# Identity Inclusion: A Digital National Identification for All

Andrew Amstrong Musoke[1], Patrick Dushimimana[1], and Martin Saint[1,2(✉)]

[1] Department of Information and Communications Technology, Carnegie Mellon University Africa, Kigali, Rwanda
{amusoke,pdushimi}@andrew.cmu.edu, msaint@cmu.edu
[2] Kigali Collaborative Research Centre, Kigali, Rwanda
http://www.africa.engineering.cmu.edu, http://www.kcrc.rw

**Abstract.** Governments offer civil services to their citizens if the citizen can identify themselves using a government-issued identification document. Several documents are often required, such as a national ID and driving license. These identification documents do not share data, or even validity, between different civil entities. Organizations like Sovrin, SecureKey, and ShoCard have presented solutions to ease identification using digital identification based on blockchain technology because of the benefits of immutability, transparency, reliability, and secure sharing of identity data. The solutions, however, all require the use of Internet-enabled devices to access the solution. To accommodate developing countries where smartphones and computers are not prevalent, we designed a proof of concept digital national identification based on the Ethereum blockchain that utilizes Unstructured Supplementary Service Data (USSD) for end-user communications. The solution gives governments control over lawfully required data while allowing the citizen to retain sovereignty over personal data using trust zones. Consequently, a citizen can use a single identity across multiple civil service providers, even with a feature phone.

**Keywords:** Digital identity · National identity · Blockchain 2.0 · Smart contract · Ethereum · Digital assets · E-infrastructure · E-government

## 1 Introduction

The ISO/IEC 24760-1 specification for IT Security and Privacy defines identity as a set of attributes related to an entity [1]. A digital identity is an identity in an online or networked environment that represents a real-world entity like a person or business.

A digital identity enables institutions like governments, banks, and telecommunication service providers to incorporate secure digital services into their operations. In the digital realm, any assertion we make about ourselves, the identity owner, is called a claim. Claims can be anything from the name of the


S. Paiva et al. (Eds.): SmartCity360° 2020, LNICST 372, pp. 511–525, 2021.
https://doi.org/10.1007/978-3-030-76063-2_34

identity owner to the school from which they graduated. These claims can be nearly impossible to verify, unlike in the physical world, where possession of an acceptable document is considered sufficient proof of identity. For this reason, organizations like the Sovrin Foundation have embarked on digital identification implementations using blockchain technology, as explained in the Sovrin white paper [2].

A blockchain is a distributed, decentralized, public ledger. Private or permissioned versions are also possible. It is a record-keeping technology with a distributed network of participating nodes that maintain a majority-consensus of the state of the entries in the ledger. Records kept in the ledger are considered immutable due to the infeasibility of altering records across a large number of independently distributed nodes. These properties make a blockchain a desirable technology for the implementation of digital identity due to the transparency, immutability, and global nature of a blockchain network.

Here, the term *government* is used to collectively refer to the executive, legislative and judiciary branches including ministries, local governments, public sector offices, etc.

### 1.1 Background

A national identification document or card is a government-issued portable document given to each citizen or resident in some countries that serves as legal proof, for government and many other services, that the person is whom they claim to be. Taking the case of the country of Rwanda, for instance, the first Rwandan national ID was issued during the Belgian colonial period starting in 1930 and was paper-based and written by hand. A new plastic laminated national identity card system was implemented in 2008, improving both durability and the system for issuing identity documents [3].

To get a national identity card in Rwanda, the citizen must be above the age of 15. Rwanda has an online platform called IREMBO that helps citizens access different e-government services such as national identity document issuance, birth certificates, insurance payments, and police declarations.

To get the national identity card in Rwanda, a citizen needs to get both an application number from their residential sector office and a biometric data form with information such as fingerprints. They then apply online [4]. The application cost is 500 Rwandan Francs (about $0.53 US at the time of this writing), and a card is issued within one month and sent to the applicant's sector office for them to pick up.

Each Rwandan identity card has a National Identity Number (NIN) that can serve as a unified interface between a unique individual and any civil service availed by the government. The card is also legal identification for hospitals that keep patient details, banks, school registration, and when accessing government services like birth certification, driving permits, and land permutation [5].

