Role of Blockchain technology in managing the pandemic (COVID-19)

Aditya Vadgama
Student of Computer Science at
Royal Melbourne Institute of Technology
Melbourne, Australia
s3845898@student.rmit.edu.au

***Abstract*—**Countless sectors like finance, medicine, manufacturing, and education are adopting the Blockchain technology for the robust integrity and flawless traceability it provides which is absolutely essential in today's market. In this paper, I conduct an analysis on Blockchain's unique properties and how they could pave the way to managing data better in a pandemic such as COVID-19. In other words, a systematic review of blockchain-based applications is demonstrated that could provide support across multiple domains, while consistently referring to the key factors revolving around blockchain, i.e. the integrity, security and traceability of the data. Lastly, I also point to the benefits as well as the shortcomings that the blockchain technology presents, with which I hope to define the understanding of this technology better for open science and beyond.

Keywords—*Blockchain; Applications; COVID-19 pandemic*

I. Introduction

Blockchain technology is, at its very core, a chain of blocks that contain some real-world information, for example, a list of transactions. The way these blocks are connected is what defines their strength – each subsequent block contains its own unique hash, along with the hash from the previous block. Essentially, this whole network of blocks can be visualized as an "open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way", which offers an alternative to the traditional intermediary for financial transactions.

The hash code contained by every block in the network is created by a math function that takes digital information and generates a string of letters and numbers from it. Any change to the original input will generate a new hash. If an intruder modifies the information buried in the 564th block, it's hash will also get modified and the chain will break. In order to avoid that, the intruder will have to recalculate the hash of the 563rd block, and then of 562nd block, and so on and so forth. Recalculating all the previous hashes would take an enormous amount of computing power and time, given the real-world applications have millions of blocks. In general, appending a new record to the Blockchain database is allowed, however, by design a Blockchain provides outstanding resistance to modification of the data already committed to the network.

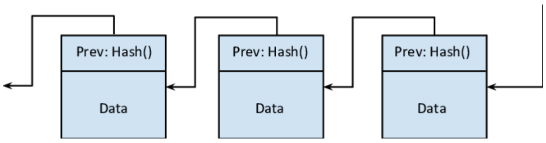

Figure 1. Hashes in a Blockchain

Because of being able to deliver such a unique approach to securing information, Blockchain technology can be applied to any multi-step transaction where traceability and visibility is required. Major portions of the financial industry are implementing distributed ledgers for use in banking. Supply chain is another notable use case where Blockchain can be leveraged to manage and sign contracts and audit product provenance. It could also be leveraged for voting platforms, titles and deed management. Additionally, the development of Blockchain solutions in the healthcare industry are dominated by prototypes, proof-of-concept efforts and initial phases of project investments. These prototypes aim to solve existing problems, with a focus on public health, advanced research modalities, prescriptions monitoring, lowering administrative overheads, and organizing patient data.

The analysis in this report will primarily discuss how a system could be designed using Blockchain concepts that will potentially help enhance the traceability, immutableness and integrity of data in a situation like the COVID-19 pandemic, by providing multiple real-world scenarios and diagrams. Following on, I will also highlight the key advantages and disadvantages of using Blockchain technology in my specified system. Upon researching many existing security and privacy preserving approaches, in the last section, I will put forward one that may be useful for managing sensitive data on the Blockchain before finishing with a conclusion.

II. System design using Blockchain

In an effort to flatten the curve of the COVID-19 infections, governments are exploring and beginning to adopt contact tracing measures to monitor the reach of exposure of infected people. Since these efforts require the collection of granular, private information about infected parties that must remain transparent and highly traceable, states and territories could implement Blockchain technology at various airports that serve as one of the key entry points for the virus. A practical benefit of doing this is that Blockchain could offer a solution to protect an individual's privacy while allowing the governments to observe their health status and take speedy actions as required.

One efficient way to execute this Pandemic Control Blockchain System would be for airports to have a 'health tunnel' just before the boarding gates that can carry out multiple checks, starting with the passenger's identity at the entry. As the passenger walks through, her public ID (or public key) is captured by live video cameras straight from her health card, followed by her personal identification details. In addition, health monitoring surveillance systems assess her body temperature and other symptoms (see details below). Lastly, her boarding pass is imaged by a scanner that collects her flight details. All of the information garnered is converted to a cryptographic hash that must be registered to individual blocks. The key details to be included would be:

