BLOCKVAC: A Universally Acceptable and Ideal Vaccination System on Blockchain

Manika Sharma
Center for Security,
Theory, and Algorithmic Research
International Institute of Information
Technology, Hyderabad
Gachibowli, Hyderabad, India 500 032
manika.sharma@research.iiit.ac.in

Kishore Kothapalli
Center for Security,
Theory, and Algorithmic Research
International Institute of Information
Technology, Hyderabad
Gachibowli, Hyderabad, India 500 032
kishore@iiit.ac.in

Sujit Gujar
Machine Learning Lab
International Institute of Information
Technology, Hyderabad
Gachibowli, Hyderabad, India 500 032
sujit.gujar@iiit.ac.in

2022 IEEE International Conference on Blockchain (Blockchain) | 978-1-6654-6104-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/BLOCKCHAIN55522.2022.00051

***Abstract*—Vaccines are essential in protecting individuals and communities from the risk of harmful and fatal diseases. The world is migrating towards the digitization of vaccination documentation. Still, the current digital vaccination is a centralized model, lacking a universal acceptance. A Universally Acceptable and Ideal Vaccination System (UAIVS) should possess (a) a standard vaccination certificate verification algorithm, (b) privacy to personal information, (c) scalability, (d) support for all vaccinations, (e) accountability for vaccination information access, and (f) a scope for scientific research and development. Blockchain technology introduces decentralization, immutability, accountability, persistence, and liveliness. These properties make blockchain an ideal candidate to solve the existing problems in digital vaccination. In this paper, we propose a novel blockchain-based system, namely BLOCKVAC, to implement a *UAIVS*. Furthermore, our work provides a way to track an individual's and family's vaccination history, which is essential for scientific research and development. BLOCKVAC is highly modular, scalable, and cost-efficient, providing enough room for future feature additions. The current works lack cost and scalability analysis. We show the scalability of our system through a thorough analysis. Our implementation shows that adding one vaccination record costs 7.16828×10^{-6} ETH (~ 0.026USD) for registration, 2.5089×10^{-5} ETH (~ 0.078USD) for vaccination, and the system can easily handle up to 20K vaccinations per hour.**

***Index Terms*—Blockchain, Ethereum, Smart Contracts, Public Accountability, Scalability**

I. INTRODUCTION

The vaccination process, also known as immunization, was introduced in the late 18th century by the British physician Edward Jenner against the deadly smallpox virus [1]. Since then, it has become an inevitable medical procedure, protecting individuals and communities from harmful and fatal diseases. The World Health Organization (WHO) estimates that vaccination saves around 2.5 million child lives every year [2]. A record of vaccination details massively aids in providing quality health care to individuals [3]. While secure storage and verification of vaccination details are challenges even within a country, it is tedious to merge them from across all the countries [4]. Moreover, a definitive process is the need of the hour to verify the required vaccination certification for travelers when they enter a country.

We would like to thank MeitY and Ripple for funding this research.

Overview of existing vaccination models: Traditional paper-based vaccination records [5] are prone to challenges such as the possibility of losing, damaging, or forging the records without any accountability. Digital solutions replace the need for paper, provide an immutable card, and reduce manual labor [6]. However, the current vaccination systems follow a centralized model, where the users need to trust the central authority. Further, these systems are prone to single-point failures and jeopardize data security [7]. Moreover, current vaccination portals mainly deal with just slot bookings and issuing non-verifiable vaccination certificates.

Motivation: The Covid-19 pandemic has caused a digital revolution in vaccination data management. Countries are shifting towards a digital solution to secure vaccination data and issue certificates. However, such a system should be universally acceptable. We identify the properties required for such a system and call it a *Universally Acceptable and Ideal Vaccination System* (*UAIVS*). We further categorize the properties of *UAIVS* into two subcategories: *Universally Acceptable Vaccination System* and *Ideal Vaccination System*.

A *Universally Acceptable Vaccination System* consists:

1) **Universally Reliable Vaccination Certificate (URVC):** The vaccination certificate should be verifiable using a standard algorithm. Also, it should enhance data security by ensuring the immutability of the information [8].
2) **Universally Accountable CRUD (UACRUD):** Every data creation, read, update and delete in any vaccination record should be publically accountable and can be performed only by authorized individuals.