### 1.2 Problem Statement

Despite holding the national identity card, for a Rwandan to access different forms of civil services, they may require different forms of identification. For example, a citizen needs to show a driver's permit to access traffic control services, despite having a national ID that duplicates much of the same information. Despite being "national", the current physical identity card system is challenged by a lack of interoperability amongst civil service providers. Even in cases where integration is attempted, this is done in silos for different services as opposed to a single integration platform with a unified interface to ease and accelerate integration. The physical card is also subject to loss or damage, forgery, and fraud. A physical document does not interface well with an increasingly digital world and the proliferation of e-government and online services.

In this paper, we demonstrate a technical approach to implementing a secure digital identity system using the Ethereum blockchain. This system is appropriate for Africa because it requires little in the way of new infrastructure and builds upon a well-accepted blockchain platform. We also address a problem not well explored in other papers: implementation in the context of a country with a prevalence of feature phones over smartphones or computers. While we use the case of Rwanda in our examples, our approach is appropriate for many African countries or developing nations where citizens rely primarily on feature phones to access the Internet or digital services. We focus on demonstrating the technology without attempting to address the myriad of policy and socio-economic challenges that come with a blockchain-based national identity scheme. It is not our intent to minimize the non-technical challenges. Instead, they exist outside of the scope of this paper.

### 1.3 Objectives

Considering the digital identity problems mentioned in the prior section, we define the following objectives for our solution:

1. Build a robust and resilient platform that is sufficiently reliable to be used nationally.
2. The solution must be distributed for robustness and flexible enough to be deployed despite civil service providers' heterogeneity.
3. The solution should be usable by citizens who own only a feature phone.
4. As a national identity, the solution should be under the control of the government.

## 2 Literature Review

There are several approaches to providing digital identity for individuals using a blockchain. The Sovrin Foundation is an open-source project working toward creating a digital identity that is entirely controlled by the user, a concept called

self-sovereignty. Here, the user chooses which attributes to share. The architecture, however, requires trusted and authorized organisations called stewards to provide resources towards the network and intermediaries like trust anchors that control how you acquire your identity [2]. The concept of self-sovereign identity would present challenges in a government setting where a user is mandated by law to share identification information. For a national identity, the government should retain control over the identity attributes and issuing or revoking a national ID [2,6].

Another project that does not utilize the self-sovereignty principle is called ShoCard. A citizen takes a picture of an existing verified credential, like a passport, in a process called bootstrapping [7]. The credential is then bound to a cryptographic identity, and this forms their digital ID. ShoCard then acts as a trusted third party that stores the credentials and interactions with a party requesting a user's ID. This system's reliance on a third party voids certain benefits of decentralization, such as the resiliency of a distributed network, should the company go out of business. Dunphy and Petitcolas compare Sovrin and ShoCard against the Facebook Connect digital identity solution, which does not utilize blockchain technology [8]. Their work concluded that the blockchain-based digital identity systems suffered from poor user experience, which is a barrier to uptake because users have to understand cryptographic key management in both cases.

Mudliar et al. proposed a framework to integrate an existing national identity system in India, the Aadhar number, into the blockchain [9]. They explore the benefits of migrating to a decentralized national ID, such as voting or healthcare, where one simply scans a barcode to be identified. Under this system, officials have access to all information, and a record of all actions performed with the identity is kept on a public ledger.

Other work, using the country of Columbia as an example, suggested using three aspects to identify a citizen [10]. The proposed model introduces a digital identity that provides strong authentication comprising something the user has, like a physical smart card, something the user knows, like a personal identification number (PIN), and something the user is, like a fingerprint.

A paper by Wolfond discusses how Canada has used a digital ID to improve their service delivery in both the public and private sectors in a completely decentralised model [11]. Current systems of identification are either too cumbersome, like passwords, or less secure and harder to validate, like driving licenses. Another drawback of traditional systems is the inherent vulnerability of relying on a centralized system with a single point of failure and audit. Centralization affects both the system's resilience and user privacy, since all user transactions may be tracked through one application if compromised. The author concludes with the perceived benefits of using a blockchain, such as reduced wait times, quick verifiability of third party documents, and improved citizen privacy protection when delivering government services.

