COVID-19 and future pandemics: A blockchain-based privacy-aware secure borderless travel solution from electronic health records

Justice Odoom¹ | Xiaofang Huang¹ | Samuel Akwasi Danso²

¹Department of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, Sichuan, China
²Department of Computer Science, Ghana Communication Technology University, Accra, Ghana

Correspondence
Justice Odoom, Department of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, Sichuan 621010, China.
Email: odoom.justice@ieee.org

Funding information
National Natural Science Foundation of China (Youth); Image Source Forensics Security Research, Grant/Award Number: 61702429; Sichuan Provincial Department of Science and Technology, A trusted basic service platform for universities based on independent and controllable blockchain technology, Grant/Award Number: 2021YFG0311

Abstract
COVID-19 pandemic undoubtedly lingers on and has brought unprecedented changes globally including travel arrangements. Blockchain-based solutions have been proposed to aid travel amid the pandemic. Presently, extant solutions are country or regional-based, downplay privacy, non-responsive, often impractical, and come with blockchain-related complexities presenting technological hurdle for travelers. We therefore propose a solution namely, Borderless to foster global travel allowing travelers and countries collaboratively engage in a secure adaptive proof protocol dubbed Proof-of-COVID-19 status a number of arbitrary statements to ascertain the fact that the traveler poses no danger irrespective of the country located. As far as we know, this is first of its kind. Borderless is implemented as a decentralized application leveraging blockchain as a trust anchor and decentralized storage technology. Security analysis and evaluation are performed proving security, privacy-preservation, and cost-effectiveness along with implementation envisioning it as a blueprint to facilitate cross-border travel during the present and future pandemics. Our experimental results show it takes less than 60 and 3 s to onboard users and perform proof verification respectively attesting to real usability scenarios along with the traits of arbitrary proofs to aid responsiveness to the dynamics of pandemics and blockchain abstraction from travelers.

KEYWORDS
blockchain, coronavirus, decentralized application, electronic health records, smart contract, travel

1 | INTRODUCTION

Coronavirus (COVID-19) pandemic has radically disrupted global norms and has brought unimaginable hardship globally with efforts still underway to effectively control it and its variants and possibly eradicate it. Presently, the World Health Organization (WHO) puts the number of confirmed cases at 445,096,612 with almost 6 million fatalities. In the last 24 h, there has been over 1,200,707 confirmed cases globally. Meanwhile, a total of 10,704,043,684 vaccine doses have been administered globally.¹

Abbreviations: EHR, electronic health records; EUDCC, EU Digital COVID certificate; PII, personable identifiable information; TC, testing centers.
The quest to contain and control the pandemic in the area of contact tracing, testing and vaccination, managing misinformation, medical and scientific cooperation, data aggregation and analysis, supply of needed essentials and so forth has witnessed a wide range of technologies deployed encompassing artificial intelligence and robots, 3D printing, blockchain technology as well as potential security and privacy risks in the use of IoT devices in combating the pandemic. Amid the containment and control protocols is travel restriction which is partly in force. In an attempt to facilitate travel amid the pandemic, a myriad of blockchain-backed solutions including movement passes, immunity certificates among others have been proposed. There also exist non-blockchain-based solutions like CommonPass, EU Digital COVID certificate (EUDCC), UK’s NHS COVID Pass, Africa’s Trusted Travel and so forth.

Carefully analyzing the extant solutions reveals the reliance on centralized databases under the administration of organizations with vested interests, inadequacies in user privacy protection mechanisms as unraveled by a recent study, no global solution allowing verifiability in any country to alleviate the need for re-testing upon arrival as virtually all extant solutions are private blockchain-based for specified jurisdictions, impractical assumptions requiring travelers to deploy and manage smart contracts (SCs), inherent blockchain-related complexities that potentially would be overwhelming for travelers, and no provision for an update mechanism when pertinent data of travelers/patients are stored on blockchain-an indispensable feature since test/vaccination status from traveler’s electronic health records (EHR) is dynamic. With healthcare being the industry with the highest number of internal bad actors and almost half of healthcare breaches emanating from within the same organization, centralized databases and entrusting organizations with healthcare data raise security concerns including privacy breaches, data loss, and data integrity.

There is therefore the need to address the aforementioned challenges that have bedeviled extant works. Moreover, proving one’s COVID-19 status in a his/her country is trivial. However, same cannot be said when the user is in another country’s jurisdiction resulting in cost incurred from re-testing. The problem is further exacerbated given current variants (Delta, Omicron etc.) of the virus with evidence of the variants on the effectiveness of different vaccines preliminary and developing rapidly. The result is that, currently, territorial authority is asserted, trust scarce and details of COVID-19 test/vaccination proof vary vastly from airline to airline, state to state, country to country, and regional body to regional body which is a huge bottleneck to opening up and easing travel arrangements amid the pandemic as noted by some airlines hence calls for a global reconfigurable system. To this end, we present a responsive, borderless, secure, and privacy-preserving blockchain-based solution that guarantees global verifiability of COVID-19 test/vaccination credentials backed by decentralized storage technology while abstracting blockchain-related complexities from patients/travelers. We summarize our contribution to the body of knowledge as follows:

- A blockchain-based decentralized storage solution that allows for cross-border and in-country verification of COVID-19 updatable test and vaccination credential while abstracting blockchain-related complexities from travelers/patients without sacrificing high levels of security and privacy. We include in our solution a proof technique dubbed Proof-of-COVID-19 status based on the traveler’s EHR to prove any number of arbitrary statements regarding test and vaccination in response to the dynamic nature of this and future pandemics.
- Robust security analysis and system evaluation including performance and cost analysis of the proposed solution are performed to attest to system feasibility and reliability.
- We present the efficiency and feasibility of our solution by developing a decentralized application (dApp) and make it globally available as part of our commitment to the principle of open source application development.
- Provision of benchmark comparison with existing blockchain-backed solutions to assert the uniqueness of our solution.

1.1 Organization

The remainder of this article is organized as follows: Section 2 presents a thorough review of extant works. Section 3 expound the solution advanced in this work followed by Section 4 with implementation details and testing of our solution including compelling algorithms. We perform comprehensive system evaluation in Section 5 including security analysis and feature comparison. Section 6 presents concluding remarks and our ongoing efforts.
Blockchain technology has been one of the core technologies touted and utilized in the fight against COVID-19 in different aspects like contact tracing, financial aid, misinformation management, personal protective equipment (PPE) supply and vaccine delivery, medical collaboration, and immunity certificate also known as vaccine passport or COVID passports as verifiable credentials. Reference 7 also expounded on the use of IoT in fighting COVID-19 and future pandemics mindful of privacy and security by way of comprehensive survey in which key requirements encompassed such guarantees as unforgeability, patient anonymity, data integrity, patient identity privacy among others. The use of blockchain together with IoT devices like drones as well as 5G and artificial intelligence in the fight against the pandemic has also been put forward. Similarly, Reference 38 leveraged blockchain technology for multi-robot collaboration management in a decentralized manner to monitor quarantine areas, perform deliveries among others to reduce human interaction during the pandemic. Reference 39 narrows done on blockchain technology and posits a number of ways including high-level view of how the technology can be leveraged amid the pandemic. A similar approach is also presented in Reference 40 with focus on how blockchain can help resolve development challenges during the pandemic. Given that thorough evaluation of such blockchain-powered solutions are vital, Reference 41 sheds light on performance evaluation of IoT solutions that have blockchain as their underlying technology. For conciseness, following, we focus on works relating to verifiable credentials particularly based on blockchain pertaining to COVID-19 testing and vaccination.