Furthermore, features of an *Ideal Vaccination System* are:

1) **Personal Data Security (PDS):** A vaccination system should respect the data privacy of an individual [9].
2) **Scalability (S):** The proposed vaccination system should be scalable to any-sized country [10].
3) **Vaccination History (VH):** Providing an individual's and their ancestral vaccination histories favors genetic medical research and development [11].
4) **Unified Platform (UF):** A single platform should be able to record all the different kinds of vaccinations.

978-1-6654-6104-7/22/$31.00 ©2022 IEEE
DOI 10.1109/Blockchain55522.2022.00051

Though we can partially achieve the above through a Simple Public Key Infrastructure (PKI) system, it will not provide decentralization, and key management would become a tedious task on a large scale. Blockchain technology overcomes the challenges of *UAIVS* by offering decentralization, immutability, accountability, persistence, and liveliness [12], [13].

Our Contribution: We achieve a *UAIVS* on blockchain through BLOCKVAC. The data once entered on blockchain, is immutable. We use this property to securely keep the hash of the vaccination certificate on blockchain and verify it with the original certificate whenever needed. We also use this property for real-time vaccination statistics. Blockchain-based systems are an alternative to creating distributed databases with much more trust and transparency while offering better privacy. Moreover, the cost of transactions on blockchain could go very high. Hence, We take the help of secure off-chain storage to minimize the cost of transactions and achieve data privacy on blockchain. Every change is accountable on blockchain. We use this property to ensure that every access to the vaccination records by the verifiers, vaccinators, or any other party gets recorded on blockchain. We have performed a thorough system analysis, showing that our efficiently designed smart contracts make our system highly scalable to any sized country, with extreme pocket-friendly costs. The current vaccination systems mainly deal with only slot booking and issuing vaccination certificates. Our blockchain accountable algorithms fetch an individual's and family's vaccination history for any disease. We analyzed the performance of BLOCKVAC with reasonable assumptions of (i) a reasonable number of 200 vaccinations per person in its lifespan and (ii) the typical life expectancy of a person of 100 years (Currently, the highest life expectancy is ~ 82.3 years). Our storage analysis shows that BLOCKVAC is sustainable for the next 100 years with the current technology. It provides our system with the capability to have a unified vaccination platform. We validate the practicality of our system using Ethereum-based smart contracts.

Our Approach: A vaccination system consists of three steps: (i) Registration, (ii) Vaccination, and (iii) Vaccination Record Access (Verification, Vaccination Updates/Deletes, Access to Vaccination History, Real-Time Vaccination Statistics).

To one-time register at BLOCKVAC, we take the help of an official national identity issuing government body, *Beneficiary Identity Registration Center* (*BIRC*). BIRC stores a beneficiary's details (along with biometrics) in its secure database by validating the beneficiary, ensuring BLOCKVAC is not linked directly to personal details. It also returns a unique randomized registration token to the beneficiary and stores its hash on the smart contract. This existence of the hash of the token on-chain serves as the proof of the beneficiary's registration on BLOCKVAC. The beneficiary provides its biometric, registration token, and the list of desired vaccines to BLOCKVAC center (*BC*) for vaccination. After BIRC and BC authentication, the vaccination record is updated by the vaccinator, and the beneficiary finally receives a vaccination certificate from the BC. The certificate's hash and the real-time statistics variables get updated on the blockchain. Our system also takes care of eligibility for vaccination, authorized vaccinators making any create, delete, or updates in the beneficiary's vaccination record, and the current vaccine's impact on future vaccinations, which we discuss in detail in the system design. To be noted here, BC is not a centralized body but is a decentralized blockchain system.