Some of the previous work mentioned relies on physically issued identification or does not lend itself to solving the interoperability challenge. Other work builds

upon the self-sovereignty principal, which is inappropriate for a government-controlled identification. Finally, because many developing countries have a low prevalence of smartphones, for instance, about 15% of the population in a country like Rwanda, most of the solutions mentioned would be infeasible due to the need for a smartphone or computer. In a developing nation context, these solutions would exclude the majority of the population from using them [12].

In this work, we present a proof of concept digital national identity based on the Ethereum blockchain. It serves as a single personal data and identification store to ease government service providers' interoperability while reaping the benefits of a robust decentralized database. We utilize an Unstructured Supplementary Service Data (USSD) interface accessible on both feature phones and smartphones. Using this combination of platforms enables a solution that requires little in the way of new infrastructure and is appropriate for a government identity solution in developing countries.

## 3 Methodology

We develop our identity application using the Ethereum blockchain platform. Ethereum is a decentralized computing resource that allows users to develop applications and then deploy them on the Ethereum network. Ethereum employs smart contracts, which are programs stored on the networked computing resource that can perform defined functions based on specific inputs. Smart contracts store user data and provide the logic for modifying that data. In our case, the citizen's biometric data. Guided by the earlier objectives, the goal is to create a decentralized platform that citizens can use to procure civil services seamlessly with a single identity.

### 3.1 Developing the Prototype

For our prototype application, we focus on government and hospital services, demonstrating how a national digital ID is used with both services without carrying a physical ID.

### 3.2 Identity Trust Zones

An essential contribution of our system is the inclusion of trust zones in the ID. We define trust zones as predefined boundaries that group entities wishing to access a citizen's attributes. More highly trusted entities are closer to the center zone. This model enables using a single national ID for heterogeneous use cases.

The different trust zones are shown in Fig. 1. In the first trust zone lies the citizen, who has access to all the data represented by, or linked to, the national ID. The second trust zone will have the government and its trusted third parties, like document issuing agencies. Second zone entities have limited access to the citizen's data, but the citizen will be mandated to declare data required for civic service delivery. In the third and fourth zones, the citizen has full control over

the data that they declare. The fourth zone may be made more restrictive or limited to particular data to provide greater security and privacy.

A health care center would belong to the third trust zone. A citizen would retain the right to share information that they agree is necessary. Of course, this could affect the level of service they would be able to receive, given the individual health center's policies.

Trust zones are implemented in the logic of the smart contract. Entities are placed in trust zones by the government institutions at the point of registration. Citizens decide what data to share with entities in trust zones three and four through the USSD interface.

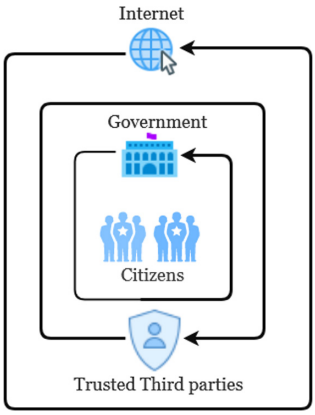


**Fig. 1.** Identity trust zones for citizen national ID.

### 3.3 Test Prototype

After building the code base for the smart contracts, we tested their functionality offline. We used a combination of the MetaMask Ethereum account manager and Rinkeby test network, a free public network for testing smart contracts before deployment to the Ethereum network [13,14].

### 3.4 Smart Contract Deployment

In the final step, we deploy the smart contract to the test Ethereum network. Our front end interacts with the smart contract using the Web3.js API. The deployment includes running an end to end demonstration of the healthcare use case to prove interoperability.

## 4 Implementation

Following our methodology, in this section, we describe the implementation of our system. First, we explain the proposed architecture and compare it with the setup used in the testing phase. Finally, we describe the process flow between the entities of the system. Our prototype's codebase is hosted in a GitHub repository at https://github.com/patrickdushimimana/national_ID.

### 4.1 Architecture

Communication between the different systems is shown in Fig. 2. Civil service providers interact with a web browser-based user interface that communicates with a government-owned server. The server hosts the logic to communicate with a mobile network operator (MNO), which communicates with the citizen's feature phone via a USSD API. The USSD protocol can take up to 182 characters which is enough to list a menu of queries [15]. The server, which also houses the application and database backend, also communicates with the Ethereum blockchain network where the smart contract and a hashed reference to the citizen registration data are stored. Here, the term server is used as a stand-in for a secure, reliable and scalable application and database infrastructure.