The work of Reference 10 proposed immunity certificates and further discusses the challenge of falsification of information. The proposed private blockchain-based idea however falls short of details like design scheme and lacks practical implementation hence not sure of its real-life feasibility. Closely related to Reference 10 is Reference 8 in which movement passes are issued to users placing a restriction on the number of people allowed to gather at a specified location. Self-testing is also proposed in Reference 11 where users upload their test results onto a centralized database/server. A commercial antibody solution stores details of persons tested directly on a consortium blockchain. Such an approach not only breaches privacy of users but in direct contradiction to healthcare guidelines. We take a different approach in our solution by employing encryption and subsequent storage of encrypted data off-chain with the blockchain storing only hashed data. We elucidate on this in subsequent sections. Test and vaccination certification is advanced in Reference 9 relying on a private blockchain in which as part of the user onboarding process, the user is required to upload a personable identifiable information (PII) document like passport, driving license and so forth with no solid guarantee of user privacy. Moreover, this like the other solutions rely on private blockchain that are not as secured as public or permissionless blockchain.

Digital medical passports are also presented in Reference 19 relying on the Ethereum blockchain. In the solution, a designated ministry (Ministry of Foreign Affairs) in a country registers Ministry of Health (MoH) in another country to ensure recognition of verifiable credentials among the two countries. At the same time each user or patient has a separate SC and the patient is responsible for on (requires cryptocurrency) and off-chain data storage. Moreover, user SC holds PII like name coupled with public information dissemination to users via the SC. Again, the deployment of SC by patient implies mandatory know-how and ownership of blockchain address and cryptocurrency-a big technological bottleneck and hurdle for patients/travelers thereby raising some doubts about feasibility.

Noteworthy is the fact that there exist other propositions based on private blockchain for specified jurisdictions. Recall there exist non-blockchain-based solutions. However, all such solutions are characterized by: use of centralized databases under an organization’s or state’s control or country/regional-based (UK, US, Australia, China, Israel, France, Africa, EU etc.). Inasmuch as each country and regional body has the duty to forestall the spread of a pandemic into her bodies, we opine that such effort is best strengthened with global coordination-a fact noted by some airlines. After all, COVID-19 is a pandemic not just an outbreak or an endemic limited to a state or region. In Table 1, we present a summary of existing works, their drawbacks and how our solution differs from extant solutions towards resolving deficiencies in such solutions.

It is obvious that existing blockchain and non-blockchain-based solutions alike lack global perspective of the pandemic given their country-specific approaches, have downplayed privacy-an effort backed by some researchers that it is justified to momentarily weaken privacy for public good amid the pandemic. Moreover, most existing works rely on centralized databases and servers for functionality with annihilating consequences in terms of data security, and they all do not provide any update mechanism of on-chain data. Towards resolving these, we propose a blockchain and decentralized storage solution with global verification in mind integrated with secure privacy-preserving techniques mindful of the fact that PII and personal data if not safe guarded can be repurposed in unimaginable ways. While our approach is...
| Reference | Purpose | Some drawbacks | Our solution |
|-----------|---------|----------------|--------------|
| 10        | Immunity certificates | • Lacks design details and implementation | • Full design and implementation |
|           |                     | • Usable within one country | • Global usage |
| 8         | Regulating movements | Country-specific | Easing movement with global perspective |
| 11        | COVID-19 testing | Use of centralized database | Decentralized storage architecture |
|           |                     | Tests administered by users | Tests administered by approved health facilities |
| 19        | COVID-19 medical passports | Blockchain and storage-related complexities for traveler | Abstraction of blockchain and off-chain storage complexities from travelers |
|           |                     | Personally identifiable information (PII) disclosed in smart contract | No PII stored on-chain |
|           |                     | Requires bilateral agreements | A global solution |
| 8-13,15,17,18 | COVID-19 tests and vaccination certificates | Applicable to permissioned blockchain | Use of permissionless blockchain |
|           |                     | Country-specific and test/vaccination data lacks update functionality | Global use and test/vaccination data are updatable |
|           |                     | Proof not responsive to viral mutations. | Proof responsive to dynamic pandemic situations |
| 14,17,21,45 | COVID-19 medical passports | Use of private blockchain | Use of public blockchain |
|           |                     | Country-specific | Global use hence borderless verification |
|           |                     | Proof not responsive to viral mutations. | Proof responsive to viral mutations. |

similar to the use of multiple SCs in Reference 19, our solution provides global verification between countries without the need for any prior bilateral relationship. In addition, we incorporate test/vaccination status update ingrained with privacy-preservation. Finally, we make our solution flexible and adaptable to the dynamic nature of pandemics while abstracting blockchain and cryptocurrency-related complexities from patients/travelers unlike extant solutions. These novel features set our solution apart from current works. We explicate on our proposed solution in subsequent sections.

# 3 | PROPOSED SOLUTION

This section presents the building blocks based on which the proposed solution is developed as well as vivid details on how the building blocks are leveraged in our solution dubbed Borderless.

## 3.1 | Building blocks

We briefly provide the underlying infrastructure upon which our solution relies.

### 3.1.1 | Blockchain

This is a peer-to-peer cryptographic-based distributed system of nodes working via an agreed upon consensus mechanism through which transactions are validated, stacked into blocks and linked to previously generated blocks in a secured,
transparent, and tamper resistant fashion to create a decentralized verifiable ledger. It can be public/permissionless (where any node can join the network and data as well as storage are globally visible) as in Bitcoin\cite{47} and Ethereum,\cite{48} private (where nodes are vetted and approved before they join the network) or consortium-based (a form of private blockchain usable within a group of organizations) like Hyperledger Fabric.\cite{49}

3.1.2 Smart contract

The Ethereum blockchain unlike Bitcoin provides a stateful Turing-complete virtual machine known as Ethereum virtual machine (EVM) paving way for blockchain programmers to create SCs that are deployed on the blockchain.\cite{50} SCs are the executable logic written in a defined programming language and run by specific virtual machines (VMs). They are deterministic (execute according to specified logic when specific conditions are met) and define a protocol of interaction between different entities with verifiability guaranteed.\cite{51} These among others make SCs ideal to automate business processes by executing according to specification once triggered thereby creating a trusted environment for hitherto untrusting parties.\cite{52}

SCs act as the backend for dApps. Note that DApps are applications that communicate with SCs hence benefits from the immutability, transparency, decentralization, and fault-tolerance or resilience that are characteristic of blockchain technology.

3.1.3 Decentralized storage technology

This is a decentralized peer-to-peer hub allowing users to store and retrieve data. Among this technology are InterPlanetary File System (IPFS),\cite{53} Storj,\cite{54} Chainsplitter,\cite{55} and Sia.\cite{56} We however utilize IPFS providing a content-addressable file storage architecture that returns a cryptographic hash (unique fingerprint) of the stored file or object. Moreover, it is a well developed and maintained framework aside its popularity in the researcher and developer communities.

3.2 System model

Figure 1 presents the high level architecture we devised to resolve the current challenges with existing solutions. It comprises of the following entities:

- **WHO:** The World Health Organization (WHO) is the global body that oversees health-related matters and is the entity that deploys the global SC. Thereafter, WHO manages the SC by way of registering countries as and when they meet approved global guidelines regarding testing and vaccination. By virtue of being the SC deployer, WHO is capable of deactivating a country on the basis of non-compliance.
- **Country:** This is any country registered by WHO upon meeting specified global testing/vaccination guidelines to enable global credential verification of her citizens. Each country is in charge of deploying and managing her SC to regulate the activities of testing centers (TCs) in her jurisdiction.
- **Testing center (TC):** This is any hospital, clinic, medical, or testing/vaccination facility a country has approved based on WHO's guidelines to perform COVID-19 testing and/or vaccination.
- **User/traveler/patient:** This denotes any person or prospective traveler who goes to a TC for COVID-19 testing and/or vaccination. Hereinafter, we refer to this entity as **Patient**.
- **Smart contract (SC):** This holds the programmable logic deployed on the blockchain as immutable code. We use two SCs in our solution: WHO and country SCs as aforementioned. Each SC is equipped with functions to execute specific tasks together with function modifiers to enforce authentication and authorization functionalities. Moreover we use the SC keyword **require** to enforce specific requirements.
- **Decentralized storage:** We utilize IPFS as an off-chain storage hub to store data relating to patients and countries. We expatiate more on this in subsequent sections.
- **Verifying institution:** This is any airport requiring proof of negative COVID-19 test and/or vaccination before boarding any airline.
We proceed on the assumptions that:

- WHO is a semi-trusted entity to regulate global health matters hence empowered to deploy an SC on a blockchain to manage pandemic-related issues. Note however that this level of trust does not in any way imply reliance on WHO for authenticity of COVID-19 health credentials or proof. Each country independently provides a set of assertions governing COVID-19-test/vaccination requirements during test/vaccination claim verification. Although WHO deploys the global SC, certain tasks can only be executed by countries (see Section 3.4.1).
- Each country has a designated ministry (for instance, MoH) that has a working relationship with WHO and has a blockchain address. It is this entity that deploys the SC to govern country-specific health-related issues.
- Every registered TC in each country has a blockchain address known to MoH in that country.