TABLE I
COMPARISION OF BLOCKVAC WITH DIFFERENT VACCINATION SYSTEMS

	URVC	VACRUD	PDS	S	VH	UF	Decentralized
Dodo et al. [14]	●	◐	●	-	-	-	●
Alkhansaa et al. [15]	●	-	●	◐	-	◐	●
Marc et al. [16]	●	-	●	◐	-	◐	●
CoviChain [17]	◐	-	●	◐	-	-	●
Justice et al. [18]	◐	◐	●	◐	-	-	●
Sanjib et al. [19]	◐	-	◐	◐	-	◐	●
Andrei et al. [20]	◐	-	-	-	◐	●	●
José et al. [21]	●	-	●	●	-	◐	●
BLOCKVAC	●	●	●	●	●	●	●

● = satisfying property strongly; ◐ = satisfying property weakly; - = not satisfying the property;

A. Related Works

Blockchain, already finds its use in auction [22], payments [23], [24], land record management [25], and voting [26] to name a few. With this premise, let us shed some light on the state-of-the-art algorithms in vaccination systems that use blockchain. The currently proposed works revolve around beneficiary identity verification, generating, issuing, and verifying vaccination certificates, and only a few works discuss the scalability scopes. Covichain [17] lacks the vaccination certificates and acts as a covid passport. Dodo et al. [14] provides only the feature of verifiable vaccination certificates to eradicate vaccination immunity certificate fraud. Alkhansaa et al. [15] lack scalability analysis for a large population with a single system supporting all vaccinations. José et al. [21] take a step ahead by focusing on performing a scalability study for the European population. Dodo et al. [14] also use a partial CRUD for the vaccination certificate. BLOCKVAC satisfies all the missing features of the current works in vaccination on the blockchain, adds the Vaccination History, and supports all the vaccinations. Also, it is not limited to just Covid-19. Interested readers can refer to Table I comparing the notable works for vaccination on the blockchain and BLOCKVAC.

II. BLOCKVAC: MODEL AND SYSTEM DESIGN

We call the stakeholders of a *UAIVS BC*. We categorize *BC* into four major groups: The *Beneficiaries* of the vaccine and owner of **c**, The authorized health care *Vaccinators* of the beneficiaries and issuer of **c**, the *Verifiers* of **c** who are granted verification rights by the beneficiaries, and the *Researchers* contributing to science with the permission of the beneficiary.

TABLE II
VARIABLES IN BLOCKVAC

Variable	Definition
β	Reference to beneficiary in algorithms of BLOCKVAC
α, γ	Registrations per hour and Vaccinations per hour respectively
b, bpd	β's biometric and personal details respectively
vd	β's vaccination details
fgn	Family group number
t	Registration token issued to β by *BIRC*
DB_{birc}	Database storing bpd
DB_{birc}	Database storing vd
c	Universally Reliable Vaccination Certificate
C	Vaccination certificates corresponding to $\mathcal{V}$
$indexR$	Index to access verification smart contract database

TABLE III
SMART CONTRACT DATABASES IN BLOCKVAC

Variable	Definition
ll	Minimum ages for vaccine ids as index
ul	Maximum ages for vaccine ids as index
sc_s	β's vaccination status
sc_{bct}	β's total completed vaccinations
sc_{ctt}	Country's total vaccinations for a vaccine
sc_{cti}	Country's total vaccinations against a disease
sc_{fv}	Family's total vaccinations using a particular vaccine
sc_{ft}	Family's total vaccinations against a particular disease

We take the help of *BIRC* to provide a beneficiary with a valid identity, store the beneficiary's personal data on the BIRC database securely, and register the beneficiary on the blockchain, and *BC*, to authorize or deauthorize vaccinators, vaccinate the beneficiaries and report any access to a beneficiary's vaccination data on the blockchain. [1]

There are five constituent functionalities in BLOCKVAC Section II-A: Registration, Section II-B: Vaccination, Section II-C: Accountable create and read, Section II-D: Vaccination History and Section II-E: Real-time Information Retrieval. We demonstrate the flow of BLOCKVAC registration in Figure 1.