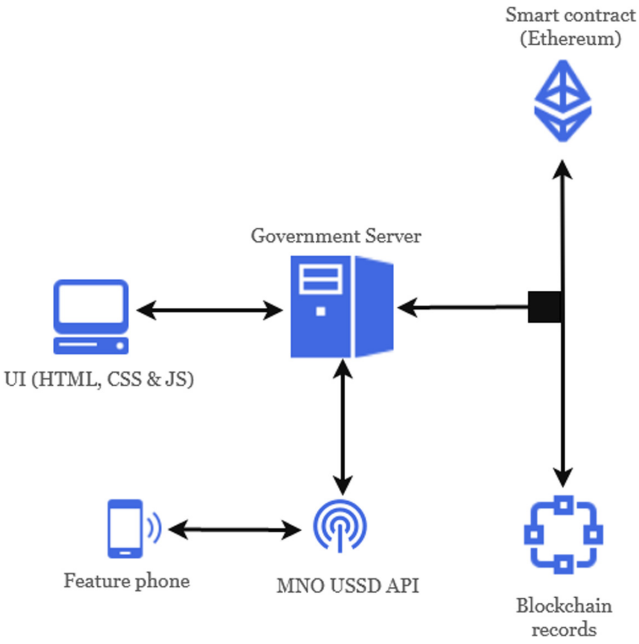


**Fig. 2.** Architecture for the national ID system.

### 4.2 Test Setup

The following tools were utilized to create and test the application.

- *Ganache* is a personal blockchain for Ethereum development that is used to deploy contracts, develop the applications, and run tests [16].
- *Truffle* is "a development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM)" [17].
- *MetaMask* allows running Ethereum distributed applications (dApps) in a browser without running a full Ethereum node [13].
- *Node.js* is a server-side platform built on the Google Chrome JavaScript Engine [18].
- *Web3.js* is a collection of libraries to interact with a local or remote Ethereum node using a HTTP or IPC connection [19].
- *Ethereum* is a distributed public blockchain network that focuses on running programming code of any decentralized application [20].
- *HTML* is the HyperText Markup Language for creating web pages [21].

The blockchain technology, Ethereum, on which our solution is based, has been tested for performance and scalability in previous works. Therefore, we focus on the proof of concept within our test environment [22].

### 4.3 Process Flow

The proposed system considers three actors, all of whom may interact directly with one another or indirectly through the logic of Ethereum smart contracts. We consider a citizen as the identity owner, a government institution as the trusted identity verifier, and a public hospital as the civil service provider. For this work, we demonstrate the feasibility of our solution in the context of only one civil service provider, a health care center.

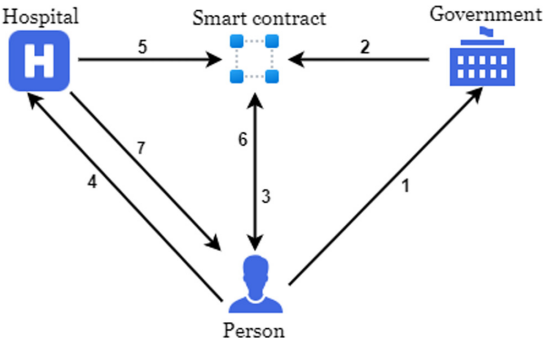


**Fig. 3.** Process flow diagram for the national ID system.

Unlike Fig. 2, which details interactions between the system components, Fig. 3 depicts the logical flow of interactions between the different actors, abstracting away the system. The flow is described as follows:

1. A citizen physically registers with an official government institution, for example Rwanda's National ID Agency (NIDA).
2. The institution verifies the citizen's information and registers the citizen's data to the blockchain. This is done through a portal interfacing with our Ethereum smart contract.
3. The citizen receives a prompt to input a four digit personal identification number (PIN). This prompt is received through a USSD application interfacing with our smart contract. Entering the PIN will confirm the registration process.
4. The citizen requests a service from a health care center.
5. The health care center requires the identifying information of the citizen. The health care center will also require national insurance information. The health care center requests the citizen's phone number, and through a portal, sends a request for the required data to the smart contract.
6. The citizen receives a prompt to input their PIN and authorize the release of their insurance, biometric, and medical history data to the health care center specified. USSD enables menu functions that would allow the aggregated authorization to all data requested by the health care center, or allow the citizen to approve only certain pieces or subsets of the requested data.
7. Upon authorization, the health care center can then confirm the identity of the citizen and proceed to offer the requested services.