Note that to eliminate the limited level of trust in WHO, other techniques like secure multi-party computation (SMPC) and local differential privacy could be leveraged. However, these require randomness which is not fully available and secure in SCs without reliance on trusted entities or blockchain oracles as well as game-theoretic approaches. Moreover, differential privacy techniques often come with error margins that are unacceptable in health information exchange (HIE).

### 3.3 Threat model

In our scheme, Persons are semi-trusted and rational (same assumption adopted in Reference 62). Consequently, they are honest yet would deviate from the proposed scheme if they stand to benefit. Specifically Persons may:

1. Attempt to present old COVID-19 credentials ostensibly to pass verification.
2. Create multiple identities within the system.

Noteworthy is the fact that some malicious opponents (WHO inclusive) may attempt to intercept or modify the data stored on IPFS or even decrypt it. Others may also attempt to impersonate a Person/Traveler or a TC.
3.4 | Design intuition and methods

We design Borderless based on the fact that pandemics are best resolved with a global effort and stratification of roles. Blockchain is best suited for this in that it is an immutable ledger with global visibility providing a transparent irrefutable data, guarantees highly ideal in tackling pandemics and related information granted only authorized entities can write data to it. Towards this end, we employ a public blockchain on which a global SC is deployed by WHO to manage countries whereas each country also deploys a separate SC to regulate TCs within her jurisdiction. We opt for public blockchain in that unlike private blockchain, it is certainly a better alternative as each node strengthens the blockchain’s scalability and more especially security and reliability granted privacy-preserving techniques are integrated.

Throughout this article, we use the notations presented in Table 2. Following, we give a brief overview of core blockchain structure and protocols that underpin our solution.

3.4.1 | WHO smart contract

This global SC deployed by WHO serves to provide a unified on-chain data pertaining to countries. Using specific functions in the SC, WHO performs such tasks as register (see Algorithm 1), deactivate and reactivate a country based on set global health requirements. Note that SCs can resolve possible disputes. Inherent in this SC is a function allowing registered countries to update the link to their respective TC document (see Section 3.4.3 for details of this document) on IPFS in the event of a newly approved TC by the country. Note that the link to the TC document can only be updated by the country that owns it. The SC allows for global verification of COVID-19 claims (test and vaccination status) by any country during patient verification using the TC document aside the capability to transparently track global statistics. We refer the reader to Figure 2A for the structure of the blockchain based on this SC.

| Table 2 | Symbols and cryptographic notations |
|-------|------------------------------------|
| Notation | Meaning |
| Addr\textsubscript{WHO} | Blockchain address of WHO |
| Addr\textsubscript{Ctry} | Blockchain address of Country |
| Addr\textsubscript{TC} | Blockchain address of testing center (TC) |
| sK\textsubscript{TC} | Private key of TC |
| Sign | Digital signature algorithm |
| \sigma_{TC} | Signature of TC |
| PcHR | COVID-19 health records of patient |
| Ts | Date/time of testing and/or vaccination |
| PHID | Hashed identifier of patient |
| statusT | Test status of patient |
| statusV | Vaccination status of patient |
| PCS | Proof of COVID-19 test and vaccination status |
| pK\textsubscript{p} | Public key of patient |
| sK\textsubscript{p} | Private key of patient |
| Enc | Public key encryption scheme |
| Dec | Public key decryption scheme |
| EPcHR | Encrypted PcHR |
| H | Cryptographic hash function |
| hEPcHR | Cryptographic hash of EPcHR |
Algorithm 1. Country registration

Require: nameCtry, AddrCtry, bcType, tcIPFShash, AddrSC
Ensure: bool
1: Require WHO == msg.sender
2: Country ← (nameCtry, AddrCtry, AddrSC, bcType, tcIPFShash)
3: if Country created then
4:     return True
5: else
6:     return False
7: end if

FIGURE 2  Data structure of the blockchain

3.4.2  |  Country smart contract

The SC deployed by each country solely manages TCs in that country and holds patient-specific data.
Notice that our approach allows every country to deploy this SC onto a blockchain of her choosing. The reader is referred to Figure 2B for the structure of the blockchain based on country-level SC.

3.4.3  |  Off-chain data storage

Geared towards preventing blockchain bloat and limiting cost incurred in storing a lot of data on-chain, the TC document of each country and patient-related data are stored off-chain on IPFS. The TC document of a country contains the blockchain addresses of all registered TCs in that country. Noteworthy is the fact that the TC document is stored as a key-value pair structured as:

\[
\begin{align*}
TC_1 & : \ 0xA179a,... \\
TC_2 & : \ 0x5C579,... \\
& \vdots \\
TC_n & : \ 0x6c3251...
\end{align*}
\]
where the key $TC_n$ denotes the $n$th TC with a unique $Addr_{TC}$. It is the responsibility of countries to keep this document up to date as the success or failure of claim verification partly depends on it. We explicate on this at the verification section. However, it is worth pointing out that countries can leverage Interplanetary Name System (IPNS) as part of IPFS so updates on the TC file would still point to the same IPFS hash thereby avoiding recurrent cost in blockchain-based transactions.

Similarly, patient data is stored as key-value pair structured as:

\[
\begin{align*}
Ts &: 1628574844, \\
PCS &: 0x{ec}34cd..., \\
\sigma_{TC} &: 0xd1c7fe..., \\
EPcHR &: f3y87?h45stuZ...
\end{align*}
\]

where the keys denote their meanings as per Table 2.

### 3.4.4 COVID-19 test and vaccination proof generation

TCs during COVID-19 testing and/vaccination create proof which forms an integral part during verification. Using status$T$, status$V$, $Ts$, PHID, and $Addr_{Ctry}$, we create a Merkle tree to derive the Merkle root as Proof-of-COVID-19 status. We simply denote this as PCS. Notice that this approach of computing PCS makes our solution generic and flexible capable of being applied to vaccine-specific types or even vaccine jabs/doses if need be. It is therefore not difficult to realize that our idea of Proof-of-COVID-19 is versatile and highly efficient allowing us not only to store just 32-bytes of data on chain but also paves way for any number of arbitrary proofs to be made as the virus mutates without the need to modify and redeploy SCs to manage future pandemics. However, for brevity we adopt status$V$ as either vaccinated or not vaccinated given that one-shot vaccines presently exist.

### 3.4.5 Patient enrollment

We envision patients upon arrival at a TC undergoing ID verification before being enrolled. This ID can be from any legally binding document. Candidate examples include passport number, drivers license number and so forth. Given that our point of interest is on global travel, we opt for passport number as an ID.

After undergoing COVID-19 testing and/or vaccination, the COVID-19 health record of patient (PcHR) as part of the EHR may encompass a variety of data like resting heart rate, body temperature, blood oxygen and pressure as well as test/vaccination status among others. However, for brevity, we assume the ID, status$T$ (positive or negative), status$V$ (vaccinated or not-vaccinated) and $Ts$ as constituents of PcHR generated by TC after which PCS is then generated. It is worth pointing out at this stage that the patient/traveler is required to undergo the procedure herein described mindful of his/her travel arrangements given that test validity based on the EHR is time bound (48 h is widely used). We refer the reader to Algorithm 2 for further details on patient enrollment regarding digital signature creation, encryption as well as off and on-chain data storage.

Note however that we do not store the original/plain test or vaccination status of patients or any personally identifiable information (PII) on or off-chain as clearly demonstrated in Figure 2B, Sections 3.4.3 and 3.4.4 as well as Algorithm 2. We only store hash of ID as PHID and a hash of the IPFS hash as $hIPFSHash$ on-chain.