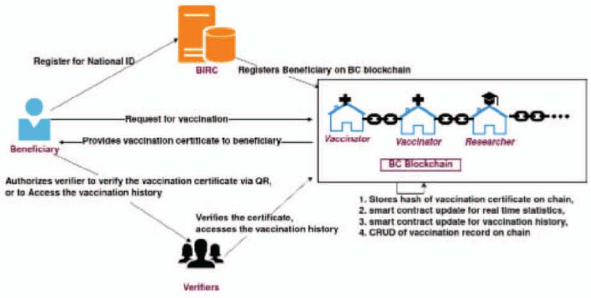

Fig. 1. BLOCKVAC Architecture

[1]This paper follows a color-coding scheme. We represent stakeholders, governing bodies in *blue*, off-chain algorithms in orange, on-chain algorithms in purple, primary driver algorithms in violet, and variables in *brown*.

A. Registration

The first step in becoming eligible for any country's official documentation is to possess a valid identity [27] by registering at an official Beneficiary Identity Registration Center (*BIRC*). We propose to add a few more steps in this process, as per Algorithm 1 `RegisterBeneficiary()`, which takes the parameters as the Beneficiary's Personal Details (**bpd**) along with biometrics (**b**), and returns a registration token (**t**) to the beneficiary. We present Registration as follows:

A beneficiary provides personal details and biometrics to the *BIRC*. The elements of **bpd** are Beneficiary's: Name (**n**), Time of birth (**tob**), Gender (**g**), and a list of family group numbers (**F**). The family group number is a unique identifier provided to the members of a particular family. A person may belong to more than one family. We take the help of *BIRC* to validate the beneficiary's personal details using `Validate()`. We suggest a biometric scanner to record the biometrics of the beneficiary. Algorithm `GetIN()` generates a unique Identity Number(**in**) for the beneficiary. If the validation succeeds, the beneficiary's personal details along with the identity number get stored against the hash of the beneficiary's biometrics in the *BIRC* database using $\texttt{UpdateDB}_{birc}\texttt{()}$. One can refer to any algorithms they wish to hash the biometrics using `GetBHash()`. One of our suggestions is Covichain [17], which uses a robust locality-sensitive hashing algorithm over an iris extraction technique. If the database write succeeds, `GetToken()` generates a registration token. The token's hash[2] is stored on the smart contract using `UpdateContract()`. The identity token gets returned to the beneficiary marking the successful Registration of the beneficiary on BLOCKVAC. The token is issued off-chain and is not stored on-chain or off-chain to secure the beneficiary's vaccination details. The smart contract assumes that the registration centers distribute unique and randomized tokens truthfully, securely, and privately. We suggest any ACID decentralized DBMS [29] for off-chain data storage.

Algorithm 1: `RegisterIdentity`(b, bpd)

Input: β's biometrics b and personal details bpd
Output: Registration token t
Require: Validate() == $true$
$h_b \leftarrow$ GetBHash(b)
$in \leftarrow$ GetIN()
if *updateDB*$_{birc}$(h_b, bpd, in) *is successful*
  $t \leftarrow$ GetToken()
  $h_t \leftarrow$ sha(t)
  UpdateContract(sc_t, h_t)
return t

B. Vaccination

BLOCKVAC Center (*BC*) runs the driver algorithm, `BVaccinate()` as listed in Algorithm 4 to vaccinate a

[2]We suggest using a suitable and efficient hash function, e.g., sha3, keccak-256,([28]) to improve the overall performance of a blockchain significantly.

beneficiary. The beneficiary provides biometrics, registration token, and the desired list of vaccines to *BC* and receives the corresponding list of vaccination certificates after successful vaccination. We present *Vaccination* as follows:

Beneficiary authentication is performed by *BIRC's* algorithm `AuthB()`, which checks if beneficiary's biometric is valid, and *BC*'s algorithm `AuthT()`, which checks if beneficiary's token's hash exists on-chain. The authentication of the biometric grants `GetPD()` permission to securely fetch the beneficiary's personal details from the database of *BIRC* using the biometric hash as the key into the smart contract temporarily. The registration token's hash on-chain shows that the beneficiary is a registered user of BLOCKVAC. The beneficiary's request for the desired vaccine is satisfied when it fulfills all of the following eligibilities:

- The prerequisite vaccinations must already be taken.
- Vaccination against a vaccine-type can be only once.
- The beneficiary's age should be at least the minimum age limit for the desired vaccination and at most the maximum age limit for the desired vaccination.

