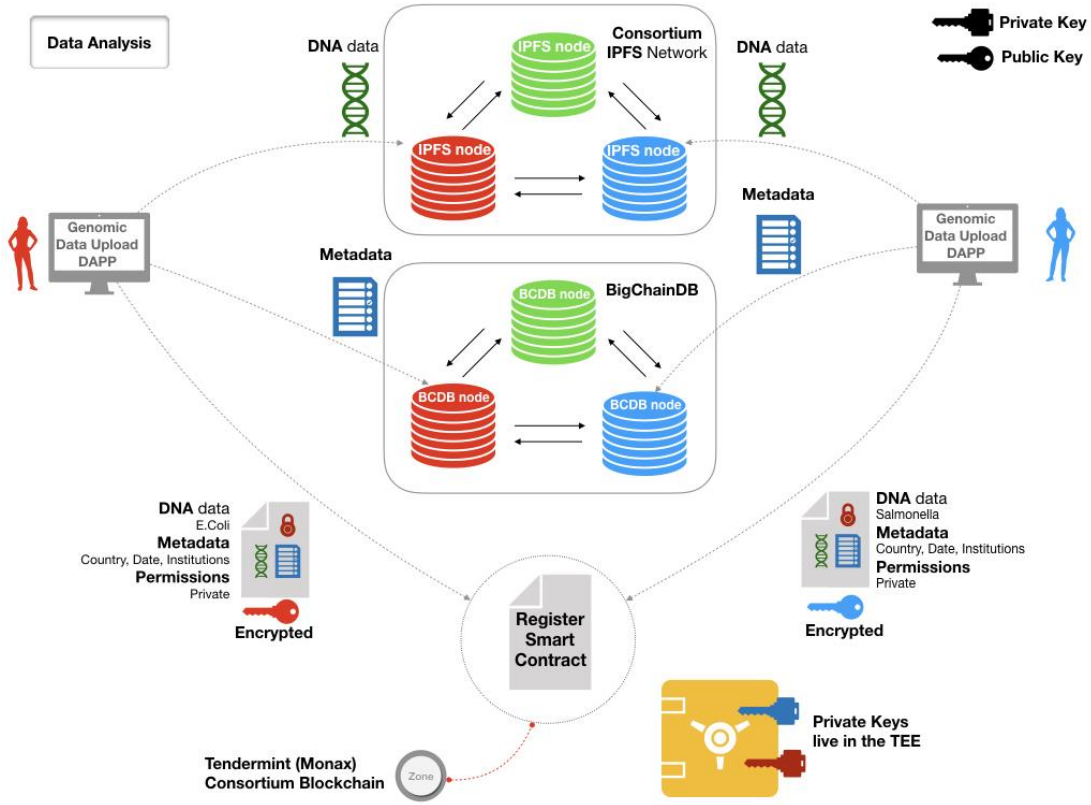

Figure 4. Proposal for analysis of data in a TEE

One caveat is that we need a method that is able to handle encrypted data. This is called homomorphic encryptio[21] and allows performing mathematical operations on encrypted data that generates the right result without revealing its content. This approach can be used in training machine learning models that use simple addition, multiplication and other mathematical operations than can be encrypted using homomorphic encryption. This method has been used by the Open Source project OpenMined, combining deep learning, federated learning, homomorphic encryption (Figure 6) and economic incentivization via smart contracts and cryptocurrency.

CONCLUSION

A brief introduction to the importance of data sharing in the context of public health surveillance has been presented, with a proposal of a decentralized solution. The goal of such a system would be to provide interoperability between several partners that want to share data but are concerned about their privacy.

There are several implications of this approach that will need to be addressed: the need of bringing institutional partners to join the system, technical challenges on how to define the interfaces to the blockchain network, the role of privacy and security for sensitive data and the impact of decentralization in the organizational infrastructure to eliminate inefficiencies for data sharing.