### 3.4.6 Patient data update

This is done when a patient’s test or vaccination status changes. A classical example is a patient testing positive and subsequently testing negative or a patient being vaccinated who hitherto was not vaccinated.

Blockchain is immutable, however, the design intuition in on-chain data update is the use of the patient’s PHID as a key to locate the patient’s data on the blockchain via the SC and modify the SC’s on-chain data to reflect the patient’s current PcHR. This is possible courtesy state changes supported by SCs.
Algorithm 2. Enroll patient

Require: ID, status\text{T}, status\text{V}, Ts, Addr\text{CTRY}

Ensure: bool

1: PcHR ← (Addr\text{p}, ID, status\text{T}, status\text{V}, Ts)  \Comment{Off-chain execution begins}
2: Hash ID: PHID ← H(ID)
3: TC creates PCS: PCS ← getMerkleRoot(status\text{T}, status\text{V}, Ts, PHID, Addr\text{CTRY})
4: EPcHR ← Enc(PcHR, pK\text{p})
5: hEPcHR ← H(EPcHR)
6: \sigma\text{TC} ← Sign(H(PCS‖hEPcHR), sK\text{TC})
7: Precompute IPFS hash: preIPFShash ← PreComIPFShash(Ts, PCS, \sigma\text{TC}, EPcHR)
8: Push data to IPFS: RH ← IPFS(Ts, PCS, \sigma\text{TC}, EPcHR)
9: Require preIPFShash == RH  \Comment{Off-chain execution ends}
10: Hash IPFS hash: hRH ← H(RH)  \Comment{On-chain execution begins here}
11: if msg.sender ∈ TCs then
12:    Check PHID does not exist: Require Patient.PHID == ""
13:    Patient ← (PHID, hRH)
14:    totalTested++
15:    emit patientRegistered event
16:    return True
17: else
18:    return False
19: end if  \Comment{On-chain execution ends}

Note that as with first time patients, the onus lies on patients (who have already been onboarded) to undergo this procedure mindful of their travel itinerary so verification of their COVID-19 credentials is based on their updated EHR as credentials outside the allowable time limit cannot pass verification. An update operation is performed by the TC as per Algorithm 3 encompassing data decryption and update operations. Note that the update occurs both on-chain (using PHID in the SC) and off-chain as evident in Figure 2B and Algorithm 3 after which a new IPFS hash is given to the patient.

Notice from Algorithm 3 that the claim (ID, RH) presented by the patient are rigorously checked off-chain and on-chain before update operation is executed.

3.4.7 Verification process

The design intuition behind verification is the fact that each country at the point of verification makes claims or assertions on test/vaccination status regarding the required standard in that country. For instance, \{Test status: Negative, Vaccination status: Vaccinated, Test status: Negative, Vaccination status: Not vaccinated\}. This and extended form like vaccine-specific assertions can be made by the country within which verification is being done. We then verify the veracity of patient-provided data (PHID, IPFS hash along with Addr\text{Ctry} if it is out-country) against the country-provided assertions. Essentially, we are recomputing PCS and together with data from both the blockchain and IPFS, checking for data integrity or attestation by a registered TC in that it is possible to recover address given signature and signed data (see Algorithm 4).

Borderless supports both in-country and out-country verification. Whereas the former depends on the country’s deployed SC and IPFS, the latter depends on WHO’s SC and IPFS as per Algorithm 4. Note that \sigma\text{TC} and the signed data by the TC are checked to ensure they actually yield a blockchain address that corresponds to a known address of a TC in a country’s TC document.

Notice from Algorithm 4 that verifiers only make calls to the SC not a transaction. In a blockchain call operation, no transaction is broadcasted hence no cryptocurrency is required.
Algorithm 3. Person status update

Require: ID, RH, tcIPFShash
Ensure: bool
1. Get Patient data from IPFS: data ← IPFS(RH)  \(\triangleright\) Off-chain execution begins
2. Data decryption: PcHR ← Dec(data, sK_p)
3. Check ID == PcHR.ID
4. Pull Country TC data from IPFS: tcFile ← IPFS(tcIPFShash)
5. Hash Enc. data: hEPcHR ← H(data.EPcHR)
6. signedData ← H(data.PCS‖hEPcHR)
7. Verify Signature: addrOfTC ← RecoverAddr(data.\(\sigma_{TC}\), signedData)
8. Require addrOfTC ∈ tcFile
9. Perform update: PcHR ← Update(PcHR)
10. Execute steps 2 to 10 of Algorithm 2  \(\triangleright\) Off-chain execution ends
11. Require msg.sender ∈ TCs  \(\triangleright\) On-chain execution begins
12. Get Patient details: Patient ← Patient.PHID
13. if Patient exist then
14. Require Patient.PHID == PHID
15. Perform update on-chain: Save(hRH)
16. totalRecordUpdate++
17. emit updatedPatient event
18. return True
19. else
20. return False  \(\triangleright\) On-chain execution ends

Algorithm 4. Out-country verification

Require: PHID, RH, Addr_coty, statusT, statusV
Ensure: bool
1. Get data: data ← IPFS(RH)  \(\triangleright\) Off-chain execution begins here
2. if data.\(T_s\) ≤ Time allowed ∨ \(\exists\) statusV==vaccinated then
3. Country claims: claims ← (statusT, statusV)
4. for \(i = 0\) to len(claims) do
5. PCS ← (ith claims, Ts, PHID, Addr_coty)
6. if PCS[i] == data.PCS then
7. proof = data.PCS
8. end if
9. end for
10. if proof ≠ null then
11. Get IPFS hash: tcIPFShash ← verificationTime(Addr_coty)  \(\triangleright\) On-chain execution
12. Get data: tcFile ← IPFS(tcIPFShash)
13. hEPcHR ← H(data.EPcHR)
14. sData ← H(data.PCS‖hEPcHR)
15. Verify Signature: addrOfTC ← RecoverAddr(data.\(\sigma_{TC}\), sData)
16. Require that addrOfTC ∈ tcFile
17. return True  \(\triangleright\) Off-chain execution ends
18. else
19. return False
20. end if
21. else
22. return False
23. end if
Table 3  Ethereum addresses of system entities

| Entity   | Ethereum address                  |
|----------|-----------------------------------|
| WHO      | 0x3c764142878ECF10FA712336CDE5Cc778878A294 |
| Country_A| 0xEC5bF0F1DE02E5FC8fEdE5ADEbe12bD4239535b7C |
| TC_1     | 0xA179a6f917D6cdC0cEA465DC20086ff1318394a5 |
| TC_2     | 0x5C57962333bA1B2BC91a067EFb41638234bd0a805 |

Table 4  Development environment and system configuration

| Component         | Description                  |
|-------------------|------------------------------|
| OS                | Windows 10 Build 18363       |
| CPU               | Intel(R)Pent.(R) G645 @2.90 GHz |
| RAM               | 8 GB                         |
| Eth. platform     | Ganache-cli v6.7.0           |
| SC compiler       | 0.8.4                        |
| Off-chain DB.     | IPFS                         |
| Programming       | Solidity & VueJs             |

4  IMPLEMENTATION AND TESTING

The proposed solution is designed as a dApp with the frontend implemented via Vue.js with two Ethereum-based SCs (acting as the backend logic) written with Solidity language, compiled in Remix IDE and deployed on a local instance of Ethereum blockchain known as Ganache. Ganache actually provides a personal blockchain (including automatic mining as part of the default settings thereby relieving developers of node, consensus, block and mining-related configurations) for development purposes only. We utilize Metamask for dApp wallet functionality. Under the hood of the interaction between the dApp and the blockchain is Web3 as the main JavaScript library for connecting to and interacting with the blockchain and SCs.

Ethereum is used due to its turing completeness, permissionless nature, flexibility, support and popularity within the researcher and developer communities. Committed to the principle of open source application, we make our solution globally available on GitHub as a platform to foster future development.

4.1  System testing

We approach system testing based on entities with Ethereum address as evident in Table 3.