BC calls the vaccinator to vaccinate the beneficiary using the vaccinator's driver algorithm `Vaccinate()`. The list, namely *Vaccinators*, stores authorized vaccinators' blockchain account addresses. If the vaccinator is authorized, it signs on blockchain that it is accessing the beneficiary's vaccination records. The vaccinator vaccinates the beneficiary by creating a new vaccination record for the beneficiary using the using `CreateVD()` and updating them with the vaccination information. The elements of vaccination record are: Vaccine ID (`vcid`), Vaccine Name (`vcn`), Vaccine Type (`vct`), Vaccination Status (`vcs`), Date Of Vaccination (`dovc`), Vaccination Location (`vcl`), Vaccinator's address(`vra`) and Vaccinator's Name (`vrn`). Algorithm `Gc()` then generates the vaccination certificate. `UpdateDB`$_{bc}$ updates the vaccination details against (hash of token, vaccination id) as key in all the family group tables of the beneficiary in the off-chain database `DB`$_{bc}$. On a successful database update, the certificate's hash is stored on-chain, the vaccination status for the vaccine's type is set on the smart contract, the vaccination count of the beneficiary, the vaccination count against the disease, and the vaccination count of the vaccine are incremented.

Algorithm 2: `IsEligible`$(h, a, vid, type)$

Input: β's token's hash h, age a, vaccine id vid, vaccine type $type$
Output: $true/false$
Require: $a \geq ll[vid]$ and $a \leq ul[vid]$ and $sc_s[h||type]==false$
for ***each*** $i \in depn[vid]$ **do**
  if $sc_c[h||i] == NULL$
    return $false$
endfor
return $true$

Algorithm 3: `Vaccinate`(pd, h)

Input: β's token's hash h, personal details pd
Output: Vaccination Certificate c
Require: $msg.sender \in Vaccinators$
if *CreateVD(h, vid, DB*$_{bc}$*, pd.fn) is success*
  $vd[h||vid] \leftarrow (vid, vname, vtype, true, curDate, curAdd, msg.sender, vrn)$
  $c \leftarrow gc(pd, vd)$
  updateDB$_{bc}$$(h||vid, pd, vd, pd.fgn)$
$sc_{vaccinators}[h||vid||index] = msg.sender$
return c

Algorithm 4: `BVaccinate`$(b, t, \mathcal{V})$

Input: β's biometric b, token t, desired list of vaccines $\mathcal{V}$
Output: β's List of vaccination certificates C corresponding to $\mathcal{V}$
Require: AuthB(b)==$true$ && AuthT(t)==$true$
h_b = sha(b)
h_t = sha(t)
$pd \leftarrow$ getPD(DB_{birc}, h_b)
$a \leftarrow$ time.time() - $pd.tob$
for ***each*** $vid \in \mathcal{V}$ **do**
  if *isEligible*$(h_t, a, vid, vid.type) == true$
    c = Vaccinate(pd, h_t)
    Add c to C
    $h_c = sha(c)$
    $sc_c[h_t||vid] = h_c$
    $sc_s[h_t||vid.type] = true$
    $sc_{bct}[h_t] = sc_{bct}[h_t] + 1$
    $sc_{ctt}[vid.type] = sc_{ctt}[vid.type] + 1$
    $sc_{cti}[vid] = sc_{cti}[vid] + 1$
    for ***each*** $f \in pd.F$ **do**
      $sc_{fv}[f||vid] = sc_{fv}[f||vid] + 1$
      $sc_{ft}[f||vid.type] = sc_{ft}[f||vid.type] + 1$
    endfor
endfor
return C

C. Accountable Read

Algorithm 5 helps a beneficiary or an authorized individual verify if its certificate is **URVC** and simultaneously update its address on blockchain using the variable $indexR$.

