

Birth Certificates Delivery, Traceability and Authentication Using Blockchain Technology

Tankou Tsomo Maurice Eddy*, Bell Bitjoka Georges, Ngohe Ekam Paul Salomon, Ekani Mebenga Vianney Boniface
Laboratory of Electrical Engineering Mechatronics and Signal Processing ENSPY, University of Yaoundé, Cameroon

Abstract—Now-a-days, the vast majority of birth certificate registration systems are paper-based and managed independently by administrative communities. This means that birth information only exists at the place where the birth is registered, which facilitates the counterfeiting or falsification of such identity documents. Therefore, the implementation of a system for the issuance, traceability, and authentication of birth certificates is imperative. Blockchain, characterized by transparency, immutability, protection, privacy, and autonomy, makes this technology the ideal solution for implementing a birth certificate registration, traceability, and authentication system. This article presents a decentralized system for the registration, traceability, and authentication of birth certificates based on Hyperledger Fabric private blockchain deployed in a Virtual Private Network - Multi-Protocol Label Switching (VPN-MPLS) network. This birth certificate is characterized on one hand by the attributes of its owner and on the other hand by a Quick Response (QR) code containing the digital signature of its signer and the unique identifier of the birth certificate. Within the network, the unique identifier of the generated document is hashed and stored using the Secure Hash Algorithm-256 (SHA-256) hash function to optimize storage space and enhance security. Furthermore, the proposed platform includes an application designed using Docker Compose, Apache CouchDB, NodeJS, Go, and Hyperledger Explorer. The designed model is a birth certificate registration platform that ensures enhanced security and transparency.

Keywords—Birth certificates; blockchain; security; traceability; authentication; counterfeiting; falsification; hyperledger fabric

I. INTRODUCTION

For many decades, centralized architectures have been used in the deployment of network infrastructures. These architectures are characterized by a main server responsible for establishing a direct trust relationship among all network participants [1]. However, this type of architecture has limitations in that the failure of the central server leads to the paralysis of the entire network, and the malfunction of a node causes a break in the communication chain without prior notification to the system's participants [2, 3].

Distributed networks, on the other hand, do not require a single trusted authority. Each node in the network acts as both a client and a server, dynamically discovering and connecting with each other while relaying requests from terminal to terminal. This architecture is robust but requires significant traffic, as searching for a file takes more time. Each request is sent to all connected users, who do the same, which can lead to a long wait for a response to a request if thousands of users are connected [4]. This horizontal chain of trust model is the foundation of blockchain technology. Blockchain is a storage

and transmission technology that operates transparently without a central control body [5, 6].

Document storage techniques are generally carried out within centralized systems. When a modification, deletion, or update is made in this centralized database, it affects the entire system. However, when it comes to a fraudulent act, the entire network is compromised [7, 8]. Considering the advantages of the decentralized model, where any modification, deletion, or update of information requires the approval of at least 51% of the network nodes.

In this article, a decentralized platform based on the Hyperledger Fabric private blockchain for the production, traceability, and authentication of birth certificates is proposed. The smart contract generates a Unique Identification Number (UIN) that identifies the birth certificate. This UIN, along with the identifiers and the digital signature of the civil registrar, is contained in a QR code that is affixed to the birth certificate. To optimize storage space and ensure security, this UIN is hashed using the SHA-256 hashing function. To verify the authenticity of a birth certificate, the hash of the UIN scanned via the QR code is compared with the one stored in the blockchain database; if they match, authenticity is guaranteed; otherwise, it is compromised.

The remainder of the document is organized as follows: Section II focuses on general knowledge. In Section III, the related work is presented. Section IV deals with the research method. Section V presents the results and discussions. Finally, conclusions and future work are addressed.

II. BACKGROUND

This section presents general knowledge on the main concepts addressed in this article. The primary objective of this section is to facilitate the understanding of the key concepts used. The following outlines represent the subsections:

A. Blockchain

1) *Definition of blockchain*: A blockchain is a secure and decentralized distributed ledger technology. It is best known for its role in cryptocurrency systems to maintain a secure and decentralized record of transactions, but it also has many other potential applications. It is a chain of blocks, where each block contains a timestamp, transaction data, and a cryptographic hash of the previous block. This hash is a unique digital fingerprint that links the blocks together and makes it very difficult to tamper with the data. When a new transaction is made, it is broadcast to the network of computers that manage the blockchain. These computers verify the transaction and add

it to a new block. Once the new block is created, it is added to the end of the chain. This process is continuously repeated, creating an ever-growing chain of blocks that is constantly verified and updated. Thus, the blockchain is a very secure and tamper-proof record of transactions [9-13].

2) *Blockchain characteristics*: Blockchain technology has several key features that make it unique and valuable for various applications. [14]:

a) *Immutability*: Once data is recorded on a blockchain, it cannot be altered or deleted. This ensures a permanent and tamper-proof record of transactions.

b) *Decentralization*: A blockchain operates on a decentralized network of nodes, eliminating the need for a central authority. This enhances security and reduces the risk of single points of failure.

c) *Transparency*: All participants in the network have access to the same data, promoting transparency and trust. Every transaction is visible to all nodes, ensuring accountability.

d) *Security*: Blockchain employs cryptographic techniques to secure data. Each block is linked to the previous one by a cryptographic hash, making it extremely difficult to modify data without detection.

e) *Consensus mechanisms*: Blockchains rely on consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Authority (PoA), to validate transactions and maintain the integrity of the ledger.

f) *Distributed ledger*: The ledger is distributed across all nodes in the network, ensuring that all participants have an up-to-date copy of the data. This distribution enhances reliability and reduces the risk of data loss.

g) *Smart contracts*: These are self-executing contracts with the terms of the agreement directly written into lines of code. They automatically execute the agreement when predetermined conditions are met, reducing the need for intermediaries.

3) *Blockchain Applications*: Blockchain technology has a wide range of applications across various industries. Here are a few examples:

a) *Finance*: Blockchain enhances the security, transparency, and efficiency of financial transactions. It is used for cross-border payments, smart contracts, and decentralized finance (DeFi) applications [15].

b) *Healthcare*: Blockchain can securely store patient records, ensuring data integrity and confidentiality. It also facilitates the sharing of medical data among various healthcare providers [16, 17].

c) *Supply chain management*: Blockchain ensures the transparency and traceability of supply chains, helping to track the origin and journey of products, which is crucial for quality control and fraud prevention [18, 19].

d) *Real estate*: Blockchain can streamline real estate transactions by reducing paperwork and enabling secure,

transparent, and tamper-proof records of property ownership and history [20].

e) *Voting systems*: Blockchain can be used to create secure and transparent voting systems, reducing the risk of fraud and ensuring the integrity of election results [21].

f) *Digital identity*: Blockchain can provide secure and verifiable digital identities that can be used for various purposes, including online authentication and Know Your Customer (KYC) processes [22].

g) *Intellectual property*: Blockchain can protect intellectual property rights by providing a secure and immutable record of ownership and creation [23].

h) *Internet of Things (IoT)*: Blockchain can improve the security and efficiency of IoT [24].

i) Blockchain technology offers numerous advantages across various sectors. Some of the key benefits include:

j) *Enhanced security*: Blockchain uses advanced cryptographic techniques to secure data. Each transaction is encrypted and linked to the previous one, making it extremely difficult for unauthorized parties to modify data [25, 26].

k) *Greater transparency*: As blockchain operates on a decentralized network, all participants have access to the same data. This transparency ensures that all transactions are visible and verifiable by all network members.

l) *Improved traceability*: Blockchain creates an immutable record of transactions, which is particularly useful in supply chains. It allows for tracking products from their origin to their final destination, reducing the risk of fraud and ensuring authenticity.

m) *Increased efficiency and speed*: By eliminating intermediaries and automating processes through smart contracts, blockchain can significantly speed up transactions and reduce the time required for various operations.

n) *Reduced costs*: Blockchain can reduce costs by eliminating the need for third-party intermediaries and reducing the amount of paperwork and administrative tasks required.

o) *Decentralization*: The decentralized nature of blockchain means there is no single point of failure. This enhances the system's resilience and reduces the risk of data loss or corruption.

p) *Improved privacy*: Blockchain can enhance privacy by allowing users to control their account data.