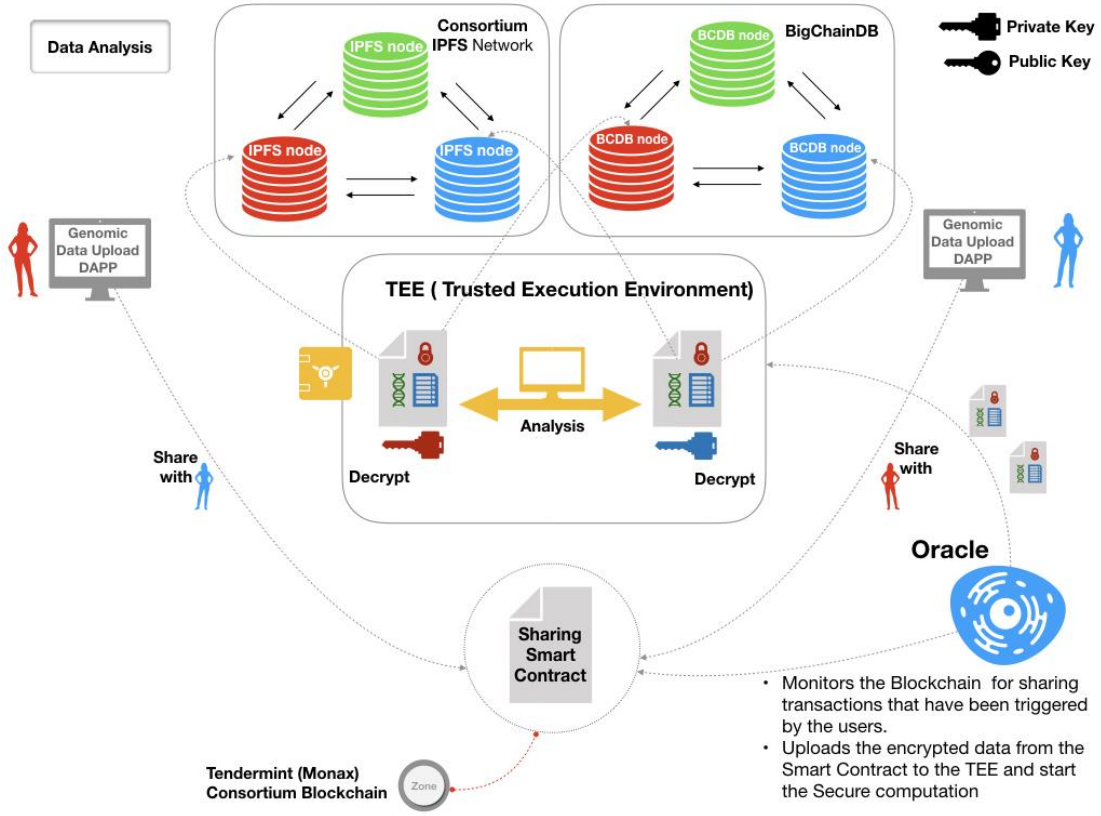

Figure 5. Proposal for analysis of Data in a TEE (II)