We proceed with the testing scenario that a patient visits TC_1 for testing and possible vaccination and at a later date visits TC_2 for a re-test resulting in an update operation. We assume both TCs are in Country_A.

The exact configurations of our testing environment are presented in Table 4.

4.2  Smart contract deployment

Two SCs are deployed: One by WHO and another by Country_A as shown in Figures 3 and 4 respectively.

https://github.com/JustNETOrgani/borderlessSolnForPandemic
4.3 Country and TC registrations

In Figure 5, WHO registers Country_A whereas Country_A in turn registers TC_1 and TC_2. For brevity, we show in Figure 6 blockchain logs for that of TC_1. The existence of Country_A and the subsequent registration of TCs presupposes that Country_A has a TC document uploaded to IPFS (see Section 3.4.3).
Figure 5  Registration of Country_A by WHO

Figure 6  Registration of TC_1 by Country_A
4.4  Enrolling a patient

TC_1 after testing patient for COVID-19 enrolls her as previously described. See Figure 7 as an attestation to the success of this process where the patient tests positive for COVID-19 hence is not vaccinated.

4.5  Updating patient data

An update operation is performed by TC_2 at a later time when patient visits for re-testing. The patient now tests negative and is subsequently vaccinated (see Figure 8). As part of the update process, a new QR code (see Figure 9) in which the new IPFS hash and blockchain address of Country_A are embedded is given to the patient. Note that only this latest IPFS hash is now valid for successful verification as patient’s records off-chain and on-chain data stored in the SC have been modified to reflect the current records.
4.6 Verification

We perform both in-country and out-country (for instance where a patient/traveler arrives at destination country’s airport) verification. However, for brevity we present results regarding out-country or global verification as seen in Figure 10. In Figure 11 we give credence to the fact that once an update operation is done, prior data like IPFS hash are invalidated. Consequently, any attempt to present old credentials for verification fails.

It is worth mentioning that although our focus is not on combating misinformation, incidentally, our solution makes it possible for authentic information regarding number of tests and updates to be known based on the state variables (see lines 14 and 16 of Algorithms 2 and 3 respectively) and shown in Figure 12. Consequently, using the addresses of every country’s SC known in WHO’s SC, it is therefore possible for WHO using the blockchain to provide transparent and irrefutable global data regarding the pandemic.
5 | SYSTEM EVALUATION

We perform evaluation based on specific metrics in subsequent sub-sections.

5.1 | Cost analysis and benchmark comparison

In Table 5, we show details pertaining to transaction-related costs with respect to WHO, CountryA, and Verifiers as they interact with key functions in the SC. We use the average gas price on December 28, 2021 which was 58.59 Gwei based on ETH gas station with percentage of acceptance by miners being over 70% guaranteeing expedited inclusion into the blockchain at current ETH/USD price.

Notice that cost is incurred only by WHO, countries and TCs not verifiers.

Following, we compare these costs with extant works based on findings pertaining to gas reported in Reference 21. For consistency, we maintain the aforementioned gas price of 58.59 Gwei and use issuance to denote the procedure of issuing COVID-19 certificates or passports.
TABLE 5 Gas cost on key features related to our solution.

| Caller     | SC-related task | Gas used   | Cost ($) |
|------------|-----------------|------------|----------|
| WHO        | SC deployment   | 2,260,622  | 417.37   |
| WHO        | Country registration | 219,260    | 40.47    |
| Country_A  | SC deployment   | 2,256,159  | 416.56   |
| Country_A  | TC registration | 74,126     | 13.67    |
| TC_1       | Enroll patient  | 48,276     | 8.91     |
| TC_2       | Update patient data | 24,128    | 4.45     |
| Verifiers  | Verification    | Free       |          |

TABLE 6 Comparison of gas cost with other solutions

| Solution | Feature     | Gas used   | Cost ($) |
|----------|-------------|------------|----------|
| 42       | Issuance    | 131,398    | 24.23    |
| 9        | Issuance    | 24,128     | 4.45     |
| 21       | Issuance    | 24,128     | 4.45     |
| Our solution | Issuance (first time) | 48,276    | 8.91     |
|          | Update      | 24,128     | 4.45     |

TABLE 7 Benchmark comparison of our solution to existing solutions

| Criteria                      | 9       | 11      | 8       | 10      | 13-15,17,18,21,45 | 19      | 42      | Ours |
|-------------------------------|---------|---------|---------|---------|--------------------|---------|---------|------|
| Public blockchain             | No      | No      | No      | No      | No                 | Yes     | No      | Yes  |
| Global support                | No      | No      | No      | No      | C2C                | C2C     | No      | Yes  |
| Arbitrary proofs              | No      | No      | No      | No      | No                 | No      | No      | Yes  |
| Blockchain abstraction        | No      | No      | No      | No      | No                 | No      | No      | Yes  |
| Data update support           | No      | No      | Partly  | No      | Partly             | Partly  | No      | Full |
| Privacy protection            | No      | Partly  | No      | Partly  | Partly             | Partly  | No      | Full |
| QR code support               | No      | No      | No      | No      | No                 | Yes     | Yes     | Yes  |
| Managing misinformation       | No      | No      | No      | No      | No                 | No      | No      | Yes  |
| Data storage architecture     | DB/cloud| DB      | DB      | DB      | DB/P2P             | P2P     | DB      | IPFS |
| Source of test data upload    | TC      | Users   | TC      | TC      | TC                 | TC      | TC      | TC   |
| Vaccination support           | Yes     | No      | No      | Yes     | Yes               | Yes     | Yes     | Yes  |
| Proof of implementation       | Yes     | No      | No      | No      | Yes               | Yes     | Yes     | Yes  |
| Security analysis             | No      | No      | No      | No      | Partly             | Yes     | No      | Yes  |

Notice from Table 6 that cost-wise, although Enroll Patient analogous to first time issuance is higher than some existing solutions, subsequent issuance shares same cost with extant solutions since only one hash value $hIPFS$ is stored (updated) on-chain.

In Table 7, we present feature benchmark comparison of our solution to existing blockchain-based solutions. We denote database, country-to-country or bilateral relationship, testing center and peer-to-peer network as DB, C2C, TC, and P2P respectively.

While our solution is similar to References 9,13-15,17-19,21,45,71,72, we reiterate the fact that they unlike our solution rely on a private blockchain composed of only few nodes and often dependent on hosting servers. Moreover, no update
feature is supported and they are primarily for in-country or allied countries only hence not truly global. For clarity, we refer the reader to our discourse at Section 3 and the concluding part of same on the uniqueness of our solution.

5.2 Performance analysis

We measure the performance of our solution in terms of communication and computational overhead as per the system configuration stated in Table 4.

5.2.1 Communication overhead

Notice that communication overhead is witnessed during the data upload and download to and from IPFS, transaction propagation onto the blockchain during patient enrollment and update phases as well as SC-related call operation at the verification phase.

It’s obvious from Figure 13A it takes TCs < 700 ms to store or retrieve data from IPFS. Meanwhile, as at December 28, 2021, Ethereum’s average block time was approximately 13.24 s. We therefore make the projection that the entire duration regarding enroll or update tasks would be ≤ 1 min. (including data entry and computations). In Figure 13B, we see it takes ≤ 3 s to perform verification of a patient’s test/vaccination status which unarguably is realistic.

Noteworthy is the fact that storing data on-chain also come with some overheads that results in latency. Given that extant works including do not make code base available in a public repository, we compute the overheads based on publicly available data (see Table 8) in the current Ethereum paper and the amount of data stored on-chain to determine the number of user certifications that can be done in each block (average block size being 111,811 Bytes) under Ethereum’s current block creation time of 15 s. This can easily be computed using Equation (1) where DataSize denotes the size of data to be stored on-chain.