D. Vaccination History

A beneficiary's or anyone in the beneficiary's family(ies) history of missing vaccinations can be found as:

1) Beneficiary's Vaccination History: After traveling to a pandemic-affected country, an individual might be a disease carrier to the home country. An individual vaccinated with the yellow fever vaccine will be less prone to catching the fever or becoming a carrier. The beneficiary's vaccination history

Algorithm 5: `VerifyCertificate`(b, t, vid, c)

Input: β's biometric b, token t, vaccination id vid, certificate c
Output: $true/false$
Require: AuthB(b) == $true$ && AuthT(t) == $true$
h_t = sha(t)
$sc_{verify}[h_t||indexR] = msg.sender$
$indexR = indexR + 1$
h_c = sha(c)
if $sc_c[h_t||vid] == h_c$
  return $true$
return $false$

Algorithm 6: `familyVaccinationHistory`($t, b, choice$)

Input: β's token t, biometric b, variable $choice$
Output: $true/false$
Require: AuthB(b) == $true$ && AuthT(t) == $true$
h_b = sha(b)
h_t = sha(t)
$pd \leftarrow$ getPD(DB_{birc}, h_b)
if $choice == 1$
  for ***each*** $f \in pd.F$ **do**
    if $sc_{fv}[f||vid]! = pd.F.size()$
      return $true$
  endfor
if $choice == 2$
  for ***each*** $f \in pd.F$ **do**
    if $sc_{ft}[f||type]! = pd.F.size()$
      return $true$
  endfor
return $false$

helps check if the beneficiary has missed any vaccinations or protection against any disease.

2) Beneficiary's Family Vaccination History: Genetic research is a prominent field in science and technology. It might be possible for a person to develop a disease due to a missing vaccination in his or her ancestry. Also, an individual's family history may help detect the spread of disease in the family. For example, if an individual is not vaccinated for yellow fever and catches the disease, there is a high possibility of his or her family members being infected. We can know from the family history if family members have missed any vaccination. Algorithms 6, with choice 1 remarks if anyone in the beneficiary's family is missing a particular vaccination and choice 2 remarks if anyone in the beneficiary's family is missing a vaccination against a particular disease.

E. Real Time Vaccination Statistics

The current vaccination portals actively present the doses of vaccinations completed. Using the smart contract variables listed in Table III, our system presents several real-time vaccination statistics such as the total number of completed vaccines for a beneficiary, number of completed vaccines against a disease for a country, and the total people vaccinated against a particular disease in a country. If the beneficiary's age lies in the vaccination limits for the desired vaccine, we derive the due dates of a vaccine using the as follows:

$$dueDates[vid] = currentDate + (ul[vid] \text{ - } age)$$

III. BlockVac:System Analysis

We designed on-chain algorithms using Ethereum-based smart contracts in `Solidity` programming language and off-chain algorithms in `Python` and deployed them on Ganache. `web3.py` establishes the communication between off-chain and on-chain algorithms. We perform analysis using centos with x86-64 architecture, Intel(R) Xeon(R) Gold 6226R CPU @ 2.90GHz, and 95 GB of memory. We show the scalability of our system on the vaccination data of the three most populous countries [30]: China, India, and the United States assuming BlockVac functions for eight hours ($time$) per day.

A. Cost Analysis

This section describes the estimated Ether (ETH) required by the smart contracts in BlockVac and the corresponding cost in USD[3]. We perform our protocol analysis in two parts: Beneficiary's Vaccination Registration and Beneficiary's Vaccination. The one-time registration process is performed by *BIRC* by adding the registration token of a new beneficiary to the blockchain. The average number of newborns per day (n_1) in China, India, and the USA are 49388, 67385, and 10267, respectively. For these countries, we take an upper bound of 0.05 million, 0.1 million, and 0.02 million registrations per day. Therefore, we estimate per hour registrations to be 6250, 12500, 2500 ($\alpha = \frac{n_1}{time}$). The highest number of vaccinations recorded (n_2) in a day are 14 million, 25 million, and 4.6 million in China, India, and the USA. We assume 1000 vaccination sites (w) per country. Hence, vaccinations per hour per site ($\gamma = \frac{n_2}{time \times w}$) for China is 1750, India is 3125, and the USA is 575. From Figure 2, we can observe that the average cost per registration and vaccination is 0.026 USD, and 0.078 USD, respectively. This cost is modest compared to the current price of vaccinations.