4) *Blockchain typology*: There are three main types of blockchain:

a) *Public blockchain*: A public blockchain allows transactions to be recorded and validated by the entire network. This type of blockchain can be compared to a tamper-proof ledger maintained by all its participants. A public blockchain is a decentralized network that operates on a peer-to-peer basis. Peer-to-peer means exchanging between two actors without an intermediary through a relationship of trust.

b) *Private blockchain*: In contrast to a public blockchain, a blockchain is considered private if the consensus principle is verified by a limited and predefined number of participants. The

ability to participate in transactions is defined by an organization, as is the verification work [27].

c) *Consortium blockchain*: A consortium blockchain brings together several private actors who have an interest in working together. Decisions (block validations) are made by the majority of the most important members and not by the entire network as in a public blockchain. Only the decision-makers can verify the validity of the blocks [28].

5) *Hyperledger fabric*: Hyperledger Fabric is an open-source private blockchain platform developed by the Linux Foundation and IBM. Unlike Bitcoin and Ethereum, it does not require a virtual currency, the consensus is open, and smart contracts can be written in multiple programming languages including Go, Java, Python, etc., with tokenization through smart contracts [29]. The particularity of this technology lies mainly in the fact that, depending on the information, transactions can be viewed by everyone (public) or restricted to a group of organizations (confidential). It allows for the deployment of blockchain applications.

A Hyperledger Fabric blockchain network is composed of several nodes or peers, which host the blockchain and execute smart contracts, or chaincode. These smart contracts are executed by the peers of the network specific to a group of organizations and are inaccessible to members who are not part of that organization. Thanks to channels in Fabric, all smart contracts and data are only accessible to members who are part of the channel.

In addition to the network peers, a Fabric network can include an ordering service/ordered that performs the total ordering of transactions accepted by the Fabric network.

As for smart contracts, they are executed in a Docker container, in order to isolate them from the Fabric code and other smart contracts running on the same machine. Each smart contract has a persistent state called a key-value store [30].

Smart contracts manipulate key-value pairs using the put and get methods, which allow reading from the key-value store. These key-values are stored internally in a Level DB database on the same node, and CouchDB is used for the implementation of the database. This database allows storing key-value pairs [31-34].

In Hyperledger Fabric, a transaction goes through the following steps:

- Client proposes the transaction: This transaction is a request to invoke a smart contract. The request is signed by the client and sent to the channel where the chaincode is deployed. The number of endorsements it expects to receive is in accordance with the chaincodes endorsement policy.
- Endorsing peers verify the signature and execute the transaction: Peers verify the authenticity, form, replay protection, and client authorization.
- The client collects endorsements and sends them to the ordering service: The client examines and compares all endorsements and verifies that they meet the criteria

defined in the smart contract. If the request is a read-only type, no request is sent to the ordering service. If the request is a smart contract invocation or write request, the endorsements are gathered into a transaction and sent to the ordering service which, in turn, includes it in the blockchain. The transaction is validated and recorded: The transactions ordered in the blocks are transmitted to all peers on the organization's channel via the ordering service. Peers perform a verification of the transaction and apply the endorsement policy by the endorsing peers. If all verifications are successful, the endorsing peers add the block to the distributed ledger.

6) *Birth certificate*: A birth certificate is a legal document that proves a person's civil status. Indeed, a birth certificate contains the name, first name(s), date, time, and place of birth, etc. A birth certificate is used to prove one's identity and family status.

However, the procedure for obtaining one is governed by a law that varies from country to country. For many years, birth certificates were produced manually by the responsible parties. The complexity, the burden, and the falsification or fraud in the establishment process have motivated the migration towards the digitalization of birth certificates. The completed birth certificate form is then recorded in a central or non-central database. One of the limitations of the vertical trust chain is that the central node can be compromised. Moreover, the administrations in charge of certification do not have a means of authenticating certificates produced at the time of their certification.

III. LITERATURE REVIEW

The secure production of birth certificates is paramount for both individuals and the organizations that interact with them. There is a risk of fraudulent activities within these databases, and the authorities responsible for authenticating birth certificates may not be able to verify in real-time the identity of the person who produced a given document. Falsification can involve altering the date of birth to appear younger or older, changing the names of the parents, the place of birth, etc. Table I refers to the most recent literature review.

In [35], the authors study the cumbersome procedures caused by the manual registration of births and deaths, and they propose a decentralized, simplified, and transparent application based on the Ethereum blockchain, guaranteeing immutability and providing the true and irrefutable origin of records. However, a problem arises with the consensus algorithm due to the slowness of the transaction verification system, compromising availability, and high energy consumption, leading to economic and environmental issues. Furthermore, less developed chains are highly susceptible to 51% attacks.

In [36], the authors propose a traceable online will system based on the Ethereum blockchain and smart contract technology to address the issues of complexity, falsification, slowness, and high cost in the establishment of wills. To this end, they propose a traceable online will system integrating an arbitration strategy in case of disputes based on blockchain technology. The main problems lie in the flaw in the consensus

algorithm used, which is proof of work, and the solution is energy-intensive.

TABLE I. SYSTEMATIC LITERATURE REVIEW

Authors (Year)	Model+Applications	Advantages	Disadvantages
Shah et al., (2020) [35]	Ethereum-based, simplified and transparent application for birth and death registration	Accelerated registration processes	Slow system, susceptible to 51% attacks, energy-intensive
Chen et al., (2021)[36]	Ethereum-based online will creation and storage system	Traceability of wills, accelerated processes, simplified procedures, reduced costs	System complexity, slow system, susceptible to 51% attacks, energy-intensive
Okoth et al.,(2023) [37]	Centralized architecture-based security policy for civil registration systems	Data confidentiality and access control	Failure of the central node paralyzes the entire system
Danquah et al., (2022) [38]	Ethereum-based platform for birth registration	Accelerated birth registration process	Lack of experimental data
Sharma et al., (2020) [39]	Ethereum and blockcerts-based application for issuing birth certificates	Simplified birth certificate acquisition process	Monetization of generated transactions, system complexity, slow system, susceptible to 51% attacks, energy-intensive
Bennett et al., (2022) [40]	Ethereum and Corda-based application for birth registration and certificate issuance	Simplified birth registration and certificate issuance process	Incompatibility with existing systems

The author in [37] presents the security vulnerabilities faced by civil registration systems, compromising the integrity and confidentiality of information. Moreover, the digitalization of civil records is accompanied by multiple threats related to cyber threats, and malicious actors can compromise the security of the database to manipulate or steal civil records. Cybersecurity measures such as encryption, firewalls, intrusion detection systems, and regular security audits can protect data and ensure the continuity of civil registration operations. The limitation of this approach is the use of a centralized architecture.