- A unique public ID of each passenger
- Passenger's name and contact number
- Passport number
- Any COVID-19 symptoms they currently have, or have recently experienced – temperature range; shortness of breath; coughing
- Their flight details – flight number; seat
- Date of arrival; timestamp
- Current hash – hash of all the information above
- Previous hash – hash of the previous block (previous passenger's data)

The hash structure would follow the given format (MD5 hashing algorithm has been opted for this system):

HASH(Previous Hash | Public Id | Name | Contact | Passport | Temperature | Coughing | Shortness of breath | Flight | Seat | Date | Time)

Current Hash: 8b0000c4ebe8bd04a3b8f9c7fcd84b60 Previous Hash: Nil (since this is the 1st block)	
Public Id: 4478	Flight: M2494F
Name: Hannah Foster	Seat: 22A
Contact: 0123 456 789	
Passport: Y7654321	
Temperature (in C): 38	
Coughing: No	Date: 02/10/20
Shortness of breath: No	Time: 22:09

Figure 2. Basic architecture of a block containing details of Hannah Foster

HASH(4478 | Hannah Foster | 0123 456 789 | Y7654321 | 38 | No | No | M2494F | 22A | 02/10/20 | 22:09) = **8b0000c4ebe8bd04a3b8f9c7fcd84b60**

Current Hash: 8f87ea1c259e3ae75ce15d1f2f28ed4e Previous Hash: 8b0000c4ebe8bd04a3b8f9c7fcd84b60	
Public Id: 4479	Flight: M2494F
Name: Paul Foster	Seat: 22B
Contact: 0234 567 891	
Passport: Y8765432	
Temperature (in C): 38.7	
Coughing: Yes	Date: 2/10/20
Shortness of breath: No	Time: 22:11

Figure 3. Basic architecture of another block containing details of Paul Foster

HASH(8b0000c4ebe8bd04a3b8f9c7fcd84b60 | 4479 | Paul Foster | 0234 567 891 | Y8765432 | 38.7 | Yes | No | M2494F | 22B | 02/10/20 | 22:11) = **8f87ea1c259e3ae75ce15d1f2f28ed4e**

As shown in *Fig. 2*, the details obtained from a passenger named Hannah Foster are used to generate a block with a specific hash value, and the same process is carried out for the next passenger. Places where passengers' biometric data is used to identify them at airport touch points can also be included in place of their passport number. In this pattern, the authenticated and encrypted activity inside every block that gets generated is appended to the common Blockchain system.

III. Integrity and Traceability

The authorities that could potentially query this Pandemic Control Blockchain System can include regulators, government agencies, WHO, pharmaceutical manufacturers and a variety of research organizations funded by state governments. If any authority wants to scrutinize the Blockchain information coming from any particular airport, they can only access non-identifiable passenger details, such as symptoms and flight number, while only the passenger's themselves have complete ownership of their personal records. However, they can indeed allow the authority access to this data if they wish, using their private key. But the underlying fact that absolutely no organization can touch their private details because of the Blockchain's architecture, wherein each subsequent block contains the hash value from the previous block, helps preserve the integrity of the network.

Moreover, for the purposes of monitoring the health status of people flying in on a commonly basis, the state government agency can submit queries to the Blockchain and track down some specific data of every traveller that entered their territory. What they can examine are the symptoms of passengers, and if they have high temperature, shortness of breath, or any other indicators or signs of coronavirus, then the agency can investigate further by obtaining the flight details of those passengers. Due to the highly traceable nature of the Blockchain network, authorities can reach out and find the true and consistent information that they need by simply accessing the public data available on each block. After they have the flight details, airport customs can be contacted and asked for details of all passengers who travelled in that flight, so that others can be warned or in some cases asked to self-quarantine as deemed necessary by the government.

In these ways, the passenger's identity as well as data liquidity and immutability is maintained in the Pandemic Control Blockchain System.

IV. Benefits and Drawbacks

A. Advantages

In addition to the properties of Blockchain technology discussed in the previous section, there are a few more advantages to it:

a) Blockchain's "privacy by design" property ensures that every piece of passengers' information on the block is completely trustworthy and true. The design also stores all of the hash values in the most secure, encrypted and tamper-proof manner such as it stays unalterable, which effectively serves as an ideal feature fulfilling the requirement to prevent censorship of any kind.

b) Data immutability – “Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of passenger records.”

c) This Blockchain-based system architecture enables participants to own, control and share their private information upon will without relying on any foreign authority or having to violate their privacy.

d) In some unprecedented cases such as spontaneous flight delays, differences can arise between passenger apps, airport flight information displays, and airline agents. The Blockchain implementation described above provides a cryptographically immutable transaction ledger, a complete copy of which is distributed to all the interested authorities and can help prevent such scenarios and avoid confusions.