In addition to requesting a citizen's information to authorize the provision of health care services, a health worker can then record the citizen's health data and link it to their identification. This data can then be stored privately on the blockchain. When the citizen visits the same or a different health care center, they can opt to share previously stored medical information, effectively having an immutable and readily available medical history that is not dependent on the health care center's information system.

In the case where a citizen does not posses their phone, they can still be identified with their National ID number. This benefits from the fact that developing countries like Rwanda have established National ID frameworks that can be extended. The National ID number will act as a reference to one's biographical and biometric data that the government and related trusted third parties have access to anyway. Verification then proceeds with biometric data like facial images, fingerprint, or voice-print identification.

### 4.4 Implementation Overview

This section shows some of the primary functions of the implemented project.

Individuals already registered for the national ID are shown in Fig. 4. They can access available services.

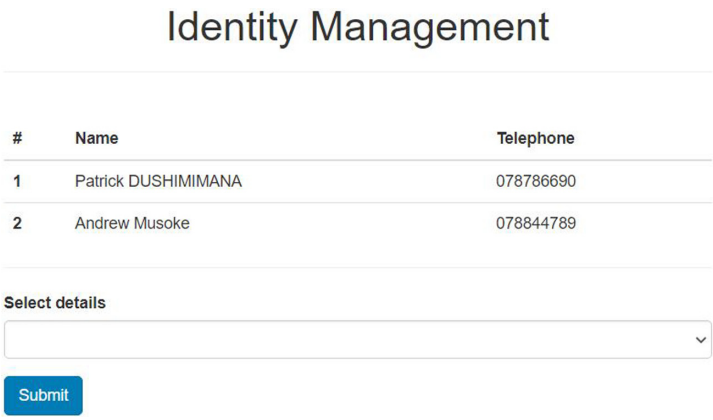


**Fig. 4.** Sample list of individuals registered for the national ID.

Individuals who have provided their insurance information as requested by the health center, are shown in Fig. 5. The document registration is recorded as a transaction in Ethereum.

The cost, in Ether, Ethereum's native cryptocurrency, charged for transactions related to registering insurance, is shown in Fig. 6. The account balance prior to a series of transactions is 100 Ether and 99.80 after.

## 5 Discussion

We implemented a proof of concept system that can serve as a foundation for a more sophisticated digital national identification platform in a developing country with low smartphone technology penetration. The system has two user interfaces, a web-based one for a government entity or civil service provider interaction, and another USSD-based one for a citizen. Compared to the current alternative, where citizens have to carry multiple forms of physical identities which can be lost or damaged, our system requires them to carry nothing but a phone to receive civil services from many different providers. Even without a phone, having a national ID or national ID number is sufficient to begin the verification process. Civil service providers can be held accountable for the use or misuse of citizen personal data since each request and use of this data is recorded as an immutable and transparent transaction on the blockchain. This can expedite audits of government entities and authorized third parties against data protection policies. It can also significantly reduce the cases of fraudulent identification claims.

### 5.1 The Issue of Cost

The system contains two levels of charges: (1) the *Ethereum gas* fee, in Ether, which is the cost of making a transaction on the Ethereum network, and (2) the