The author in [38] presents a statistic that approximately one-third of births are not registered. The proposal of a model aims to improve the birth registration process. The platform is based on Ethereum technology, which uses an energy-intensive consensus. Additionally, an experimental study could be conducted to confirm the validity of the processes described in the study.

Another author in [39] mentions that half of the world's population faces a problem with the complexity of the procedure for obtaining a birth certificate, and the authentication of these certificates is tedious. The Ethereum

blockchain coupled with blockcerts is used to issue and verify a transaction. A major difficulty in using blockcert technology lies in the monetization of generated transactions. Other authors mention that civil registry data mostly exists in paper form, which can differ from one place to another without any form of interoperability within the same country, consequently increasing the falsification of birth certificates since information about births only exists where the birth is registered. A system for registering births and issuing certificates, storing a digital copy of the certificate, and verifying the validity of the certificate is proposed using the private blockchain Corda. The major difficulty of this blockchain lies in its difficulty of integration into existing information systems, and the lack of documentation on the technology is an obstacle to the development of the Corda community [40].

IV. METHODOLOGY

The primary objective of the literature review is to identify, evaluate, and analyze existing research related to the production of birth certificates. In this section, the research question, the research methods aimed at reducing fraud in the birth certificate issuance process, and the gap observed in the authentication process of these certificates by the responsible organizations are presented.

Initially, an algorithmic method is used to write smart contracts that are subject to prior verification by certain peer approvers within the network. The cryptographic method, which relies on asymmetric cryptography, such as RSA encryption and electronic signatures, is also employed. Finally, a virtual simulation method based on containerization (Docker) is used to create network nodes, define the protocol, and the consensus algorithm.

A. Valuable Research Questions

This article aims to develop a blockchain-based system for issuing, tracking, and authenticating birth certificates, ensuring traceability between products from the operational birth certificate from the production facility and the actors involved in their creation without compromising confidentiality due to transparency.

B. Research Methods

1) *Network architecture:* The agglomerations are interconnected via VPN/MPLS links over an operator network whose backbone is based on MPLS technology. The specificity of MPLS lies in label switching along the path that packets must take to reach the destination network. Since the path is predetermined, routers only need to read the label and do not need to check the packet's IP address. This allows for faster and more efficient routing. Additionally, to enhance VPN security, the IPsec protocol is a complement, as it is widely deployed to restrict access or selectively apply security operations in VPN implementations.

As illustrated in Fig. 1, the edge routers of each agglomeration have interfaces addressed on the operator side with public addresses and on the side of internal local networks with private addresses. In the firewalls, access control lists are

configured to filter incoming and outgoing packets to the different networks. The interfaces of the switch connected to the firewall are in different VLANs from the local network VLANs for added security. In each internal network, workstations of decentralized territorial authorities (town halls, civil registry offices, prefectures, sub-prefectures) are connected. The operator network is represented by a cloud due to the security policy.

Fig. 1 presents the network architecture interconnecting 10 agglomerations.

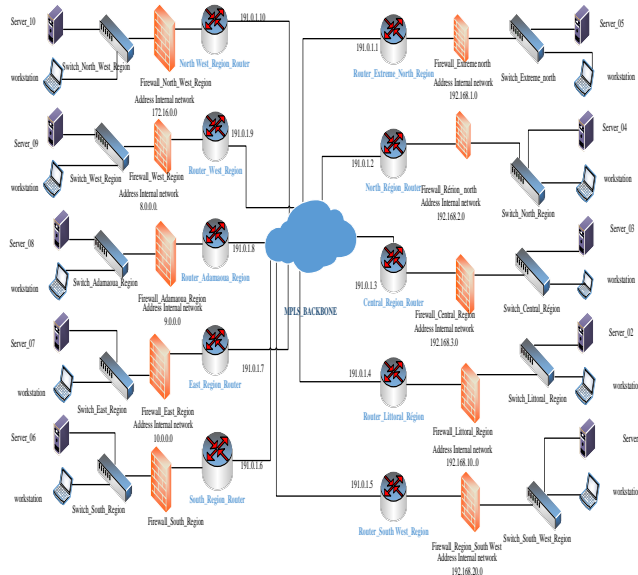


Fig. 1. Physical network architecture of the proposed solution.

2) *Smart contract specifications:* In this section, the technical specifications of the smart contract for document registration and verification, ensuring immutability and transparency are presented. Developed in Golang due to its simplicity, performance, compatibility with the Hyperledger Fabric blockchain platform, and extensibility, the smart contract offers high performance and efficient concurrent management, making birth certificate management reliable and secure. These specifications cover registration and verification, node transaction approval, transparency and traceability, security, compatibility and extensibility, architecture, and data structure.

C. Registration and Verification

The smart contract incorporates several technical features to ensure optimal and secure management of birth certificate documents:

1) *JSON serialization:* Documents are serialized into JSON format for easy storage and manipulation on the blockchain.

2) *Authenticity:* When a birth certificate is submitted to the network, the smart contract verifies its authenticity. A digital fingerprint of the document is then generated and recorded on the blockchain, ensuring data integrity and immutability.

D. Transaction Approval

The smart contract is deployed across multiple nodes in the blockchain network. This decentralized approach ensures an equitable distribution of responsibilities and enhances system security. Additionally, transaction validation is contingent upon approval from all validating nodes in the network.

E. Transparency and Traceability

Every interaction with the smart contract is time-stamped and recorded on the blockchain, creating an immutable audit trail. This enables full traceability of document lifecycle events, from creation to deletion, and facilitates compliance with regulatory requirements.

1) *Action logging:* Each interaction with the smart contract, including the creation, update, and deletion of documents, is recorded on the blockchain. This comprehensive audit trail ensures full transparency and accountability.

F. Security

The smart contract is deployed across multiple nodes of the blockchain network. This decentralized approach ensures an equitable distribution of responsibilities and enhances system security. Additionally, transaction validation requires the approval of all validating nodes within the network.

G. Cryptographic Method

RSA asymmetric cryptography is used to generate public and private key pairs, as well as digital signatures to ensure the authenticity and integrity of transactions. The public key must be shared with others to receive birth certificate data. The private key is used to sign the transactions within the platform. The key generation process is as follows: [41]

- Choose two distinct, large prime numbers p and q ;
- Calculate their product $n = p \times q$ which is called the encryption modulus;
- Calculate $\phi(n) = (p - 1)(q - 1)$ which is Euler's totient function;
- Choose an encryption exponent e such that the greatest common divisor (GCD) of $(e, \phi(n)) = 1$ i.e., they are coprime;
- Calculate the multiplicative inverse d of e modulo $\phi(n)$ using the extended Euclidean algorithm
 - $d \times e \equiv 1 \text{ modulo } \phi(n)$;
- The public key is the pair (n, e) , and the private key is d , which must be kept confidential.

H. Data Security

Blockchain data is immutable and resistant to unauthorized modification or disclosure.