![Graphs showing communication overhead](image)

**FIGURE 13** Time overhead (A) uploading and downloading data (B) at verification phase

| Variable          | Value (in gas units) |
|-------------------|----------------------|
| $G_{blockLimit}$  | 29,995,567           |
| $G_{transaction}$ | 21,000               |
| $G_{txdata nonzero}$ | 16                  |
| $G_{set}$         | 20,000               |

**TABLE 8** Ethereum values for computing overhead
Using Equation (1) and implementation details from extant works where $DataSize$ is 46 Bytes (IPFS hash), 32 Bytes (hash of certificate), and 32 Bytes (hash of IPFS hash) in References 21 and 9 and our solution respectively, we get the cardinality of persons that can be anchored on-chain per block to be 1379 for Reference 21 and 1393 for Reference 9 as well as our solution. Notice that for fairness, we do not include Reference 42 given that specifics on three on-chain data (tested individual, test kid ID and validity) stored are not explicitly indicated.

5.2.2 | Computational overhead

We measure the computational costs while enrolling patients, performing data update and claim verification. Consequently, we compute the computational costs (see Table 9) on TCs and Verifiers as they execute defined tasks which clearly points out that verification is actually not computationally intensive as it requires only hashing operations-tasks that can even be achieved on resource-constrained devices.

5.3 | Security analysis

Following, we present security analysis of our solution comprising vulnerability testing of the SCs governing the proposed solution and core security metrics.

5.3.1 | Vulnerability analysis

We employ Slither, a static analysis tool that runs a suite of vulnerability detectors for SCs. Given that the Solidity compiler Solc version 0.8.4 we used is fairly recent for Slither, we downgrade our two SCs to Solc version 0.5.7 for vulnerability testing purposes only. Notice in Figure 14 that our two SCs have no known vulnerabilities based on the 75 detectors used by Slither. It is only the compiler version solc 0.5.7 which is flagged as not ideal for deployment.

5.3.2 | Security proof and requirements

Following theoretical security evaluation as part of guidelines on formal security analysis specified in a recent paper, we prove the security of our solution via the following theorems and subsequently buttress them with security metrics.

| Table 9 | Computational costs |
|---|---|---|---|
| Entity | Enroll patient | Data update | Verify |
| TCs | $12H + Enc + Sign$ | $14H + Enc + Sign$ | - |
| Patient | - | Dec | - |
| Verifier | - | - | $\leq 11H$ |

$\text{slither}$

INFO:Detectors:
Pragma version0.5.7 [CountryLevel.sol#2] allows old versions
Solc-0.5.7 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Pragma version0.5.7 [Witness.sol#2] allows old versions
Solc-0.5.7 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Slither: Analyzed (2 contracts with 75 detectors), 4 result(s) found

FIGURE 14 | Results of SC vulnerability tests
**Theorem 1.** *The proposed system is secure against privacy breach.*

**Proof.** In the process of data transmission and storage on IPFS and the blockchain, no PII is disclosed. On and off-chain data are totally anonymous and unlinkable to real identity of Persons in the real world hence adversarial blockchain inferences cannot breach privacy of a *Person*. Identity-revealing and COVID-19-related information of a *Person* are encrypted before storage on IPFS. As a consequence, the real identity of a *Person* cannot be deduced from both on-chain and off-chain data even by WHO. The public key encryption ensures that only the patient (traveler) can decrypt the data.

**Theorem 2.** *Assume a Person attempts to present an old COVID-19 test or vaccination credential with the intent of passing verification. Such an attempt will not suffice.*

**Proof.** In our design, we include a timestamp in the data stored on IPFS. Once the data is received from IPFS, this timestamp is checked to ascertain its validity within a set time limit. Any modification of the timestamp in the data on IPFS would be detected as the resultant IPFS hash would not match the hash stored in the SC. Besides, such change in timestamp would result in a Merkle root hash or proof (PCS) different from the original PCS. Moreover, due to state changes in the SC, an old credential (presupposes that it has been updated) would no longer match on-chain data hence verification will fail.

**Theorem 3.** *Suppose that a Person attempts to create multiple blockchain identities for same or different COVID-19 records. This attempt will fail.*

**Proof.** Even though blockchain allows any person to create multiple identities, in our proposed solution, PHID is computed from the legal ID via a cryptographic hash function (SHA-256 in our case) hence the same legal ID will always yield the same PHID. Consequently, any attempt to create multiple identities would not suffice.

**Theorem 4.** *Assume an adversary attempts to intercept or modify data on route to or stored on IPFS. Such attempts would be detected and not suffice.*

**Proof.** Leveraging the multihash scheme, we precompute the IPFS hash of the packaged data to IPFS before pushing to IPFS. We compare the returned IPFS hash with the precomputed hash for equality thereby guaranteeing that the IPFS node is acting honestly in accordance with the IPFS protocol. Besides, leveraging the tamper-proof trait of the blockchain, any such change in the IPFS hash would be detected.

Following, we analyze our solution based on core security metrics. These act as countermeasures against the threat model we considered in this article which in fact aligns with some threat models expatiated in a recent paper.7

- Confidentiality and privacy: The original COVID-19 data of patients are encrypted hence it is only the patient that can successfully decrypt the encrypted data. On and off-chain, no PII is disclosed. Also, on-chain data neither point to the off-chain IPFS location (this delinks any association) nor give away the actual COVID-19 test or vaccination status of patients. Moreover, owing to encryption employed, the solution adheres to health regulations.
- Data integrity: Based on the returned hash from IPFS, it is computationally impossible to modify off-chain data to get the same digest. Moreover, it is computationally infeasible for any adversary to modify the on-chain data.
- Data availability and resistance to attacks: Our solution employs decentralized storage technology and public permissionless blockchain consequently making data readily available with zero downtime coupled with resilience to DoS and DDoS attacks.
- Authentication and authorization (AA): The SCs employ function modifiers to perform AA checks to verify the transaction initiator based on the Ethereum address before any transaction can succeed.
- MITM and replay attacks: MITM and replay attacks cannot suffice in blockchain technology due to the inherent safeguards: Private key needed to sign transaction and duplicate transaction are detected by miners and swiftly discarded. From the perspective of the off-chain storage, we thwart any MITM attack by first precomputing the data to be stored on IPFS based on multihash technology. When we push data to IPFS, we verify that the returned hash matches the precomputed hash to ascertain the fact the IPFS node that received it is acting honestly.
### Table 10 Evaluation on security properties

| Solution | Security guarantees | Other guarantees |
|----------|---------------------|------------------|
|         | Forgery | Binding | Uniqueness | Revocation | Key exposure | Arbitrary Proofs | Borderless |
| 9        | ✓       | ✓       | ✓          | ×          | ×            | ×                | ×          |
| 21       | ×       | ✓       | ✓          | ✓          | ✓            | ×                | ×          |
| 42       | ×       | ✓       | ✓          | ×          | ×            | ×                | ×          |
| 72       | ✓       | ×       | ✓          | ✓          | ×            | ×                | ×          |
| Our solution | ×       | ✓       | ✓          | ✓          | ×            | ✓                | ✓          |

- **Impersonation:** AA checks are performed by the SCs using function modifiers and the SC keyword `msg.sender`. Note that it is computationally impossible to impersonate another address since it is computed from Keccak256 cryptographic hash of the public key. Given the fact that the SCs store relevant addresses like address of WHO, each Country and TC, the SCs cannot be tricked. Also, it is impossible to impersonate a Patient not without knowledge of her ID and RH. This is akin to impersonating another person at an airport as in our case where the ID is the passport number.

- **Collusion resistance:** Even amid collusion among WHO, Countries, TCs and IPFS, a patient’s PcHR cannot be obtained not without the cooperation of the patient due to the public-key encryption employed.

We present other security properties of our solution compared with extant works in Table 10. For brevity, we refer the reader to Reference 21 on the security definitions of the security guarantees. Key exposure on the other hand has to do with the possibility of the private/secret key of the user (person) being known or compromised by other entities. The comparison is made possible given that these works show detailed specifications pertaining to their implementations. Notice from Table 10 that security guarantee-wise, our solution parallels existing schemes. Moreover, our solution accommodates arbitrary COVID-19-related proofs making it versatile and responsive to dynamics of pandemics while guaranteeing borderless verification unlike extant schemes. The risk of private key exposure during proof verification by verifiers is eliminated in our solution since computation is done on hashes unlike in Reference 21 where verifiers need to know the private key of the user to decrypt data.