B. Space Analysis

Consider a country with over a billion population. Assume 1% population growth. We believe that no country will have more than a 3B population in the next 100 years even with these numbers [31]. Assuming a person lives up to the age of 100 years and gets vaccinated with all the prescribed vaccines,i.e., 200 vaccines. Each vaccination record on a blockchain is of a maximum size 1 KB. Hence, data size per individual is based on the number of vaccines administered per individual and the size of each vaccination record on blockchain, which is estimated to be 200×1 KB = 200 KB.

[3]At the time of writing this paper, 1 ETH = 2,934.88 USD.

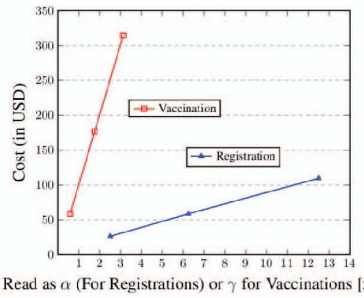

Fig. 2. Cost Analysis trend of BLOCKVAC

Hence, the total data storage size on BLOCKVAC over the entire population for the next 100 years is 200 KB $\times$ 3 billion 545.69 TB (or, 181.89 TB per billion). We can meet the storage amount with current storage technology solutions. It is possible to naturally distribute the needed storage across multiple storage servers and multiple sites. Even with vaccinations per individual as 500, the required storage is under 1.5 PB.

IV. CONCLUSION AND FUTURE WORK

In this paper, we built a scalable *UAIVS* over a blockchain. We studied the requirement for countries with a population of over a billion and identified the key challenges. We proposed a blend of off-chain and on-chain algorithms to design *UAIVS* as cost-effective and scalable while offering data security. We call the proposed system as BLOCKVAC. Our experiments show that our proposed system is highly reliable, secure, cost-efficient, and sustainable with the current technology for the next 100 years. We believe a complete solution to *UAIVS* over blockchain will significantly impact handling vaccination records. In the future, we would like to add DApp and use cryptographic accumulators for family grouping. Also, we aim to perform security and privacy analysis of BLOCKVAC.

REFERENCES

[1] S. Riedel, "Edward jenner and the history of smallpox and vaccination," in *Baylor University Medical Center Proceedings*, vol. 18, no. 1. Taylor & Francis, 2005, pp. 21–25.

[2] W. A. Orenstein and R. Ahmed, "Simply put: Vaccination saves lives," pp. 4031–4033, 2017.

[3] T. Bärnighausen, D. E. Bloom, E. T. Cafiero-Fonseca, and J. C. O'Brien, "Valuing vaccination," *Proceedings of the National Academy of Sciences*, vol. 111, no. 34, pp. 12 313–12 319, 2014.

[4] K. Sharun, R. Tiwari, K. Dhama, A. A. Rabaan, and S. Alhumaid, "Covid-19 vaccination passport: prospects, scientific feasibility, and ethical concerns," *Human Vaccines & Immunotherapeutics*, vol. 17, no. 11, pp. 4108–4111, 2021.

[5] D. W. Brown, M. Gacic-Dobo, and S. L. Young, "Home-based child vaccination records–a reflection on form," *Vaccine*, vol. 32, no. 16, pp. 1775–1777, 2014.

[6] W. Maurer, L. Seeber, G. Rundblad, S. Kochhar, B. Trusko, B. Kisler, R. Kush, B. Rath, and V. V. S. Initiative, "Standardization and simplification of vaccination records," *Expert Review of Vaccines*, vol. 13, no. 4, pp. 545–559, 2014.

[7] S. P. Burger, J. D. Jenkins, S. C. Huntington, and I. J. Perez-Arriaga, "Why distributed?: A critical review of the tradeoffs between centralized and decentralized resources," *IEEE Power and Energy Magazine*, vol. 17, no. 2, pp. 16–24, 2019.

[8] E. Mbunge, S. Fashoto, and J. Batani, "Covid-19 digital vaccination certificates and digital technologies: lessons from digital contact tracing apps," *Available at SSRN 3805803*, 2021.