I. The System Architecture

The smart contract architecture is designed to maximize efficiency, security, and transparency in managing birth certificate documents. The key components of this architecture are:

1) Imported packages:

- *Encoding/json*: Used for JSON data manipulation, allowing for easy serialization and deserialization of documents;
- *Fmt*: Used for input and output formatting, facilitating debugging and maintenance.
- *Time*: Used for date and time management, crucial for time-stamped records;
- *github.com/hyperledger/fabric/core/chaincode/shim*: Used for interactions with the Hyperledger Fabric framework, allowing the smart contract to communicate with the blockchain;
- *github.com/hyperledger/fabric/protos/peer*: Used for protocol definitions, ensuring compatibility with Hyperledger Fabric blockchain standards.

2) *Data Structures*: The smart contract's data structures are designed to provide a granular representation of birth certificates. The following outlines the data structure for birth registration and the resulting birth certificate.

- *BirthRegistration*: a data structure defining the attributes of a birth registration, such as child's information, parental details, and registration metadata.

BirthRegistration struct type {

```
Number    string `json:"N°"`
Type      string `json:" Document type"`
Registration string `json:" Registration designation"`
The       string `json:"Registration date"`
At        string `json:"Registration place"`
Hour      string `json:"Registration hour"`
Surname:  string `json:"Child's surname (s) "`
Name      string `json:" Child's name (s) "`
Sex       string `json:"Child's sex "`
Of0       string `json:"Father's name "`
Sur0      string `json:"Father's surname "`
BornOn0   string `json:"Father's date of birth "`
BornAt    string `json:"Father's place of birth "`
Job       string `json:"Father's job "`
IdCartP   string `json:"Father's Id cart "`
Of1       string `json:"Mother's name "`
Pre1      string `json:"Mother's surname "`
BornOn1   string `json:"Mother's date of birth "`
BornAt    string `json:"Mother's place of birth "`
Job2      string `json:" Mother's job "`
Dom       string `json:"Parents' residences "`
SM        string `json:"Marital status of the parents "`
IdCartP   string `json:"Mother's ID card "`
City      string `json:"City where the declaration was made "`
Tem       string `json:"Witnesses "`
DECDate   string `json:"Date of the declaration "`
Signature of the declarant string `json:"Signature "`
Signatory string `json:"Signatory of the declaration "`
```

```
NumCNIDEC    string `json:"Declarant's national identity card number "`
ProfDEC      string `json:"Declarant's job "`
DateENREG    time.Time `json:"Date of definitive registration "`
}
```

- *Birth certificate*: A legal document detailing the birth of a child, including the child's name, date and place of birth, gender, as well as the parents' names, dates and places of birth, nationalities, addresses, and occupations, and any associated declarations.

Type of birth certificate struct {

```
Number    string `json:"N° "`
Type      string `json:"Type of document "`
PROVINCE  string `json:"PROVINCE "`
DEPARTMENT string `json:"DÉPARTMENT "`
BOROUGH   string `json:" BOROUGH "`
At        string `json:"De "`
Child's surname (s) string `json:"Child's surname (s) "`
Child's name (s) string `json:"Child's name (s) "`
Was born   string `json:"Birthplace "`
The        string `json:"Date of birth "`
Sex        string `json:" Child sex "`
At0        string `json:"Nom du père "`
NeLe0     string `json:"Father's date of birth "`
NeA       string `json:"Father's place of birth "`
Natio0    string `json:"Father's Nationality "`
Residences A string `json:"Parents' residences "`
Job        string `json:"Father's job "`
At1       string `json:"Mother's name "`
The1      string `json:"Mother's date of birth "`
Born in   string `json:"Mother's place of birth "`
Natio1    string `json:"Mother's nationality "`
Residences string `json:"Mother's residences "`
Job2      string `json:"Profession de la mère "`
Declaration of string `json:"On the declaration of "`
By us     string `json:"By us "`
Center    string `json:"Registering officer of "`
Assisted by string `json:"Assisted by "`
Civil registrar's signature string `json:" Civil registrar's signature "`
DEC Number    string `json:"Original birth certificate number "`
Dated         time.Time `json:"Dated "`
```

3) Main Functions:

- *Initialization Function (Init)*: Initializes the smart contract. It requires no input parameters and returns a success response if the initialization is successful.
- *Invocation Function (Invoke)*: Routes the request to the appropriate function based on the invoked method's name. It requires the parameters stub, function, args as input and returns the response of the invoked method as output Fig. 1.

4) Functions of a Birth Certificate:

- Create Birth Certificate: Creates a new birth certificate. As input, it requires an array of 29 strings representing the details of the birth certificate and returns a success response if the birth certificate is successfully created.
- Retrieve Birth Certificate: Retrieves a birth certificate by its unique number. As input, it takes an array with one string (the unique number) and returns the details of the birth certificate if found.
- Consult All Birth Certificates: Retrieves all birth certificates. As input,

5) Functions of a birth certificate

- CreateBirthCertificate: Creates a new birth certificate. As input, it takes an array of strings representing the birth details (name, date of birth, place of birth, parents' names, etc.) and returns the unique identifier of the newly created certificate.
- RetrieveBirthCertificate: Retrieves a birth certificate based on its unique identifier. As input, it takes a string representing the unique identifier and returns an array of strings containing the birth certificate details.
- ListAllBirthCertificates: Lists all birth certificates. It doesn't require any input parameters and returns a list of all birth certificates in JSON format.

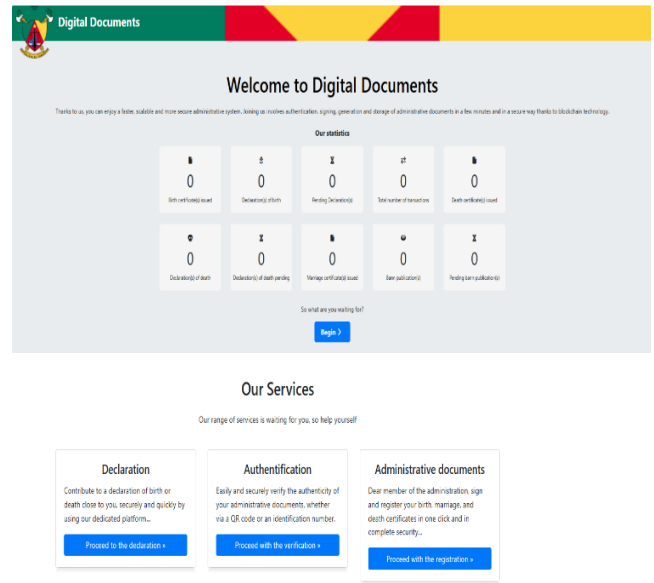


Fig. 3. Government portal homepage.

To enhance traceability and accountability, we recommend the following roles:

Healthcare professional: Verifies births and submits declarations to approving nodes.

Civil registrar: Creates and digitally signs birth certificates.

After a healthcare professional's profile is created, they submit a birth declaration for approval (Fig. 4). The declaration includes a QR code with a unique identifier, the signatory's name, and ID number. It contains details such as...

Establishment name: This is the name of the hospital that issued the birth certificate;

Child's name and surname: This is the first name and last name of the infant;

Date of birth: This refers to the date the baby was born;

Place of birth: This is the location where the baby was born;

Gender: This refers to the sex, in this case, male.