### 5.4 Scalability and feasibility of our solution

The scalability of Borderless depends on the scalability of its blockchain network implemented. At the moment, Ethereum processes over 1 million transactions daily\(^77,78\) with further improvements scheduled\(^79\) coupled with over 2800 active nodes\(^80\) and counting attesting to its scalability.

It is also worth pointing out that our solution is still feasible with the coming of Ethereum 2.0. The existing EVM would be Shard 0 or one of the 64 shard chains of the Ethereum 2.0 system.\(^81\) Consequently, our solution would still be feasible even when Ethereum 2.0 is fully completed (projected to be in the year 2023).

### 6 CONCLUSION

This article presents for the very first time a borderless COVID-19 testing and vaccination status verification solution called Borderless that requires no prior bilateral cooperation between countries while abstracting blockchain-related complexities from travelers. Our solution allows travelers prove their COVID-19 test and vaccination status in a privacy-preserving and secured fashion based on a mechanism dubbed Proof-of-COVID-19 test and vaccination status irrespective of the country located by leveraging blockchain, smart contract (SC) and decentralized storage technology. Although the cost of certain transactions particularly SC deployments is high, countries can still benefit from Borderless even with their SC deployed on permissioned blockchain where no cryptocurrency is required to avert such costs. Our ongoing efforts consist of a myriad of tasks including: integrating AI as well as visualization features for data analytics to boost swift decision making by health professionals and development of a mobile application.
AUTHOR CONTRIBUTIONS

Justice Odoom: Conceptualization; methodology; software; writing - original draft; writing - review and editing. Xiao-fang Huang: Writing - review and editing; supervision; funding acquisition. Samuel Akwasi Danso: Methodology; writing - review and editing.

ACKNOWLEDGMENTS

This work was supported by National Natural Science Foundation of China (Youth), Image Source Forensics Security Research (Grant No. 61702429) and Sichuan Provincial Department of Science and Technology. A trusted basic service platform for universities based on independent and controllable blockchain technology (Grant No. 2021YFG0311).

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Justice Odoom https://orcid.org/0000-0003-2765-6977

REFERENCES

1. WHO. Coronavirus disease (COVID-19) dashboard; 2022. Accessed March 7, 2022. https://covid19.who.int/
2. He W, Zhang ZJ, Li W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. Int J Inf Manag. 2020;57:102287. doi: 10.1016/j.ijinfomgt.2020.102287
3. Abdel-Basset M, Chang V, Nabeeh NA. An intelligent framework using disruptive technologies for COVID-19 analysis. Technol Forecast Soc Change. 2020;163:120431. doi: 10.1016/j.techfore.2020.120431
4. Yang GZ, Nelson BJ, Murphy RR, et al. Combating COVID-19—The role of robotics in managing public health and infectious diseases; 2020. 10.1126/scirobotics.abb5589
5. Choong YYC, Tan HW, Patel DC, et al. The global rise of 3D printing during the COVID-19 pandemic. Nature Reviews Materials. 2020;5(9):637-639. doi:10.1038/s41578-020-00234-3
6. Fusco A, Dicuonzo G, Dell‘Atti V, Tatullo M. Blockchain in healthcare: insights on COVID-19. Int J Environ Res Public Health. 2020;17(19):7167. doi:10.3390/ijerph17197167
7. Ferrag MA, Shu L, Choo KKR. Fighting COVID-19 and future pandemics with the internet of things: security and privacy perspectives. IEEE/CAA J Automat Sin. 2021;8(9):1477-1499. doi:10.1109/JAS.2021.1004087
8. Garg C, Bansal A, Padappayil RP. COVID-19: prolonged social distancing implementation strategy using blockchain-based movement passes. J Med Syst. 2020;44(9):1-3. doi:10.1007/s10916-020-01628-0
9. Eisenstadt M, Ramachandran M, Chowdhury N, Third A, Domingue J. COVID-19 antibody test/vaccination certification: there’s an app for that. IEEE Open J Eng Med Biol. 2020;1:148-155. doi:10.1109/OJEMB.2020.2999214
10. Bansal A, Garg C, Padappayil RP. Optimizing the implementation of COVID-19 “immunity certificates” using blockchain. J Med Syst. 2020;44(9):1-2. doi:10.1007/s10916-020-01616-4
11. Mashamba-Thompson TP, Crayton ED. Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing; 2020. 10.3390/diagnostics10040198
12. Chaudhari S, Clear M, Bradish P, Tewari H. Framework for a DLT Based COVID-19 Passport. Springer International Publishing; 2021:108-123.
13. Alabdulkarim Y, Alameer A, Almukaynizi M, Almaslukh A. SPIN: a blockchain-based framework for sharing COVID-19 pandemic information across nations. Appl Sci. 2021;11(18). doi:10.3390/app11188767
14. Butler D, Hicks C, Bell J, Maple C, Crowcroft J. Differentially private health tokens for estimating COVID-19 risk. ArXiv 2020; abs/2006.14329.
15. HRJ L, Georgios K, Dimitris G, Tania M, Georgios K, Nai FI. Sharing pandemic vaccination certificates through blockchain: case study and performance evaluation. Wirel Commun Mob Comput. 2021;2021:1530-8669. doi:10.1155/2021/2427896
16. Odoom J, Soglo RS, Danso SA, Xiaofang H. A privacy-preserving Covid-19 updatable test result and vaccination provenance based on blockchain and smart contract; Vol. 1, 2019:1-6; IEEE.
17. Capece G, Bazzica P. Vpassport: a digital architecture to support social restart during the SARS-CoV-2 pandemic. Sustain For. 2021;13(7). doi:10.3390/su13073945
18. Haque AB, Naqvi B, Islam AKMN, Hyrynsalmi S. Towards a GDPR-compliant blockchain-based COVID vaccination passport. Appl Sci. 2021;11(13). doi:10.3390/app11136132
19. Hasan HR, Salah K, Jayaraman R, et al. Blockchain-based solution for COVID-19 digital medical passports and immunity certificates. IEEE Access. 2020;8:222093-222108.
20. Biswas S, Sharif K, Li F, Bairagi AK, Latif Z, Mohanty SP. GlobeChain: an interoperable blockchain for global sharing of healthcare data—a COVID-19 perspective. IEEE Consumer Electron Mag. 2021;10(5):64-69. doi:10.1109/MCE.2021.3074688

21. Abid A, Cheikhrouhou S, Kallel S, Jmaiel M. NovidChain: blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Softw Pract Exp. 2021;52:841-867. doi:10.1002/spe.2983

22. F. C. The commons project; 2021. Accessed July 12, 2021. https://thecommonsproject.org/commonpass

23. Euronews. The EU’s digital COVID certificate is now live; 2021. Accessed July 10, 2021. https://www.euronews.com/travel/2021/07/01/digital-covid-certificate-eu-wide-travel-pass-officially-comes-into-force

24. NHS. NHS COVID Pass; 2021. Accessed June 18, 2021. https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/

25. AfricanUnion A. Trusted travel; 2021. Accessed May 19, 2021. https://africacd.org/trusted-travel/

26. AfricanUnion A. Trusted travel; 2021. Accessed May 19, 2021. https://africacd.org/trusted-travel/

27. WHO. The effects of virus variants on COVID-19 vaccines; 2021. Accessed July 9, 2021. https://www.who.int/news-room/feature-stories/detail/the-effects-of-virus-variants-on-covid-19-vaccines

28. Karopoulos G, Hernandez-Ramos IL, Kouliiaridis V, Kambourakis G. A survey on digital certificates approaches for the COVID-19 pandemic. IEEE Access. 2021;9:138003-138025. doi:10.1109/ACCESS.2021.3117781

29. C. C. Blockchain in California: a roadmap; 2021. Accessed May 9, 2021. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf

30. Verizon. 2020 data breach investigations report; 2021. Accessed May 19, 2021. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

31. Nakamoto I, Wang S, Guo Y, Zhuang W. A QR code-based contact tracing framework for sustainable containment of COVID-19: evaluation of an approach to assist the return to normal activity. JMIR Mhealth Uhealth. 2020;8(9):e22321. doi:10.2196/22321

32. Idrees SM, Nowostawski M, Jameel R. Blockchain based digital contact tracing applications for pandemic management (COVID-19): issues, challenges, solutions and future directions. JMIR Med Inform. 2020;9. doi:10.2196/25245

33. Wu H, Zhu X. Developing a reliable service system of charity donation during the Covid-19 outbreak. IEEE Access. 2020;8:154848-154860. doi:10.1109/ACCESS.2020.3017654

34. Marbouh D, Abbasi T, Maasmi F, et al. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. Arab J Sci Eng. 2020;45:9895-9911. doi:10.1007/s13369-020-04950-4

35. Musamihi A, Jayaraman R, Salah K, Hasan HR, Yaoqib I, Al-Hammadi Y. Blockchain-based solution for distribution and delivery of COVID-19 vaccines. IEEE Access. 2021;9:71372-71387.