B. *Disadvantages*

As is the case with any technology, there are several limitations to this Blockchain system:

a) With many government authorities trying to analyse data from the inflow of poulation in their respective states all at the same time, the processing of the Blockchain system is subject to slowing down. Interpreting digital information swiftly is important as time is critical in the growing risk of this pandemic, thus network congestion would not be helpful.

b) When a commerial system grows too large on data, it can result in major inefficienties. As whenever new data is appended, nodes need to replicate it, as a result the ledger has been found to cross 100’s of GBs quite easily.

c) Data immutability might be a plus, but it also is a negative. If someone’s contact number gets updated a week after it being recorded, it would be very difficult to change on the database. But this leads to another major drawback, which is that the blockchain network could be *controlled* by an entity if he owns 50% or more of the nodes – given the data immutatbility – making the private details of passengers extremely vulnerable.

d) When the coronavirus gets wiped out completely in the next few years, this gigantic blockchain network would not be of critical importance anymore due to which it might just become nothing but a large cumbersome database.

V. Other Privacy Preserving Models

Instead of having to send a passenger’s personal data over to any one organization or government authority, this data gets sent over to the common Blockchain network. However, we can send this sensitive data in a different, more encrypted form, using sophisticated privacy preserving applications, in order to make certain that the visibility of such information is as minimised as practically possible. One of the many such existing emerging applications that hold the potential to increased security over one’s sensitive data is discussed below:

A. *Biometric matching*

In the future, Biometrics such as fingerprint, iris or face recognition are likely to be used extensively for identity management. The traditional biometric matching system stored a massive database of fingerprint or iris templates, wherein a person’s distinct fingerprint pattern had to be extracted from the fingerprint image, which then had to match the copy in the database. In contradiction, modern biometric recognition technology is logically more tamper-proof and reliable, with a simple difference in the way it stores information using encryption.

A Blockchain-based biometric recognition system would serve the function of delivering some form of identity document (ID) that could uniquely identify a citizen to the database of the government registry office via Blockchain. Considering the vulnerabilities and security threats that national ID systems have, particularly when making transactions, there is a clear gap for the implementation of ICT technologies to track and validate transactions. Certainly, the blockchain network combined with the authentication and user identification processes could be applied to overcome the aforementioned problems. Due to the current advance of technology, a novel concept of Electronic Identity Document (e-ID) has appeared, which mainly consists of generating the same ID in a smart card where the data of the carrier can be stored digitally including new features such as facial and fingerprint information for recognition. In addition, it includes more complex security measures by means of encryption of personal information, that when uploaded to the Blockchain network would intensify the robustness of the database.

As an example of the implementation, the citizen which owns its own electronic ID (inside which fingerprint and iris template are stored) generates a security certificate through a match on card (MoC) system. MoC system allows local verification of the templates stored on the card, these are read by a standard 32K Near Field Communication (NFC) storage chip and governed by the common criteria Evaluation Assurance Level (EAL) 5, allowing the authentication of the user against the national government through generic software. During the operation, the transaction is protected by the media on the card and by the encryption offered by the Blockchain. All nodes are aware of the existence of the transaction but only the receiver knows the content.

Usually, software used to validate the user identity leaves gaps in security such as possible phishing of identity through NFC failures and the possible acceptance of a fingerprint that does not coincide. In order to tackle the user’s impersonation threat, a double biometric user validation system together with public and private keys encrypted in the security certificate through NFC could be utilized. Also, extra security is guaranteed when transactions are stored by means of the Blockchain technology in a distributed system that ensures traceability, security, and scalability.

VI. Conclusion

This paper contains an introduction to the basic architecture of the widespread Blockchain technology whose uses are being investigated within many sectors. A better part of this report focuses on a simple system design that could be applied at international airports, and which flows upon the benefits presented by Blockchain and aims to mitigate the risks of coronavirus infections, while also critically evaluating its advantages and flaws. Additionally, how the system offers robust integrity and traceability of information that has crucial importance is also explained based on thorough research from a large number of papers. On a final note, key considerations need to be made around how this technology can be thoughtfully integrated into an organization’s existing infrastructure, and organizations should consider a use-case driven approach to assessing the fit of a blockchain-enabled solution for their existing business and clinical needs.

REFERENCES

[1] En.wikipedia.org. 2020. *Blockchain*. [online] Available at: <https://en.wikipedia.org/wiki/Blockchain#Financial_services> [Accessed 3 October 2020].