Subsequent to the infant's details, we have the following parental information:

Name and surname of father: Father's full name;

Father's occupation: Father's profession;

Father's date of birth: Father's date of birth;

Father's place of birth: Father's place of birth;

Father's Id card number: Father's national ID number;

Mother's full name: Mother's full name;

Mother's occupation: Mother's profession;

Mother's date of birth: Mother's date of birth;

Mother's place of birth: Mother's place of birth;

Mother's ID card number: Mother's national ID number;

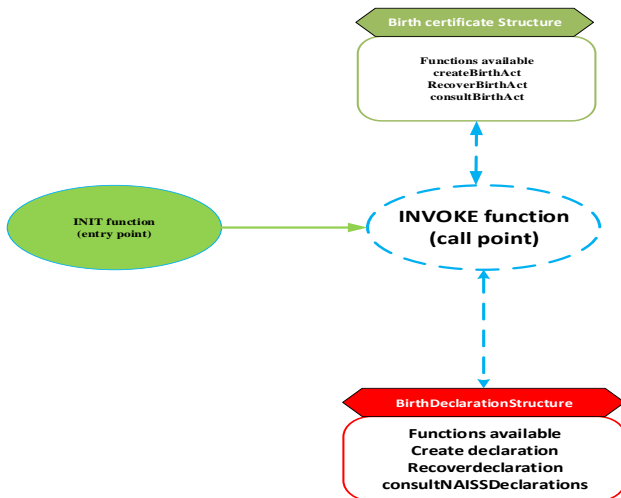


Fig. 2. Components of a smart contract.

V. RESULTS AND DISCUSSION

In this part, the effectiveness of the methodology outlined in the preceding section is demonstrated. Through a series of tests, the performance of birth certificate registration, authentication processes, and the generation of birth declaration statistics are evaluated. To accomplish this, the capabilities of the Hyperledger Fabric private blockchain platform are leverage. Fig. 3 showcases the user interface of the government portal specifically designed for civil registry and authentication. This portal facilitates the creation, verification, and statistical analysis of civil status records, providing granular data at weekly, monthly, and annual levels, segmented by region.

Parent's address: Parents' address;

Marital status: Marital status. In this case, the parents are married.

Subsequent to the parental data, the registrar's information is provided:

Name and surname of the declarant: Dota Paul;

Profession: Healthcare professionals;

ID card number;

Place and date of the declaration: [Location], on [Date] at [Time];

Birth declaration

Name of the establishment : Central hospital

Name and surname of child : TANKOU KENGNE Yoan kylian

Date of birth : 2020-02-22 à 14:46

Place of birth : Douala

Gender : masculin

Information about the parents :

Name and surname of father : TANKOU EDDY

Father's occupation : Computer sciences

Father's date of birth : 1994-06-22

Father's place of birth : DOUALA

Father's CNI number : 1010247569

Mother's full name : Kengne_steva

Mother's occupation : computer sciences

Mother's date of birth : 1999-08-22

Mother's place of birth : Douala

Mother's CNI number : 1145239

Parents address : yaounde,Douala

Marital status : Mariés

Information about the declarant :

Name and surname of the declarant : Dota Paul

Declarant's profession : médecin

CNI number : 102042759

Done at : Yaounde

On : 22-07-2024 à 13:54


Signature of declarant : 

Fig. 4. Birth certificate.

Finally, there is the QR code, which is a type of two-dimensional barcode typically composed of square modules arranged in a square on a white background. It contains the unique identification number (UIN), the name of the document signer, and their national identity card number. Additionally, this QR code generated on the form bears the signature of the civil registrar, allowing for verification of the signer and the document's author. This signature incorporates the SHA-256 cryptographic hash function, which generates a unique 64-character hexadecimal hash for each block of transactional data.

The security of the forms primarily relies on a UIN (unique identification number) designed using a pseudorandom number generator. At the end of the declaration form completion process, a UIN issued by the aforementioned function serves as a unique identifier for each document.

This cryptographic hash function dates back to 2001 and originated from the NSA (National Security Agency). It is increasingly used in blockchain technology today due to its high level of security. Furthermore, its algorithm is undeniably complex, as the generation of a SHA-256 hash requires a highly sophisticated binary calculation, utilizing several compression functions (addition, substitution, and rotations). Ultimately, it relies on the Merkle tree to provide a reliable guarantee of the integrity of the manipulated data.

Once the birth declaration is established, a user account is created for the civil registrar to finalize the birth certificate issuance process. The civil registrar profile is authorized to issue civil status acts. Additionally, the national identity card number entered during account creation uniquely identifies the civil registrar within the platform. Once the user account is created, it is hashed using the SHA-256-bit hash function and stored in the distributed node database for strong authentication. Thus, during account authentication, the account hash is compared to the hash stored in the database; if there is a match, the authenticity of the account owner is guaranteed.

The civil registrar logs into the platform using these created user account parameters and finalizes the birth certificate issuance process. Fig. 5 illustrates this process.

Creation Process Conclusion Form
Declaration of birth:DD8379173725218346

Finalization of the birth certificate

Province	Department
<input type="text" value="CENTER"/>	<input type="text" value="MFOUNDI"/>
District	From
<input type="text" value="Yaounde"/>	<input type="text" value="4"/>
Under-reporting	
<input type="text" value="PITTER JOHN"/>	
By us	
<input type="text" value="MAMA BELLO"/>	
Center	Assisted by
<input type="text" value="CENTER 4"/>	<input type="text" value="MAMA ROSE"/>
Linked birth declaration	
<input type="text" value="DD8379173725218346"/>	
<input type="button" value="Generate the birth certificate"/>	
Dashboard	

Fig. 5. Birth certificate finalization form.

When the finalization form is opened, the civil registrar completes the missing fields and generates the final act. They perform the final checks on the document and submit the transaction via the API (Application Programming Interface) to the network for consensus. All nodes with a copy of the smart contract execute the transaction, approve it, and return the result to the API. In turn, the API sends it to the scheduling service,

which hashes the transaction and generates the block. Having only one transaction per block in the Hyperledger Fabric platform makes it faster compared to the Ethereum blockchain. Fig. 6 shows the generated birth certificate.

The left figure represents the previously established birth declaration, and the right figure represents the birth certificate finalization form corresponding to the previously established birth declaration. On this right-hand form, there are the following information: Province: the province where the birth certificate is issued; Department: the department where the certificate is issued; District: the district where the certificate is issued, as well as the district number, which is 4; Sub-declaration: the name of the person who establishes the act; By us: it represents the name of the civil registrar who signs the birth certificate, in the locality of the center and the district of Yaoundé 4; Assisted by: represents the civil registrar's secretary who assisted the civil registrar in this process; Linked birth declaration: is the UIN generated on the previously established birth declaration, this number links the birth declaration to a birth certificate and is not modifiable.

The civil registrar finally generates the birth certificate transaction and redirects us to the interface allowing us to view the transaction identifiers of the birth declaration and the corresponding birth certificate issuance in the blockchain. A SHA-256-bit hash function is finally generated and stored in the distributed node database for strong authentication. Thus, during document authentication, the document hash is compared to the hash stored in the database; if there is a match, the authenticity is guaranteed.

In a blockchain context, each actor who wants to interact with the network needs an identity. In this context, one or more certification authorities can be used to define the members of an organization from a digital perspective. It is the certification authority that provides the basis for actors in an organization to have a verifiable identity.

Hyperledger Fabric provides a built-in certification authority component to enable the creation of certification authorities in formed blockchain networks. This component, called Fabric CA, is a private root certification authority provider capable of managing the digital identities of Fabric participants in the form of X.509 certificates.