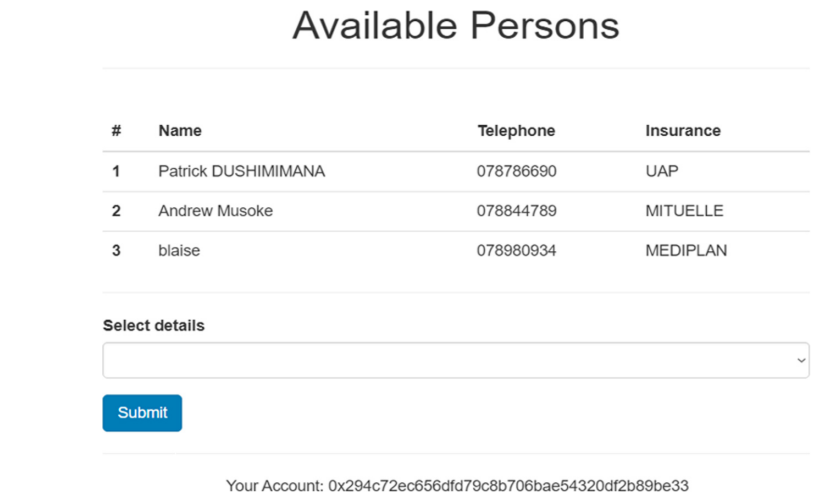


**Fig. 5.** List of individuals and their insurance providers.

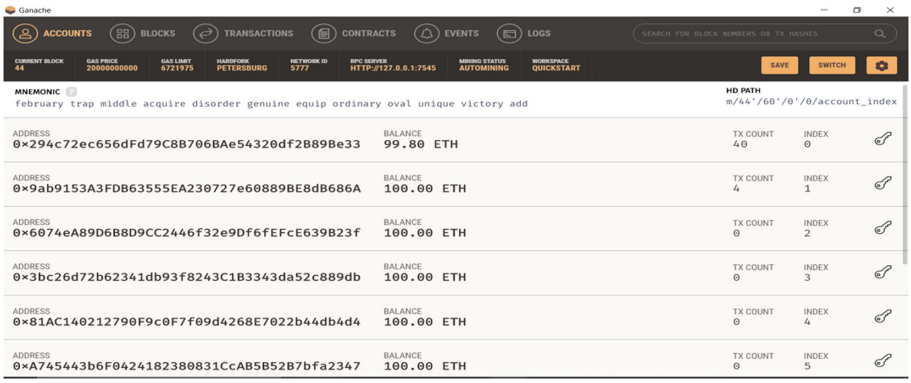


**Fig. 6.** Ether (cost) charged for the transactions.

USSD cost, paid to the MNO per USSD session. Our tests show that registering one citizen on the Ethereum network costs approximately 19 USD at the time of writing. The cost per USSD session is estimated through the pricing of an integrator like *Africa's Talking*, with charges of approximately 0.014 USD [23]. The USSD cost is low enough to be of minimal concern, but the Ethereum cost would be prohibitive in most applications. However, our implementation assumes on-chain storage of citizen data. Storing a hash of the off-chain data on-chain and keeping the actual data itself off-chain would reduce the majority of the Ethereum cost. Data storage alternatives are also under active development by the Ethereum Foundation, as this is a general problem for all applications.

### 5.2 The Issue of Centralization

The architecture proposed introduces some aspects of centralization, where the government is seen as the single point of contact. We worked under the assumption that the country has a government whose majority membership is trusted to offer its citizens civil services. The system, however, makes no assumption about the trustworthiness of any one individual. From this perspective, the system can still be viewed as decentralised because no one person can control the blockchain network without consensus from the majority of the trusted government.

An authorized individual can still perform malicious activity, like unauthorized access of citizen data. Without the ability to control the blockchain network, however, and given the immutable and transparent nature of the blockchain, such malicious actors will be deterred when faced with inevitable discovery by the trusted government.

### 5.3 Adoption of the Solution

The proposed solution does not require the invention or engineering and testing of a scalable and reliable framework that includes auditing and integration. The Ethereum blockchain is a tested platform that provides these features by default, reducing the cost of development and maintenance. Our proposal also utilizes existing infrastructure that is already familiar to citizens, the USSD interface.

As a precursor for the move to a Smart Government, Rwanda has invested heavily in the provision of Internet, with 4G coverage available in 95% of the entire country [24]. Indeed, the International Telecommunication Union reports that in 2019, 97% of the world's population lived within range of a mobile phone signal [25]. Rwanda has also automated and delivered selected civil services online through a platform called Irembo for several years [26]. Those who cannot get online directly can do so at a government service center in most villages.