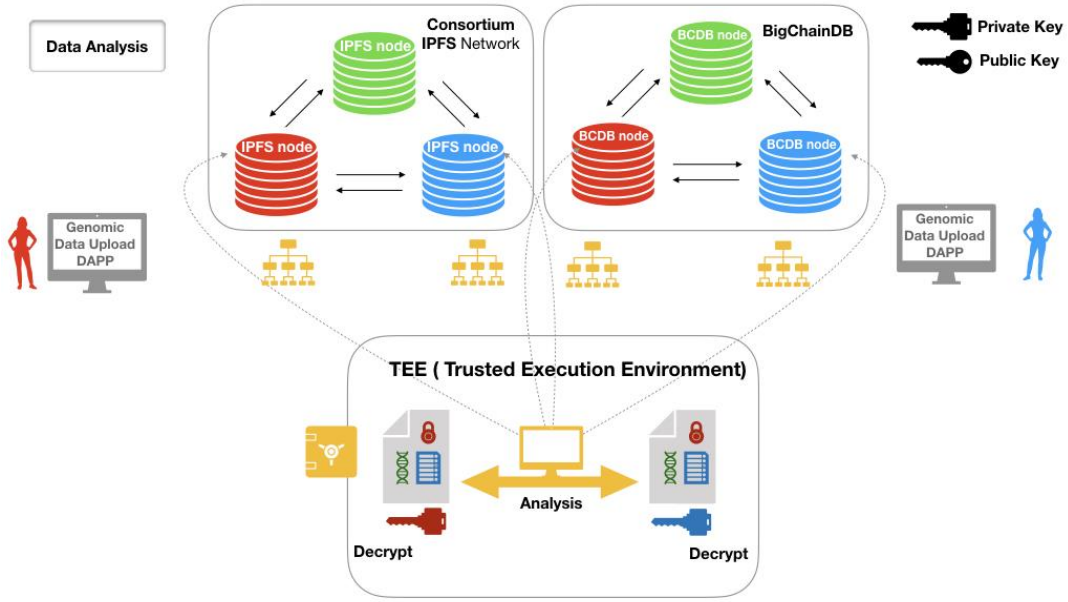

Figure 6. Proposal for analysis of Genomic Data using Homomorphic encryption

The proposed design of a network of blockchains with data upload and sharing capabilities could be built in different stages. First, a simple data-uploading interface to IPFS or BigchainDB that can be later expanded into a consortium blockchain, using Cosmos, that finally adds computing capabilities using TEEs or federated learning via homomorphic encryption. Another aspect that has not been analyzed here, but worth mentioning, is the possibility of the creation of a genomic data market place. Keeping in mind the exponential progression of sequencing technologies, one can imagine a future where sequencing devices become small enough to become pervasive, making it possible to sequence "everything, everywhere." One of the latest developments in this direction is the Ocean Protocol powered by BigchainDB that aims to unlock siloed data for AI research, connecting data providers and consumers. The challenge here is how to incentivize high-quality data that is public or private but that has to comply with privacy and security regulations.

Competing interests

There are no competing interests

List of abbreviations used (if any)

AWS = Amazon Web Services
ABCI = Application Blockchain Interface
EU = European Union
GMI = Global Microbial Identifier
IPFS = Interplanetary File System
NGS = Next Generation Sequencing
TEE = Trusted Execution Environment

Funding statement

This study was supported by the Center for Genomic Epidemiology (www.genomicepidemiology.org) grant 09-067103/DSF from the Danish Council for Strategic Research and by COMPARE http://www.compare-europe.eu/, a European Union project under grant agreement No 643476.

References

1. Nanopore O. SmidgION. URL https://nanoporetech.com/products/smidgion.
2. Cao, MD, Ganesamoorthy D, Elliott AG, et al. "Streaming algorithms for identification of pathogens and antibiotic resistance potential from real-time MinION™ sequencing." *GigaScience* 5.1 (2016): 32.
3. COMPARE. Collaborative management platform for detection and analyses of (re-) emerging and foodborne outbreaks in Europe. URL http://www.compare-europe.eu/about.
4. Aarestrup FM, Koopmans MG. "Sharing data for global infectious disease surveillance and outbreak detection." *Trends in microbiology* 24.4 (2016): 241-245.
5. Keller M, Blench M, Tolentino H, et al. "Use of unstructured event-based reports for global infectious disease surveillance." *Emerging infectious diseases* 15.5 (2009): 689.
6. Auffray C, Balling R, Barroso I, et al. "Making sense of big data in health research: towards an EU action plan." *Genome medicine* 8.1 (2016): 71.
7. Burgun A, Bernal-Delgado E, Kuchinke W. et al. "Health Data for Public Health: Towards New Ways of Combining Data Sources to Support Research Efforts in Europe." *Yearbook of medical informatics* 26.01 (2017): 235-240.

8. Krawiec R. White M. Blockchain: Opportunities for health care. URL https:// www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf.
9. Stephens, ZD, Lee SY, Faghri F, et al. Big data: astronomical or genomical? *PLoS Biol*. 13, e1002195 (2015).
10. Yuan, B., Lin, W. & McDonnell, C. Blockchains and electronic health records. McDonnell. mit. edu.
11. Merkle, Ralph C. "A digital signature based on a conventional encryption function." *Conference on the Theory and Application of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1987.
12. Monax. Permissioned blockchains. URL https://monax.io/explainers/permissioned_blockchains/.
13. Labs P. Filecoin: A decentralised storage network. URL https://filecoin.io/filecoin.pdf.
14. McConaghy T. Marques R, Muller A, et al. Bigchaindb: a scalable blockchain database. white paper, BigchainDB (2016).
15. Back A, Corallo M, Dashjr L, et al. "Enabling blockchain innovations with pegged sidechains."*URL:http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains* (2014).
16. Buchman E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. Diss. 2016.
17. Castro M, Liskov B, et al. Practical byzantine fault tolerance. In OSDI, vol. 99, 173–186 (1999).
18. Buterin V, Griffith V. "Casper the Friendly Finality Gadget." arXiv preprint arXiv:1710.09437 (2017).
19. Jakobsson M, Juels A. "Proofs of work and bread pudding protocols." Secure Information Networks. Springer US, 1999. 258-272.
20. Kwon, J. & Buchman, E. Cosmos: A network of distributed ledgers. 2016. URL https://cosmos.network/whitepaper
21. Armknecht F, Boyd C, Carr C, et al. A Guide to Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*. 2015 (2015): 1192.