In the operational platform for producing birth certificate forms, an X node acts as the root certification authority (Fabric_CA), and the intermediate certification authorities are the local servers with respective users (Fabric client) being hospitals and community users.

Certificates are generated offline by the root certification authority (X). Once these certificates are created, they are securely distributed to the intermediate certification authorities, which in turn issue certificates to the platform users, namely hospitals, health centers, and communities.

To evaluate the performance of the root certification authority, the SCP protocol via SSH (Secure Copy Protocol) allows us to develop a bash script that runs intermittently to ensure high data availability in case of failure of the main root_CA for each organization. This SCP protocol allows the

copying of information from a root_CA1 to a root_CA2 every three seconds (3s) through a bash script [42].

The civil registrar profile is authorized to establish birth certificates. Furthermore, the national identity card number provided during account creation uniquely identifies the civil registrar within the platform.

Once the user account is created, it is hashed using the SHA-256-bit hashing function and stored in the distributed database of nodes for strong authentication purposes. Thus, during account authentication, the hash of the account is compared to the hash stored in the database; if there is a match, the authenticity of the account holder is guaranteed.

On this birth certificate (Fig. 7), there are the following information:

Birth certificate number: A unique identifier characterized by the initials of the locality that issued the certificate.

Province: The province where the birth certificate was issued.

Department: The department where the certificate was issued.

District: The district where the certificate was issued, specifically District number 4.

Name and surname of child: The given name(s) and surname of the newborn.

Place of birth: The location where the newborn was born.

Date of birth: The date and time of the newborn's birth.

Gender: The sex of the child, in this case, male.

Of: The given name and surname of the newborn's father.

Born on: The date of birth of the newborn's father.

At: The place of birth of the newborn's father.

Nationality: The nationality of the newborn's father.

Resident at: The residence of the newborn's father.

Occupation: The profession of the newborn's father.

By us: The name of the civil registrar who issued the certificate.

Under declaration of: The person who assisted the civil registrar in this process.

Office: The district of the locality and the number associated with that district in that locality.

Assisted by: The name of the civil registrar's secretary who assisted in the issuance of the birth certificate.

The QR code contains a unique identification number (NIU), the name of the document signer, and their national identity card number. This QR code is a type of two-dimensional barcode typically composed of black square modules arranged in a square on a white background, encoding the unique identification number (NIU), the name of the document signer, and their national identity card number.

Additionally, the QR code generated on the form bears the signature of the civil registrar, allowing for verification of the signer and the document's author. This signature incorporates the SHA-256 cryptographic hash function, which generates a unique 64-character hexadecimal hash for each block of transactional data.

The security of the forms initially relies on a NIU (unique identification number generated using a pseudo-random number generator). At the end of the declaration form completion process, a NIU issued by the aforementioned function serves as a unique identifier for each document. This cryptographic hash function dates back to 2001 and originated from the National Security Agency (NSA). It is now increasingly used in blockchain technology due to its high level of security. Furthermore, its algorithm is undeniably complex as the generation of a SHA-256 hash requires a sophisticated binary calculation, employing various compression functions (addition, substitution, and rotations). Ultimately, it relies on the Merkle tree to provide a reliable guarantee of the integrity of the manipulated data.

All data contained in the act is hashed using the SHA-256 hash function. The resulting hash is signed by the civil registrar using their private key. The obtained signature is finally recorded in the QR code.

On the generated birth certificate, all contained data is hashed using the SHA-256 hash function. The resulting hash is signed by the civil registrar using their private key. The obtained signature is finally recorded in the QR code. Fig. 8 illustrates this solution.

The details of the block containing the transaction are shown in Fig. 6.

Fig. 8 provides an experimental history of the number of blocks generated per hour. The figure visualizes the hourly and minutely block count over time. In terms of scalability, measured by the number of transactions processed per unit of time, this work demonstrates approximately 3500 transactions per second on the Hyperledger Fabric blockchain, compared to 38 transactions per second on the Ethereum platform referenced in the literature. This exponential increase in transaction processing speed makes the proposed platform a suitable solution for the digitalization of birth certificates in localities with multiple civil registry centers, including secondary centers and affiliated civil registry offices.

A. Comparison of Works with those of Other Authors

Table II compares the proposed scheme with those of previous studies to identify both areas of convergence and the unique contributions of this research.

Block Details	
Channel name:	canaladministration
Block Number	5
Created at	2024-07-22T14:32:24.622Z
Number of Transactions	1
Block Hash	6274c70f346bc417c3d4233742e82d4e2129a8bef8daf071e63c565cb231289
Data Hash	face743927dfc9a87ab76f0731caadbe0b827a0d9742f3bcb22779da8d3bcf9
Prehash	090916e483ff51890c364d5d50081180d03a08e70f0192cccc132931113145b1e

Fig. 6. Details of the transaction block.

Birth certificate

N° : DD2627025445930364

Province : CENTER

Department : MFOUNDI

Arrondissement : Yaounde

From : 4

Child's full name : TANKOU KENGNE Yoan kylian

Born in : Douala

On : 2020-02-22

Gender : masculin

Of : TANKOU EDDY

Born on : 1994-06-22

at : DOUALA

Nationality : cameroon

Resident at : yaounde

Occupation : Computer sciences

And of : Kengne steva

Born on : 1999-06-22

at : Douala

Nationality : Cameroon

Resident at : Douala

Occupation : computer sciences

By us : MAMA BELLO

Under declaration of : PITTER JOHN

Office : CENTER 4

Assisted by : MAMA ROSE

Signature of officer :



Fig. 7. Birth certificate.

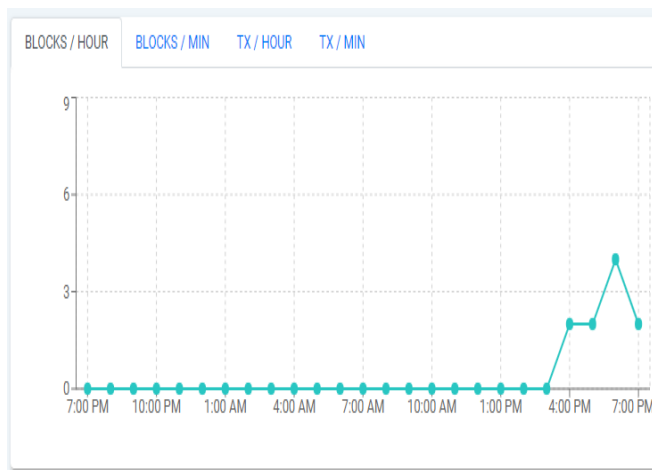


Fig. 8. Hourly blockchain statistics.

TABLE II. COMPARISON OF WORKS WITH RECENT LITERATURE

Criteria		Authors	Proposals	Shah, et al. [14]	Mthethwa, et al. [43]	Thamrin, et al. [44]	Shi, et al. [38]
Energy consumption			—	+++	—	+++	+++
Blockchain	Blockchain type		Private	Public	Public	Public	Public
	Technology used		Hyperledger fabric	Ethereum	Ethereum	Ethereum	Ethereum
Security features	Unique ID for civil status documents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	QR code on a civil registry form	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Transaction ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Digital signature on civil status documents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SHA-256	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Consensus	Open	Closed	<input checked="" type="checkbox"/>	Closed	Closed	Closed
	Data privacy in channels	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Functionality	Birth certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Death certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Marriage banns publication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Birth record establishment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Death record establishment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Marriage record establishment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Scalability (Transactions per second)		3500	38 [45, 46]	<input checked="" type="checkbox"/>	38 Berné [45] [46]	38 Berné [45] [46]	
Mining		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Evolvability		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Distributed architecture		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
License (open source)		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
From a demographic standpoint		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

This section benchmarks the results obtained against existing literature to elucidate both shared insights and the original contributions to the field.