### 5.4 Tradeoffs

Our system is not a genuinely decentralized application, as is typically characteristic of applications built using the blockchain. Our system trades decentralization for ease of governance. We assumed that a government using the system would require centralized control over the process of acquiring a digital national identity. As a result, the system introduces centralization, since the citizen must appear in person before an appropriate government entity for verification and then registration.

For usability reasons, we traded the security of the public-private key pair typically used for interacting with a blockchain application. Due to the introduction of a PIN, citizens have an easier method of authenticating to the application that is consistent with other USSD applications. However, a four-digit PIN is less secure than the cryptographically secure keys typically used by blockchain apps. In the event of a mismanaged identity, such as a PIN that is lost or stolen, our system allows the issuer to block access as soon as it is reported. Rwanda's major

telecom service provider, MTN, established precedent by requiring their users to secure their mobile money wallets with PIN authentication, so this approach to securing sensitive data in a developing country is not untested [27]. Work is underway to enable more novel forms of two-factor authentication, like voice-print technology, which is already being offered by companies like Phonexia [28] and implemented by organizations like Chase Bank [29].

Finally, we traded self-sovereignty, also for ease of governance. Citizens own their identities, but do not have full control over what portions of the data they can share with different entities, as explained in the methodology section. If citizens had full control over their data, they could deny government entities and related trusted third parties legally required information. As a compromise, we introduced the concept of trust zones, so that different categories of entities have different levels of access to citizen's information.

## 6 Conclusion

Citizens in countries with national identification systems require multiple forms of identification to access different civil services like police records or national healthcare. We proposed a blockchain-based national identification that would ensure interoperability among the different government entities and trusted third parties when providing civil services to citizens. Although a significant amount of work has been completed in the area of digital IDs, they do not address the nuances of a digital national identity in a country with low adoption of smartphone technology. We developed and described a proof of concept national ID system appropriate to the context of government service while using the concept of trust zones to retain a measure of self-sovereignty for the citizen.

For the future, we suggest further work on ways of reducing the cost of operating the system, such as off-blockchain storage of data and use of private blockchain networks. Future work could also include improving authentication methods, for example, by using fingerprint or voice-print scanners. Developing further use cases in more detail or a test deployment in a real-world setting would also be logical next steps.

## References

1. ISO: IT security and privacy–a framework for identity management–part 1: terminology and concepts. International Standard ISO/IEC 24760–1:2019(E), ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), Geneva, Switzerland, 2nd Ed, May 2019
2. The Sovrin Foundation: Sovrin: a protocol and token for self-sovereign identity and decentralized trust. White paper, Sovrin Foundation, Provo, Utah, USA, March 2018. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
3. Times Reporter: National ID launch today. The New Times, Online, July 2008. https://www.newtimes.co.rw/section/read/4519. Accessed 05 July 2020