[9] A. Rieger, T. Roth, J. Sedlmeir, and G. Fridgen, "The privacy challenge in the race for digital vaccination certificates," *New York Medical Journal*, vol. 2, no. 6, pp. 633–634, 2021.

[10] N. Bonvin, T. G. Papaioannou, and K. Aberer, "An economic approach for scalable and highly-available distributed applications," in *IEEE International Conference on Cloud Computing*, 2010, pp. 498–505.

[11] H. Ding, J.-H. Xu, Z. Wang, Y.-Z. Ren, and G.-H. Cui, "Subsidy strategy based on history information can stimulate voluntary vaccination behaviors on seasonal diseases," *Physica A: Statistical Mechanics and its Applications*, vol. 503, pp. 390–399, 2018.

[12] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018.

[13] S. Siddiqui and S. Gujar, "Quicksync: A quickly synchronizing pos-based blockchain protocol," *arXiv preprint arXiv:2005.03564*, 2020.

[14] D. Khan, M. A. Hashmani, L. T. Jung, and A. Z. Junejo, "Blockchain enabled track-and-trace framework for covid-19 immunity certificate," in *2nd International Conference on Computing and Information Technology (ICCIT)*. IEEE, 2022, pp. 248–253.

[15] A. A. Abuhashim, H. A. Shafei, and C. C. Tan, "Block-vc: A blockchain-based global vaccination certification," in *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2021, pp. 347–352.

[16] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third, and J. Domingue, "Covid-19 antibody test/vaccination certification: there's an app for that," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148–155, 2020.

[17] P. Bradish, S. Chaudhari, M. Clear, and H. Tewari, "Covichain: A blockchain based covid-19 vaccination passport," *arXiv preprint arXiv:2112.01097*, 2021.

[18] J. Odoom, R. S. Soglo, S. A. Danso, and H. Xiaofang, "A privacy-preserving covid-19 updatable test result and vaccination provenance based on blockchain and smart contract," in *ICMRSISIIT*, vol. 1. IEEE, 2019, pp. 1–6.

[19] S. K. Deka, S. Goswami, and A. Anand, "A blockchain based technique for storing vaccination records," in *2020 IEEE Bombay Section Signature Conference (IBSSC)*. IEEE, 2020, pp. 135–139.

[20] A. Carniel, G. Leme, J. de Melo Bezerra, and C. M. Hirata, "A blockchain approach to support vaccination process in a country," 2021.

[21] J. L. Hernández-Ramos, G. Karopoulos, D. Geneiatakis, T. Martin, G. Kambourakis, and I. N. Fovino, "Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[22] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *IEEE international conference on communications (ICC)*. IEEE, 2018, pp. 1–6.

[23] D. Chatzopoulos, S. Gujar, B. Faltings, and P. Hui, "Localcoin: An ad-hoc payment scheme for areas with high connectivity: Poster," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2016, pp. 365–366.

[24] S. Nakamoto, "Re: Bitcoin p2p e-cash paper," *The Cryptography Mailing List*, 2008.

[25] V. Thakur, M. Doja, Y. K. Dwivedi, T. Ahmad, and G. Khadanga, "Land records on blockchain for implementation of land titling in india," *International Journal of Information Management*, vol. 52, p. 101940, 2020.

[26] S. Damle, S. Gujar, and M. H. Moti, "Fasten: Fair and secure distributed voting using smart contracts," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–3.

[27] H. Agarwal and G. Pandey, "Online voting system for india based on aadhaar id," in *2013 Eleventh International Conference on ICT and Knowledge Engineering*. IEEE, 2013, pp. 1–4.

[28] F. Wang, Y. Chen, R. Wang, A. O. Francis, B. Emmanuel, W. Zheng, and J. Chen, "An experimental investigation into the hash functions used in blockchains," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1404–1424, 2019.

[29] S. Yu, "Acid properties in distributed databases," *Advanced eBusiness Transactions for B2B-Collaborations*, 2009.

[30] B. Milanovic, "Half a world: Regional inequality in five great federations," *Journal of the Asia Pacific Economy*, vol. 10, no. 4, pp. 408–445, 2005.

[31] M. Roser, "Future population growth," *Our World in Data*, 2013.