36. Rézière D, Resiere D, Kallel H. Implementation of medical and scientific cooperation in the caribbean using blockchain technology in coronavirus (Covid-19) pandemics. J Med Syst. 2020;44:123. doi:10.1007/s10916-020-01589-4

37. Chamola V, Hassija V, Gupta V, Guizani M. A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, ai, blockchain, and 5G in managing its impact. IEEE Access. 2020;8:90225-90265. doi:10.1109/ACCESS.2020.2992341

38. Alsamhi SH, Lee B. Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics. IEEE Access. 2021;9:44173-44197. doi:10.1109/ACCESS.2020.3032450

39. Kalla A, Hewa T, Mishra RA, Ylianttila M, Liyanage M. The role of blockchain to fight against COVID-19. J Med Syst. 2020;44:123. doi:10.1007/s10916-020-01589-4

40. Karnouskos S. Blockchain for development in the era of the COVID-19 pandemic. IEEE Open J Ind Electron Soc. 2021;2:556-567. doi:10.1109/OJIES.2021.3215149

41. Ferrag MA, Shu L. The performance evaluation of blockchain-based security and privacy systems for the internet of things: a tutorial. IEEE Internet Things J. 2021;8(24):17236-17260. doi:10.1109/JIOT.2021.3078072

42. ImmuPass. Covid-19 immunity certificate; 2020. Accessed May 25, 2022. https://www.immupass.org/files/IMMUPASS_V2.1_En.pdf

43. ActA. Health insurance portability and accountability act of 1996.

44. Tene O, Evans K, Gencarelli B, Maldoff G, Zanfir-Fortuna G. GDPR at year one: enter the designers and engineers.

45. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains; 2018:1-15.

46. Nakamoto S, Bitcoin: a peer-to-peer electronic cash system. Decentral Bus Rev. 2008;21260.

47. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Pap. 2014;151:1-32.

48. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains; 2018:1-15.

49. Antonopoulos AM, Wood G. Mastering Ethereum: Building Smart Contracts and Dapps. O’Reilly Media; 2018.

50. Karnouskos S. Blockchain for development in the era of the COVID-19 pandemic. IEEE Open J Ind Electron Soc. 2021;2:556-567. doi:10.1109/OJIES.2021.3215149

51. Ferrag MA, Shu L. The performance evaluation of blockchain-based security and privacy systems for the internet of things: a tutorial. IEEE Internet Things J. 2021;8(24):17236-17260. doi:10.1109/JIOT.2021.3078072

52. ActA. Health insurance portability and accountability act of 1996. O’reillyMedia; 2018. MasteringEthereum:BuildingSmartContractsandDapps

53. ActA. Health insurance portability and accountability act of 1996. O’reillyMedia; 2018. MasteringEthereum:BuildingSmartContractsandDapps

54. ActA. Health insurance portability and accountability act of 1996. O’reillyMedia; 2018. MasteringEthereum:BuildingSmartContractsandDapps

55. ActA. Health insurance portability and accountability act of 1996. O’reillyMedia; 2018. MasteringEthereum:BuildingSmartContractsandDapps

56. ActA. Health insurance portability and accountability act of 1996. O’reillyMedia; 2018. MasteringEthereum:BuildingSmartContractsandDapps
57. Akbari-Nodehi H, Maddah-Ali MA. Secure coded multi-party computation for massive matrix operations. *IEEE Trans Inf Theory*. 2021;67(4):2379-2398. doi:10.1109/TIT.2021.3050853
58. Xiong X, Liu S, Li D, Cai Z, Niu X. A comprehensive survey on local differential privacy. *Secur Commun Netw*. 2020;2020.
59. Al-Breiki H, Rehman MHU, Salah K, Svetinovic D. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE Access*. 2020;8:85675-85685. doi:10.1109/ACCESS.2020.2992698
60. Chatterjee K, Goharshady AK, Pourdamghani A. Probabilistic smart contracts: secure randomness on the blockchain; 2019:403-412.
61. Hersh WR, Totten AM, Eden KB, et al. Outcomes from health information exchange: systematic review and future research needs. *JMIR Med Inform*. 2015;3(4):e5215.
62. Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Inf Sci*. 2019;485:427-440.
63. Erbguth J, Morin JH. Towards governance and dispute resolution for DLT and smart contracts; 2018:46-55.
64. Wagner E, Völker A, Fuhrmann F, Matzutt R, Wehrle K. Dispute resolution for smart contract-based two-party protocols; 2019:422-430.
65. You E. The progressive javascript framework; 2021. Accessed May 25, 2021. https://vuejs.org/
66. Ethereum. Remix IDE online; 2021. Accessed July 23, 2021. https://remix.ethereum.org/
67. Project E. Fast Ethereum RPC client for testing and development; 2021. Accessed May 19, 2021. https://github.com/trufflesuite/ganache-cli
68. ConsenSys. A crypto wallet and gateway to blockchain apps; 2021. Accessed June 18, 2021. https://metamask.io/
69. Ethereum. web3.js-Ethereum JavaScript API; 2022. Accessed May 24, 2022. https://web3js.readthedocs.io/en/v1.7.3/
70. Concourse. Eth gas station; 2021. Accessed December 28, 2021. https://ethgasstation.info/calculatorTxV.php
71. Angelopoulos CM, Damianou A, Katos V. DHP framework: digital health passports using blockchain - use case on international tourism during the COVID-19 pandemic. ArXiv; 2020.
72. Hicks C, Butler D, Maple C, Crowcroft J. SecureABC: secure AntiBody certificates for COVID-19. ArXiv 2020; abs/2005.11833.
73. Project C. Etherscan; 2021. Accessed December 28, 2021. https://etherscan.io/chart/blocktime
74. Wood G. Ethereum: a secure decentralised generalised transaction ledger; 2022. Accessed May 26, 2022. https://ethereum.github.io/yellowpaper/paper.pdf
75. Feist J, Grieco G, Groce A. Slither: a static analysis framework for smart contracts; 2019:8-15; IEEE.
76. Multiformats. Self describing hashes for future proofing; 2021. Accessed May 5, 2021. https://github.com/multiformats/multihash
77. Etherscan. Ethereum daily transactions chart; 2021. Accessed December 29, 2021. https://etherscan.io/chart/tx
78. Hafid A, Hafid AS, Samih M. Scaling blockchains: a comprehensive survey. *IEEE Access*. 2020;8:125244-125262. doi:10.1109/ACCESS.2020.3007251
79. Ethereum. Upgrading Ethereum to radical new heights; 2021. Accessed July 28, 2021. https://ethereum.org/en/eth2/
80. Etherscan. Ethereum node tracker; 2021. Accessed December 29, 2021. https://etherscan.io/nodetracker
81. Ethereum. The Ethereum upgrades; 2022. Accessed May 19, 2022. https://ethereum.org/en/upgrades/

How to cite this article: Odoom J, Huang X, Danso SA. COVID-19 and future pandemics: A blockchain-based privacy-aware secure borderless travel solution from electronic health records. *Softw Pract Exper*. 2022;52(10):2263-2287. doi:10.1002/spe.3126