Legend: The symbol "

Until 2021, the Ethereum platform used the Proof of Work (PoW) consensus mechanism. This mechanism had the major drawback of being very energy-intensive and susceptible to 51% attacks [123]. In contrast, the consensus used in this work, which is based on the Hyperledger platform, is open and consumes less energy, making it an ideal solution for countries

with significant energy deficits. In other words, developers can define their own consensus rules or choose between PoW, PoS, PoA, etc.

From a security standpoint, the results obtained in this work are varied. Forms are equipped with a unique identification number obtained after the generation of the act form, thus characterizing the uniqueness of a document in the distributed database. The QR code printed on this form allows verification of the signatory author of a document as well as the associated key pair (public key and private key). The transaction identifier recorded in the blockchain database guarantees the tamper-proof nature of documents, not to mention the SHA-256 cryptographic hash for document signing. Hyperledger Fabric has a particular characteristic in that the created channels can be

accessible or visible to a category of actors in the private blockchain, thus guaranteeing confidentiality in transactions; unlike the public blockchain used by Ethereum where channels are visible to all network members, and anyone can create and read blockchain transactions [47].

Based on the offered functionalities, this work proposes a complete system for managing civil status acts, including declarations (birth declaration, death declaration, marriage ban publication) and the establishment of civil status acts themselves (birth certificate, death certificate, marriage certificate), unlike the works of [14, 38, 44] which focused solely on the security of the form by QR code on the one hand, and on birth and death certificates on the other.

In terms of scalability, which represents the number of transactions processed per unit of time, this paper presents statistics of the order of 3500 transactions per second for the Hyperledger Fabric blockchain compared to 38 transactions per second for the Ethereum platform used in the works [14, 38, 44]. This exponential speed in transaction processing makes the platform a suitable solution for the digitalization of civil status in regions of the territory that have several civil status centers, secondary centers, and affiliated centers.

Mining, on the other hand, is a process of creating a block of transactions and adding it to the Ethereum blockchain. However, since it is computers that execute instructions, they are rewarded at the end of the transaction. For a government platform for the digitization of civil status acts, this solution is inefficient in that it will be necessary to reward the authors of transactions each time, unlike the Hyperledger platform which does not require mining for transaction validation. Finally, the evolutionary factor allows a government authority to consider a possible extension without making major changes. To add an organization, simply create the organization's channel, and its members have access to this channel according to their level of accreditation. The open-source nature of the proposed solution allows developers to make modifications to the source code as they see fit, which is not the case with the Ethereum technology used by [35, 48].

VI. FUTURE WORK

In remote regions lacking administrative infrastructure and electrical grids, establishing birth certificates is often challenging or even impossible. The use of embedded devices like the Raspberry Pi, which are inexpensive and energy-efficient nano computers capable of operating on alternative power sources such as batteries and solar panels, enables the creation of autonomous systems. Equipped with blockchain software, these systems can record birth data locally without requiring a permanent internet connection. When an internet connection becomes available, this data can be synchronized with a secure blockchain, ensuring data integrity [49, 50]. This innovative solution offers numerous advantages, including reliability (data is secure and immutable), accessibility (the solution is suitable for rural areas), equity (all individuals, even in the most remote areas, have access to an official birth certificate), and sovereignty (local communities have greater control over their data). As a result, it contributes to digital inclusion and improves the living conditions of the most vulnerable populations.

Based on the relevance of the research findings, this section outlines future directions for the design of other identity documents and official certificates to reduce document fraud. These include: Marriage certificates, which are issued by a civil registrar and serve as legal proof of marital status; death certificates, which are official administrative documents attesting to a person's death and issued by the civil registrar of the municipality where the death occurred; land titles, which are official certifications of real estate ownership and are considered irrevocable and inalienable; and diplomas, which are official documents conferring a degree or qualification.

VII. CONCLUSION

The birth certificate is a legal and vital document that proves an individual's civil status. The fact that it certifies an individual's identity and family situation makes it a major element generally required in administrative procedures such as national identity cards, passports, diplomas, bank transactions, etc. While blockchain technology is inherently secure, it remains vulnerable to side-channel attacks that exploit indirect information to compromise security[51, 52]. These attacks can leverage variations in execution time to extract cryptographic keys, potentially leading to the alteration of transactions. To mitigate these threats, techniques such as obfuscation, which aims to make code difficult to understand, analyze, or modify, are crucial. As a result, continuous vigilance is necessary to safeguard blockchain systems against such vulnerabilities. This article aims to contribute to the development of a system for issuing, tracking, and authenticating birth certificates based on Hyperledger Fabric blockchain technology. To achieve this, the network architecture model is proposed, it based on VPN/MPLS on one hand, and on the other hand, the design of the smart contract characterized by the creation, registration, and verification of birth certificates, the approval of transactions by approving nodes, the transparency and traceability of the various processes, the security throughout the network, and the architecture composed of imported packages, Data Structures, main Functions, Birth Declaration Functions, and Birth Certificate Functions. The proposed platform is an application for creating, registering, and verifying the authenticity of birth certificates, ensuring robust and efficient security-and transparency. This platform is particularly important for organizations responsible for producing birth certificates, diplomatic representations, judicial and administrative authorities, etc.

REFERENCES

- [1] J. Arkko, "The influence of internet architecture on centralised versus distributed internet services," *Journal of Cyber Policy*, vol. 5, no. 1, pp. 30-45, 2020.
- [2] R. Heeks, "Centralised vs. decentralised management of public information systems: a core-periphery solution," *Information Systems for Public Sector Management Working Paper*, no. 7, 1999.
- [3] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, "Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 73-84, 2023.
- [4] J. Sacha et al., "Decentralising a service-oriented architecture," *Peer-to-Peer Networking and Applications*, vol. 3, pp. 323-350, 2010.
- [5] L. Ghirio et al., "What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things," *arXiv preprint arXiv:2102.03750*, 2021.