4. Republic of Rwanda: e-service, application for national ID. Irembo. https://irembo.gov.rw/rolportal/en/web/nida/application-for-national-id?menu-highlight=CAT#NIDA.IDAPP. Accessed 05 July 2020
5. Atick, J.J.: The identity ecosystem of Rwanda: a case study of a performant ID system in an African development context. White paper, ID4Africa, Kigali, Rwanda, May 2016. https://www.id4africa.com/2016/files/ID4Africa2016_The_Identity_Ecosystem_of_Rwanda_eBooklet.pdf
6. Khovratovich, D., Law, J.: Sovrin: digital identities in the blockchain era. White paper, Sovrin Foundation, Provo, Utah, USA, December 2016. https://sovrin.org/wp-content/uploads/AnonCred-RWC.pdf
7. El Haddouti, S., Kettani, M.: Analysis of identity management systems using blockchain technology. In: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1–7, Rabat, Morocco, April 2019. https://doi.org/10.1109/COMMNET.2019.8742375
8. Dunphy, P., Petitcolas, F.A.P.: A first look at identity management schemes on the blockchain. IEEE Secur. Priv. **16**(4), 20–29 (2018). https://doi.org/10.1109/MSP.2018.3111247
9. Mudliar, K., Parekh, H., Bhavathankar, P.: A comprehensive integration of national identity with blockchain technology. In: 2018 International Conference on Communication Information and Computing Technology (ICCICT), pp. 1–6. IEEE, IEEE, Mumbai, India, February 2018. https://doi.org/10.1109/ICCICT.2018.8325891
10. Juan, M.D., Andrés, R.P., Rafael, P.M., Gustavo, R.E., Manuel, P.C.: A model for national electronic identity document and authentication mechanism based on blockchain. Int. J. Model. Optim. **8**(3), 160–165 (2018). https://doi.org/10.7763/IJMO.2018.V8.642
11. Wolfond, G.: A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. Technol. Innov. Manage. Rev. **7**(10), 35–40, October 2017. https://doi.org/10.22215/timreview/1112
12. Adepoju, P.: Rwanda's Kagame bemoans country's low smartphone penetration rate. ITWeb Africa, October 2019. http://www.itwebafrica.com/more-countries/rwanda/246560-rwandas-kagame-bemoans-countrys-low-smartphone-penetration-rate. Accessed 06 July 2020
13. MetaMask: a crypto wallet & gateway to blockchain apps. https://metamask.io/. Accessed 06 July 2020
14. Rinkeby.io: Rinkeby: ethereum testnet. https://www.rinkeby.io. Accessed 15 Oct 2020
15. 3rd Generation Partnership Project: digital cellular telecommunications system (phase 2+) (GSM); universal mobile telecommunications system (UMTS); unstructured supplementary service data (USSD); stage 1. Technical Specification 3GPP TS 22.090 version 16.0.0 Release 16, 3rd Generation Partnership Project (3GPP), Sophia Antipolis, France, August 2020. https://www.etsi.org/deliver/etsi_ts/122000_122099/122090/16.00.00_60/ts_122090v160000p.pdf
16. Truffle Blockchain Group: Ganache overview. https://www.trufflesuite.com/docs/ganache/overview. Accessed 05 July 2020
17. Truffle Blockchain Group: Truffle overview. https://www.trufflesuite.com/docs/truffle/overview. Accessed 05 July 2020
18. OpenJS foundation: about node.js. https://nodejs.org/en/about/. Accessed 06 July 2020
19. Ethereum Foundation: Web3.js Ethereum Javascript API. https://web3js.readthedocs.io/en/v1.2.9/. Accessed 06 July 2020

20. Ethereum Foundation: Ethereum is a global, open-source platform for decentralized applications. https://ethereum.org/. Accessed 06 July 2020
21. WHATWG Community: HTML living standard, July 2020. https://html.spec.whatwg.org/multipage/. Accessed 06 July 2020
22. Schäffer, M., di Angelo, M., Salzer, G.: Performance and scalability of private ethereum blockchains. In: Di Ciccio, C., et al. (eds.) BPM 2019. LNBIP, vol. 361, pp. 103–118. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-30429-4_8
23. Africa's Talking: USSD API – build mobile apps accessible everywhere. https://africastalking.com/ussd#pricing. Accessed 06 July 2020
24. Tashobya, A.: Four years later, 95% of Rwanda covered with 4G Internet. The New Times, May 2018. https://www.newtimes.co.rw/news/four-years-later-95-rwanda-covered-4g-internet
25. International Telecommunication Union: Facts and figures 2019: Measuring digital development. Report, International Telecommunication Union (ITU), Geneva, Switzerland (2019). https://itu.foleon.com/itu/measuring-digital-development/home/
26. Government of Rwanda: Smart rwanda 2020 master plan. Report, Government of Rwanda, Kigali, Rwanda, October 2015. https://nyamasheke.gov.rw/fileadmin/templates/DOCUMENT_Z_ABAKOZI/SMART_RWANDA_MASTER_PLAN_FINAL.pdf
27. MTN: MTN mobile money service terms and conditions. Kigali, Rwanda. https://www.mtn.co.rw/wp-content/uploads/2019/11/MOMO-TERMS-CONDITIONS.pdf
28. Phonexia: voice biometrics platform. https://www.phonexia.com/en/product/voice-biometrics/. Accessed 15 Oct 2020
29. JPMorgan Chase & Co.: With voice ID, we can verify you by the sound of your voice. https://www.chase.com/personal/voice-biometrics. Accessed 15 Oct 2020