[2] Reuters. 2020. *Blockchain Explained*. [online] Available at: <http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html#:~:text=A%20Blockchain%20is%20a%20database,is%20very%20difficult%20to%20change.&text=The%20records%20that%20the%20network,previous%20block%20in%20the%20chain.> [Accessed 3 October 2020].

[3] 2020. [online] Available at: <https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/Blockchain-explained.html> [Accessed 3 October 2020].

[4] Centerforhealthsecurity.org. 2020. [online] Available at: <https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf> [Accessed 3 October 2020].

[5] Abc.net.au. 2020. *Fever Is A Symptom Of Coronavirus, So Here's What You Need To Know About It*. [online] Available at: <https://www.abc.net.au/news/health/2020-04-26/fever-coronavirus-symptom-explainer/12178756> [Accessed 3 October 2020].

[6] Md5hashgenerator.com. 2020. *MD5 Hash Generator*. [online] Available at: <https://www.md5hashgenerator.com/> [Accessed 3 October 2020].

[7] HIMSS. 2020. *Blockchain And The COVID-19 Pandemic: How Evolving Societal Need Accelerates Emerging Technologies | HIMSS*. [online] Available at: <https://www.himss.org/news/blockchain-coronavirus-emerging-technologies> [Accessed 3 October 2020].

[8] Future Travel Experience. 2020. *Can Blockchain Technology Enable The Single Passenger Token?*. [online] Available at: <https://www.futuretravelexperience.com/2016/06/can-blockchain-technology-enable-the-single-passenger-token/> [Accessed 3 October 2020].

[9] Ey.com. 2020. *How Blockchain Could Introduce Real-Time Auditing*. [online] Available at: <https://www.ey.com/en_gl/assurance/how-blockchain-could-introduce-real-time-auditing> [Accessed 3 October 2020].

[10] Airport-technology.com. 2020. *Blockchain: The Future Of Flight Data Management?*. [online] Available at: <https://www.airport-technology.com/features/blockchain-future-flight-data-management/> [Accessed 3 October 2020].

[11] Harvard Business Review. 2020. *The Truth About Blockchain*. [online] Available at: <https://hbr.org/2017/01/the-truth-about-blockchain> [Accessed 3 October 2020].

[12] Ieeexplore.ieee.org. 2020. *An Overview Of Blockchain Technology: Architecture, Consensus, And Future Trends - IEEE Conference Publication*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/8029379> [Accessed 3 October 2020].

[13] Sun, J., Yan, J. and Zhang, K.Z.K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1).

[14] Casino, F., Dasaklis, T.K. and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, pp.55–81.

[15] Ghosh, J. (2019). The Blockchain: Opportunities for Research in Information Systems and Information Technology. *Journal of Global Information Technology Management*, 22(4), pp.235–242.

[16] europepmc.org. (n.d.). *Europe PMC*. [online] Available at: http://europepmc.org/article/MED/29016974 [Accessed 3 Oct. 2020].

[17] Xu, M., Chen, X. and Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, [online] 5(1). Available at: https://link.springer.com/article/10.1186/s40854-019-0147-z [Accessed 7 Jul. 2019].

[18] 101 Blockchains. (2020). *10 Disadvantages Of Blockchain Technology*. [online] Available at: https://101blockchains.com/disadvantages-of-blockchain/.

[19] Researchgate.net. (2020). [online] Available at: https://www.researchgate.net/profile/Akshay_Agarwal6/publication/334736201/figure/fig1/AS:785878846803968@1564379526320/The-transitivity-of-the-hash-function-involved-in-the-blockchain.png [Accessed 3 Oct. 2020].

[20] Veridium. (2018). *Blockchain & Biometrics: The Future of Identity*. [online] Available at: https://veridiumid.com/future-identity-blockchain-biometrics/ [Accessed 3 Oct. 2020].

[21] Delgado-Mohatar, O., Fierrez, J., Tolosana, R. and Vera-Rodriguez, R. (n.d.). *Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends*. [online] Available at: https://arxiv.org/pdf/2003.09262.pdf [Accessed 3 Oct. 2020].

[22] Páez, R., Pérez, M., Ramírez, G., Montes, J. and Bouvarel, L. (2020). An Architecture for Biometric Electronic Identification Document System Based on Blockchain †. *Future Internet*, 12(1), p.10.

[23] Infosys.com. 2020. [online] Available at: <https://www.infosys.com/industries/travel-hospitality/documents/safe-travel-new-normal.pdf> [Accessed 3 October 2020].