- [6] C. Zadra-Veil et al., "Blockchain et Immobilier: Le Smart Bail," ed, 2021.
- [7] A. S. Ghanghoria, A. S. A. Raja, V. J. Bachche, and M. N. Rathi, "Secure E-documents storage using blockchain," *Int. Res. J. Eng. Technol.(IRJET)*, vol. 7, pp. 1972-1974, 2020.
- [8] A. Zaky and I. G. B. B. Nugraha, "Increase activity time efficiency in official documents management using blockchain-based distributed data storage," in 2019 International Conference on Electrical Engineering and Informatics (ICEEI), 2019: IEEE, pp. 81-86.
- [9] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, 2022.
- [10] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796-3838, 2019.
- [11] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.
- [12] N. Mishra, S. Mistry, S. Choudhary, S. Kudu, and R. Mishra, "Food traceability system using blockchain and QR code," in *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, 2020: Springer, pp. 33-43.
- [13] M. Darisi, O. Modi, V. Mistry, and D. Patel, "MapReduce-based framework for blockchain scalability," in *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, 2020: Springer, pp. 119-132.
- [14] V. Shah, K. Padia, and V. B. Lobo, "Application of Blockchain Technology in Civil Registration Systems," in *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, 2020: Springer, pp. 191-204.
- [15] M. Hashemi Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," *Managerial Finance*, vol. 46, no. 6, pp. 715-733, 2020.
- [16] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of network and computer applications*, vol. 135, pp. 62-75, 2019.
- [17] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain application in healthcare systems: a review," *Systems*, vol. 11, no. 1, p. 38, 2023.
- [18] D. Dujak and D. Sajter, "Blockchain applications in supply chain," *SMART supply network*, pp. 21-46, 2019.
- [19] N. Kawaguchi, "Application of blockchain to supply chain: Flexible blockchain technology," *Procedia Computer Science*, vol. 164, pp. 143-148, 2019.
- [20] A. Saari, J. Vimpari, and S. Junnila, "Blockchain in real estate: Recent developments and empirical applications," *Land Use Policy*, vol. 121, p. 106334, 2022.
- [21] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K. R. Choo, "The application of the blockchain technology in voting systems: A review," *ACM Computing Surveys (CSUR)*, vol. 54, no. 3, pp. 1-28, 2021.
- [22] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in 2017 International smart cities conference (ISC2), 2017: IEEE, pp. 1-4.
- [23] H. Song, N. Zhu, R. Xue, J. He, K. Zhang, and J. Wang, "Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection," *Information processing & management*, vol. 58, no. 3, p. 102507, 2021.
- [24] X. Wang et al., "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10-29, 2019.
- [25] M. A. Khan, S. M. Khan, and S. K. Subramaniam, "SECURITY ISSUES IN CLOUD COMPUTING USING EDGE COMPUTING AND BLOCKCHAIN: THREAT, MITIGATION, AND FUTURE TRENDS-A SYSTEMATIC LITERATURE REVIEW," *Malaysian Journal of Computer Science*, vol. 36, no. 4, 2023.
- [26] M. Swan, "Anticipating the economic benefits of blockchain," *Technology innovation management review*, vol. 7, no. 10, pp. 6-13, 2017.
- [27] D. Guegan, "Blockchain publique versus blockchain privée: Enjeux et limites," 2017.
- [28] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan, and H. Zhang, "Meepo: Sharded consortium blockchain," in 2021 IEEE 37th International Conference on Data Engineering (ICDE), 2021: IEEE, pp. 1847-1852.
- [29] M. Valenta and P. Sandner, "Comparison of ethereum, hyperledger fabric and corda," *Frankfurt School Blockchain Center*, vol. 8, pp. 1-8, 2017.
- [30] A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat, and S. Chatterjee, "Performance characterization of hyperledger fabric," in 2018 Crypto Valley conference on blockchain technology (CVCBT), 2018: IEEE, pp. 65-74.
- [31] G. Greenspan, "Multichain private blockchain-white paper," URL: <http://www.multichain.com/download/MultiChain-White-Paper.pdf>, vol. 85, 2015.
- [32] M. Hearn and R. G. Brown, "Corda: A distributed ledger," *Corda Technical White Paper*, vol. 2016, p. 6, 2016.
- [33] D. Level, "Level DB database," *Level DB Database*, 2018.
- [34] D. Couch, "Couch DB database," *Couch DB Database*, 2018.
- [35] V. Shah, K. Padia, and V. B. Lobo, "Application of Blockchain Technology in Civil Registration Systems," in *IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology*, 2020: Springer, pp. 191-204.
- [36] C. Chen, C. Lin, M. Chiang, Y. Deng, P. Chen, and Y. Chiu, "A traceable online will system based on blockchain and smart contract technology. *Symmetry*. 13 (3), 466 (2021)," ed.
- [37] P. K. Okoth, "Security challenges in civil registration: safeguarding vital information in an evolving landscape," *World Journal of Advanced Research and Reviews*, vol. 19, no. 1, pp. 1051-1071, 2023.
- [38] J. Shi, S. K. N. Danquah, W. J. I. J. o. E. R. Dong, and P. Health, "A Novel Block Chain Method for Urban Digitization Governance in Birth Registration Field: A Case Study," vol. 19, no. 15, p. 9309, 2022.
- [39] N. Sharma, M. Afzal, and A. Dixit, "Blockchain-blockcerts based birth/death certificate registration and validation," *International Journal of Information Technology (IJIT)*, vol. 6, no. 2, 2020.
- [40] C. U. Bennett, O. A. Ojerinde, H. O. Aliyu, and A. S. Adepoju, "Registration and Verification of Birth Certificate using Blockchain Technology," 2022.
- [41] M. M. Ebenezer, P. Félix, M. Yannick, S. N. P. Junior, N. N. J. I. J. o. A. C. S. Léandre, and Applications, "Contribution to the improvement of cryptographic protection methods for medical images in DICOM format through a combination of encryption method," vol. 12, no. 4, 2021.
- [42] T. T. M. Eddy, B. B. Georges, and N. E. P. Salomon, "Towards a New Model for the Production of Civil Status Records Using Blockchain," *Journal of Information Security*, vol. 14, no. 1, pp. 52-75, 2022.
- [43] S. Mthethwa, N. Dlamini, and G. Barbour, "Proposing a blockchain-based solution to verify the integrity of hardcopy documents," in 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), 2018: IEEE, pp. 1-5.
- [44] R. M. Thamrin, E. P. Harahap, A. Khoirunisa, A. Faturahman, and K. J. A. j. o. r. i. Zelina, "Blockchain-based land certificate management in indonesia," vol. 2, no. 2, pp. 232-252, 2021.
- [45] R. Berné, "Qu'est-ce que la scalabilité d'une blockchain ?" <https://cryptoast.fr/scalabilite-definition-explication/> (accessed 11/11, 2023).
- [46] J.-P. Delahaye, "Chapitre 7. L'univers des cryptomonnaies," in *Au-delà du Bitcoin*. Paris: Dunod, 2022, pp. 149-173.
- [47] M. Castro and B. J. A. T. o. C. S. Liskov, "Practical byzantine fault tolerance and proactive recovery," vol. 20, no. 4, pp. 398-461, 2002.
- [48] T. J. W. V. L. R. Cutts, "Smart contracts and consumers," vol. 122, p. 389, 2019.
- [49] K.-K. R. Choo, M. M. Kermani, R. Azarderakhsh, and M. Govindarasu, "Emerging embedded and cyber physical system security challenges and innovations," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 235-236, 2017.
- [50] A. Jalali, R. Azarderakhsh, M. M. Kermani, and D. Jao, "Towards optimized and constant-time CSIDH on embedded devices," in *Constructive Side-Channel Analysis and Secure Design: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings 10, 2019: Springer*, pp. 215-231.

- [51] D. Jauvart, J. J. Fournier, N. El-Mrabet, and L. Goubin, "Improving side-channel attacks against pairing-based cryptography," in *Risks and Security of Internet and Systems: 11th International Conference, CRIStS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers 11*, 2017: Springer, pp. 199-213.
- [52] X. Lou, T. Zhang, J. Jiang, and Y. Zhang, "A survey of microarchitectural side-channel vulnerabilities, attacks, and defenses in cryptography," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1-37, 2021.